On Security Proofs of Existing Equivalence Class Signature Schemes

Balthazar Bauer[1], Georg Fuchsbauer[2], and Fabian Regen[2]

[1] UVSQ, France
[2] TU Wien, Austria
`first.last@{ens.fr, tuwien.ac.at}`

Abstract. Equivalence class signatures (EQS; Asiacrypt '14), sign vectors of elements from a bilinear group. Anyone can transform a signature on a vector to a signature on any multiple of that vector; signatures thus authenticate equivalence classes. A transformed signature/message pair is indistinguishable from a random signature on a random message. EQS have been used to efficiently instantiate (delegatable) anonymous credentials, (round-optimal) blind signatures, ring and group signatures, anonymous tokens and contact-tracing schemes, to name a few.
The original EQS construction (J. Crypto '19) is proven secure in the generic group model, and the first scheme from standard assumptions (PKC '18) satisfies a weaker model insufficient for most applications. Two works (Asiacrypt '19, PKC '22) propose applicable schemes that assume trusted parameters. Their unforgeability is argued via a security proof from standard (or non-interactive) assumptions.
We show that their security proofs are flawed and explain the subtle issue. While the schemes might be provable in the algebraic group model (AGM), we instead show that the original construction, which is more efficient and has found applications in many works, is secure in the AGM under a parametrized non-interactive hardness assumption.

Keywords: Equivalence class signatures · flaw in existing analysis · security proof · algebraic group model.

1 Introduction

Structure-preserving signatures (SPS) [AFG+10] are defined over a *bilinear group*, which consists of three groups $(\mathbb{G}_t, +)$, for $t \in \{1, 2, T\}$, of prime order p and a (non-degenerate) bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In SPS, messages, as well as public verification keys and signatures, consist of elements from $\mathbb{G}_1$ and $\mathbb{G}_2$.

The concept of *SPS on equivalence classes*, or *equivalence class signatures* (EQS) for short, was introduced by Hanser and Slamanig [HS14] and later securely instantiated [Fuc14, FHS19]. EQS have message space $\mathcal{M} = (\mathbb{G}_t^*)^\ell$, for some $t \in \{1, 2\}$, $\ell > 1$, where $\mathbb{G}_t^* := \mathbb{G}_t \setminus \{0_t\}$, on which one defines the following equivalence relation:

$$\boldsymbol{M} \sim \boldsymbol{M'} \;:\Leftrightarrow\; \exists\, \mu \in \mathbb{Z}_p^* : \boldsymbol{M'} = \mu \cdot \boldsymbol{M}. \tag{1}$$

EQS provide an additional functionality ChgRep: given a public key pk, a signature σ on $\boldsymbol{M} \in \mathcal{M}$ under pk, and a value $\mu \in \mathbb{Z}_p^*$, ChgRep returns a signature on the message $\mu \cdot \boldsymbol{M}$, without requiring the secret key. A signature on $\boldsymbol{M}$ thus authenticates the entire equivalence class $[\boldsymbol{M}]_\sim$ of $\boldsymbol{M}$ w.r.t. the relation in (1), and ChgRep lets one change the *representative* of that class.

Accordingly, *unforgeability* is defined w.r.t. classes, that is, for all efficient adversaries, given pk and an oracle for signatures on messages $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots$ of their choice, it is infeasible to compute a signature on any $\boldsymbol{M}^*$ for which $\boldsymbol{M}^* \notin [\boldsymbol{M}_1]_\sim \cup [\boldsymbol{M}_2]_\sim \cup \ldots$ In addition, EQS must be *class-hiding*: it is hard to distinguish random message pairs $(\boldsymbol{M}, \boldsymbol{M}')$ with $\boldsymbol{M} \sim \boldsymbol{M}'$ from random pairs $(\boldsymbol{M}, \boldsymbol{M}') \leftarrow\!\!\$\, \mathcal{M} \times \mathcal{M}$, which is equivalent to the decisional Diffie-Hellman (DDH) problem being hard in $\mathbb{G}_t$.

The last security notion is *signature adaptation*, requiring that for any (possibly maliciously generated) public key pk, any $\boldsymbol{M} \in \mathcal{M}$, any σ that verifies on $\boldsymbol{M}$ under pk, and any $\mu \in \mathbb{Z}_p^*$, running $\mathsf{ChgRep}(pk, \boldsymbol{M}, \sigma, \mu)$ returns a uniform element in the set of all valid signatures on $\mu \cdot \boldsymbol{M}$. This notion, together with class-hiding, implies that a malicious signer that is given some $\boldsymbol{M}$ and generates a signature σ on $\boldsymbol{M}$ cannot distinguish the following: either $\sigma' \leftarrow \mathsf{ChgRep}(pk, \boldsymbol{M}, \sigma, \mu)$ and $\mu \cdot \boldsymbol{M}$ for $\mu \leftarrow\!\!\$\, \mathbb{Z}_p^*$; or a uniformly random signature on a message $\boldsymbol{M}' \leftarrow \mathcal{M}$ under pk.

Applications of EQS. Equivalence class signatures have found numerous applications in concepts related to anonymous authentication. The resulting instantiations are particularly efficient, since both messages and signatures can be *re-randomized*, after which they can be given (and verified) “in the clear”, where in other constructions they need to be hidden and shown valid using zero-knowledge proofs.

Anonymous credentials. The first application of EQS was the construction of *attribute-based credentials* [CL03], which let users obtain credentials for a set of attributes, of which they can later selectively disclose any subset. Such *showings* of attributes should be unlinkable and reveal only the disclosed attributes. The EQS-based credential construction [FHS19] is the first for which the communication complexity of showing a credential is independent of the number of disclosed attributes. Moreover, it achieves strong anonymity guarantees even against malicious credential issuers. Slamanig and others added revocation of users [DHS15] and give a scheme that enables outsourcing of sensitive computation to a restricted device [HS21].

“Signatures with flexible public key” [BHKS18] adapt the concept of adaptation within equivalence classes from messages to public keys, and “mercurial signatures” [CL19, CL21, CLP22] let one adapt signatures to equivalent keys and equivalent messages. The initial motivation of mercurial signatures was the construction of (non-interactively) *delegatable* anonymous credentials [BCC+09, Fuc11], which were later improved [MSBM23]. Multi-authority anonymous credentials have also been constructed from mercurial signatures [MBG+23].

Blind signatures. Building on earlier work [FV10] that uses randomizable zero-knowledge proofs [FP09], another line of research [FHS15, FHKS16] constructs *blind signatures* from EQS. These allow a user to obtain a signature from a signer, who learns nothing about the message nor the signature. These EQS-based schemes do not assume a common reference string, achieve blindness against malicious signers and are round-optimal and thus concurrently secure.

Group signatures. Derler and Slamanig [DS16] and Clarisse and Sanders [CS20] use EQS to construct very efficient group signatures schemes. The former also added dynamic adding of members [DS18].

Further applications of EQS include *verifiably encrypted signatures* [HRS15], *access-control encryption* [FGKO17], *sanitizable signatures* [BLL+19], privacy-preserving *incentive systems* [BEK+20], *policy-compliant signatures* [BSW23], *e-voting* [Poi23], and many more.

The FHS scheme. The first EQS scheme [FHS19], to which we will refer as FHS, has signatures in $\mathbb{G}_1^2 \times \mathbb{G}_2$. This is optimal, since any EQS scheme can be transformed into a structure-preserving signature (SPS) scheme without changing the signature format [FHS15], and SPS signatures must have at least 3 group elements [AGHO11]. Concretely, e.g., when instantiating FHS over the BLS curve [BLS04] BLS12-381 [Bow17, SKSW22], which is conjectured to have 128-bit security, an FHS signature is 192 bytes long.

In addition to yielding optimal instantiations of the aforementioned EQS applications, FHS has seen further applications, such as building highly scalable *mix nets* [HPP20]. Benhamouda, Raykova and Seth [BRS23] use FHS for the currently most efficient instantiation of *anonymous counting tokens*; Hanzlik [Han23] has recently used FHS to construct the first *non-interactive* blind signatures on random messages; and Mir et al. [MSBM23] extended the scheme for their practical delegatable credentials. FHS has been also been proposed for authentication of commercial drones [WTSD23], in the context of e-health [ZYY+23], for whistleblowing reporting systems [SYF+23] and e-voting [Poi24].

Furthermore, FHS underlies the *mercurial signature* construction by Crites and Lysyanskaya [CL19], which have themselves found many applications, some of which are: *Protego* [CDLP22], a credential scheme for permissioned blockchains (like Hyperledger Fabric) and *PACIFIC* [GL23], a privacy-preserving contact tracing scheme. Putman and Martin [PM23] use a modification to construct a delegatable credential scheme that lets users selectively delegate attributes.

The major downside of FHS is that the only proof of its unforgeability to date is directly in the (bilinear) generic group model (GGM) [Nec94, Sho97, Mau05, BBG05], which only captures generic attacks (i.e., ones that work in any group). In security games in the GGM, the adversary does not see any actual group elements but is given (random) labels for them; to compute the group operation, the adversary has access to an oracle which, when given two labels of two elements, returns the label of the sum of these elements.

Constructions from falsifiable assumptions. A computational hardness assumption is *falsifiable* [Nao03] if the challenger that runs the security game with an adversary can efficiently decide whether the adversary has broken the assumption. The FHS scheme [FHS19] can be considered based on an (interactive and) *non-falsifiable* assumption: namely its unforgeability, justified via a proof in the generic group model (GGM). Recall that to determine whether the adversary broke unforgeability, one needs to check whether the message $\boldsymbol{M}^*$ returned by the adversary is in the same equivalence class as one of the queried messages (in which case the adversary could efficiently compute a signature on $\boldsymbol{M}^*$ via ChgRep). Now, by the *class-hiding* property, this is hard to decide.

The first EQS scheme from standard assumptions, namely Matrix-Diffie-Hellman assumptions [EHK+13], was proposed by Fuchsbauer and Gay [FG18], but the scheme has some drawbacks: its signatures can only be adapted once and it only satisfies a weaker notion called *existential unforgeability under chosen open message attack* (EUF-CoMA): when the adversary makes a signing query, it must provide the discrete logarithms of the components of the queried message. Note that EUF-CoMA *is* efficiently decidable: For simplicity, consider $\ell = 2$ and for all i, let $(m_{i,1}, m_{i,2}) \in (\mathbb{Z}_p^*)^2$ be the adversary's queries (i.e., the logarithms of the components of the queried message $\boldsymbol{M}_i$). Then the message $\boldsymbol{M}^* = (M_1^*, M_2^*)$ returned by the adversary is not in any of the queried classes if and only if $m_{i,2} \cdot M_1^* \neq m_{i,1} \cdot M_2^*$ for all i.

Khalili, Slamanig and Dakhilalian [KSD19] show that the notion of *signature adaption* achieved by the scheme [FG18] must assume honest keys and signatures, which makes it inadequate for most applications. To construct a scheme appropriate for applications with standard-model security, they first propose more syntax modifications: in addition to a signature, the signing algorithm also creates a *tag*, which is required by ChgRep (but not needed for signature verification). As with the previous scheme [FG18], signatures can only be adapted once (which does not affect the considered applications).

Moreover, they consider a trusted setup, which generates a *common reference string* (CRS) in addition to setting up the bilinear group. *Signature adaptation* is then defined w.r.t. honestly generated parameters. This change weakens the anonymity guarantees in applications such as anonymous credentials, which did not require trust assumptions in the original model [FHS19].

Building on an SPS scheme by Gay et al. [GHKP18], Khalili et al. [KSD19] propose an EQS construction in their new model with signatures in $\mathbb{G}_1^8 \times \mathbb{G}_2^9$. Their construction is (claimed to be) secure under the *SXDH* assumption, which states that DDH is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$. Building on this work, Connolly, Lafourcade and Perez-Kempner [CLP22] propose a more efficient scheme (with signatures in $\mathbb{G}_1^9 \times \mathbb{G}_2^4$), which requires as additional assumption *extKerMDH* [CH20].

A flaw in the security proof of the CRS-based schemes. We report a flaw in the security proofs of the two CRS-based schemes [KSD19, CLP22]. In particular, a game hop in the unforgeability proof changes the distribution of the signatures given to the adversary. The change in the adversary's winning probability is then bounded by the advantage of a reduction in solving a computational problem. However, since EQS-unforgeability is not efficiently decidable, the resulting reduction would not be efficient, and the security bound of the underlying problem can thus not be applied. In fact, the authors do specify an efficient reduction, but its winning probability is not the difference of the adversary's winning probabilities.

In more detail, the hop from Game 0 to Game 1 [KSD19, Theorem 2] modifies the way the purported forgery, i.e, the signature on $\boldsymbol{M}^*$ output by the adversary $\mathcal{A}$ is verified. The authors then argue that from a forgery that verifies in Game 0 but not Game 1 (which is a property that can be checked efficiently), a reduction $\mathcal{B}$ can extract a solution to a computational problem (*KerMDH* [MRV16]). From this, the authors deduce that $\mathbf{Adv}_0 - \mathbf{Adv}_1 \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{KerMDH}}$. This reasoning is *correct*, because (though not stated by the authors) $\mathcal{A}$'s view is equally distributed in both games and thus the probability that $\boldsymbol{M}^*$ does not fall in a class of a queried message (which is not efficiently verifiable) is the same.

In contrast, an analogous argument cannot be made for the hop from Game 2 to Game 3. Here the distribution of the signatures output by the signing oracle changes. (Note that we do not claim that the two games are efficiently distinguishable.) Since the games are different, the probability that $\boldsymbol{M}^*$ falls in a queried class can change in arbitrary ways, but, by class-hiding, this is not efficiently detectable. A change can therefore not be leveraged by an efficient reduction. In fact, the constructed reduction $\mathcal{B}_1$ (to their "core lemma", which relies on the computational hardness of *MDDH* [EHK+17]) only checks an (efficiently testable) property of $\mathcal{A}$'s forgery (but not whether $\mathcal{A}$ was successful). Since whether $\boldsymbol{M}^*$ falls in a queried class determines whether the adversary wins, one can therefore not deduce that $\mathbf{Adv}_2 - \mathbf{Adv}_3 \leq \mathbf{Adv}_{\mathcal{B}_1}^{\mathrm{core}}$, as the authors do. We detail our argument in Sect. 3.

The proof of the second CRS-based scheme [CLP22, eprint, Appendix D] is virtually identical, so the same issue arises. The security of both schemes is thus currently unclear. We believe the schemes cannot be proved from non-interactive assumptions in the standard model. They were derived from a signature scheme [GHKP18] built with proof techniques in mind that crucially rely on the winning condition being efficiently checkable, which is the case for signatures but not for EQS.

Unforgeability of FHS in the algebraic group model. A recent result [BFR24] shows it is unlikely that EQS can be constructed from non-interactive (falsifiable) assumptions in the standard model (that is, without assuming a trusted CRS). Concretely, for any EQS scheme Σ, if there is a reduction that breaks a non-interactive computational assumption after running an adversary that breaks unforgeability of Σ, then there exist efficient meta-reductions that either break the assumption or break class-hiding of Σ. For FHS [FHS19], it was already known that it cannot be proved from non-interactive assumptions via an *algebraic* reduction, since this is the case for all 3-element SPS, and thus EQS, schemes [AGO11].

In light of this result, what we can still hope for is an EQS scheme with a security proof in the *algebraic group model* [FKL18], which is a "weaker" idealized model than the generic group model. In contrast to the latter, in the AGM the adversary has access to the group elements, but the adversary is assumed to be *algebraic* in the following sense: whenever it outputs an element Y of a group $\mathbb{G}_t$, for $t \in \{1,2\}$, it also provides a *representation* $(\alpha_1, \alpha_2, \dots)$ so that $Y = \alpha_1 Y_1 + \alpha_2 Y_2 + \cdots$, where $Y_1, Y_2, \dots$ are the $\mathbb{G}_t$-elements the adversary has previously received.

Our positive result is a security proof of FHS [FHS19] in the algebraic group model. We focus on FHS due to its optimal efficiency and its many applications discussed above. While the CRS-based schemes [KSD19, CLP22] might be salvageable in the AGM, trying to would be moot, as the signatures of the more efficient scheme [CLP22] are more than 4 times longer than for FHS. Moreover, FHS requires no CRS, an assumption that bars some of the applications of EQS.

We reduce unforgeability of FHS to a parametrized assumption related to the *q-strong Diffie-Hellman* assumption in bilinear groups [BB08]. The latter states that given $G_1, xG_1, x^2G_1, \dots, x^qG_1, G_2, xG_2$, where G_i is a generator of $\mathbb{G}_i$ and x is uniform in $\mathbb{Z}_p$, it is hard to find any $c \in \mathbb{Z}_p$ together with $\frac{1}{x+c}G_1$. Boneh and Boyen [BB08] show that if G_1 and G_2 are random generators, this implies security of their *weakly secure* signature scheme, which corresponds to being given a public key xG_2 and signatures $\frac{1}{x+c_i}G_1$ on messages $c_1, \dots, c_q$ and having to find $\frac{1}{x+c}G_1$ for $c \notin \{c_1, \dots, c_q\}$.

Our assumption combines the above two but is weaker in the sense that it would correspond to security only against key-recovery attacks, where the adversary must find x. In particular, we assume that given x^iG_1 for $i = 1, \dots, 2q$ and xG_2 as well as $\frac{1}{x+c_i}G_t$ for random c_i for $i = 1, \dots, q$ and $t = 1, 2$, it must be hard to find x. Following Boneh and Boyen, we show that, assuming random generators, for $q_1 := 3q$ and $q_2 := q+1$ our assumption is implied by the (q_1, q_2)-"power"-DL assumption [Lip12], which requires finding x when given x^iG_t for $t = 1, 2$ and $i = 1, \dots, q_t$. (We note that separation results [BFL20] show it is implausible that power-DL can be shown from DL.)

When setting up the group for an FHS instantiation, one can simply sample random generators; in this case, our results imply AGM-security under power-DL, which now underlies the majority of AGM proofs in the literature, in particular for zk-SNARK schemes [FKL18, MBKM19, GWC19, CHM+20, RZ21, CFF+21, LSZ22]. (On the other hand, if generators are fixed, we still get security under our new assumption.)

Discussion. One might wonder about the value of a proof in the AGM when we already have a GGM proof. First, the AGM is closer to reality, as the adversary attacks the actual scheme and not an ideal simulation of it like in the GGM; the AGM just restricts how the adversary manipulates group elements, which is enforced in the GGM as well. Given the EQS impossibility result [BFR24], an AGM proof from a non-interactive assumption is arguably the best one can hope for. (The situation is similar for zk-SNARKs, for which there are impossibility results [GW11], and the AGM has become a common model for security analysis; see citations above.) While our proof may be more complex than the GGM proof [FHS19], we improve the result, since a proof in the AGM from an assumption that holds in the GGM implies security in the GGM. (Conversely, there are hardness assumptions, such as *one-more DL* [BNPS03, BFP21], that hold in the GGM but cannot be shown in the AGM from power-DL [BFL20].)

We thus establish a new state of the art for EQS: There are currently no EQS schemes assuming a trusted CRS with a security proof in the standard model. Moreover, our negative result indicates that new proof techniques would be required, instead of starting from existing standard-model SPS schemes like [GHKP18]. Many applications (blind signatures, credentials, etc.) without semi-honesty assumptions require fully secure EQS (without a CRS), for which FHS is the most efficient scheme and has seen many applications. We improve the security guarantees of FHS.

2 Preliminaries

Notation. Assigning a value x to a variable var is denoted by $\mathit{var} := x$. All algorithms are randomized unless otherwise indicated. By $y \leftarrow \mathcal{A}(x_1, \ldots, x_n)$ we denote the operation of running algorithm $\mathcal{A}$ on inputs $x_1, \ldots, x_n$ and letting y denote the output; by $[\mathcal{A}(x_1, \ldots, x_n)]$ we denote the set of values that have positive probability of being output. If S is a finite set then $x \leftarrow\!\!\$\, S$ denotes picking an element uniformly from S and assigning it to x. For $n \in \mathbb{N}$, we let $[n]$ denote the set $\{1, \ldots, n\}$. For $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$, we denote $\mathbf{x} \odot \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$ the Hadamard product of $\mathbf{x}$ and $\mathbf{y}$.

Polynomials. In our proof the FHS scheme in Section 4 we will make extensive use of multivariate polynomials in $\mathbb{Z}_p[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, for prime p, and use the following two lemmas.

Lemma 1 (Schwartz-Zippel). *Let p be prime and let $\mathsf{P} \in \mathbb{Z}_p[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ be a non-zero polynomial of total degree d. Then*

$$\Pr_{r_1, \ldots, r_n \leftarrow\!\$\, \mathbb{Z}_p^*}[\mathsf{P}(r_1, \ldots, r_n) = 0] \leq \frac{d}{p-1} \ .$$

The next lemma [BFL20, Lemma 2.1] has become a standard tool in AGM proofs. It implies that when embedding an indeterminate Y (which will represent the solution of a computational problem) into many indeterminates $\mathrm{X}_1, \ldots, \mathrm{X}_n$ of an adversarially chosen non-zero polynomial P by "randomizing" Y as $\mathrm{X}_i := z_i \mathrm{Y} + v_i$ for random z_i, v_i then the polynomial $\mathsf{P}'(\mathrm{Y}) := \mathsf{P}(z_1 \mathrm{Y} + v_1, \ldots, z_n \mathrm{Y} + v_n)$ will be non-zero with overwhelming probability. (This relies on the fact that the values z_i are perfectly hidden from the adversary's view.)

Lemma 2. *Let P be a non-zero multivariate polynomial in $\mathbb{Z}_p[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ of total degree d. If we define $\mathsf{Q}(\mathrm{Y}) \in \big(\mathbb{Z}_p[\mathrm{Z}_1, \ldots, \mathrm{Z}_m, \mathrm{V}_1, \ldots, \mathrm{V}_n]\big)[\mathrm{Y}]$ as*

$$\mathsf{Q}(\mathrm{Y}) := \mathsf{P}\big(\mathrm{Z}_1 \mathrm{Y} + \mathrm{V}_1, \ldots, \mathrm{Z}_n \mathrm{Y} + \mathrm{V}_n\big) \ ,$$

then the coefficient of maximal degree of Q is a polynomial in $\mathbb{Z}_p[\mathrm{Z}_1, \ldots, \mathrm{Z}_n]$ of degree d.

Bilinear groups. EQS schemes are defined over an (asymmetric) bilinear group $grp = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G_1, G_2, e)$, where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are (additively denoted) groups of prime order p, G_1 and G_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, resp., and $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map so that $G_T := e(G_1, G_2)$ generates $\mathbb{G}_T$. For $t \in \{1, 2, T\}$, we let $\mathbb{G}_t^* := \mathbb{G}_t \setminus \{0_t\}$. We assume that there exists a probabilistic polynomial-time (p.p.t.) algorithm BGGen, which on input 1^λ, the security parameter in unary, returns the description of a bilinear group grp so that the bit length of p is λ.

Following the examined work [KSD19], we use "implicit" representation of group elements: for $\mathbf{A} = (a_{i,j})_{i,j} \in \mathbb{Z}_p^{m\times n}$ and $t \in \{1, 2, T\}$, we let $[\mathbf{A}]_t$ denote the matrix $(a_{i,j}G_t)_{i,j} \in \mathbb{G}_t^{m\times n}$ and define $e([\mathbf{A}]_1, [\mathbf{B}]_2)$ as $[\mathbf{AB}]_T$, which can be computed efficiently. We use upper-case slanted font $G, \boldsymbol{G}$ to denote group elements and vectors of group elements and use $a, \mathbf{a}, \mathbf{A}$ to denote scalars, vectors and matrices of elements from $\mathbb{Z}_p$.

EQS. An *equivalence class signature (EQS) scheme* Σ specifies an algorithm $\mathsf{ParGen}(1^\lambda)$, which on input the security parameter returns general parameters par, which specify a bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G_1, G_2, e)$. $\mathsf{KeyGen}(par, 1^\ell)$, on input the parameters and the message length $\ell > 1$, returns a key pair (sk, pk), which defines the message space $\mathcal{M} := (\mathbb{G}_t^*)^\ell$ for a fixed $t \in \{1, 2\}$. The message space is partitioned into equivalence classes by the following relation for $\boldsymbol{M}, \boldsymbol{M}' \in \mathcal{M}$:

$$\boldsymbol{M} \sim \boldsymbol{M}' :\Leftrightarrow \exists\, \mu \in \mathbb{Z}_p^* : \boldsymbol{M}' = \mu \cdot \boldsymbol{M}. \tag{1}$$

A *tag-based* EQS scheme [KSD19] moreover consists of the following algorithms:

- $\mathsf{Sign}(sk, \boldsymbol{M})$, on input a secret key and a message $\boldsymbol{M} \in \mathcal{M}$, returns a signature σ and (possibly) a tag τ.
- $\mathsf{ChgRep}(pk, \boldsymbol{M}, (\sigma, \tau), \mu)$, on input a public key, a message $\boldsymbol{M} \in \mathcal{M}$, a signature σ (and possibly a tag τ) on $\boldsymbol{M}$, as well as a scalar $\mu \in \mathbb{Z}_p^*$, returns a signature σ' on the message $\mu \cdot \boldsymbol{M}$.
- $\mathsf{Verify}(pk, \boldsymbol{M}, (\sigma, \tau))$ is deterministic and, on input a public key, a message $\boldsymbol{M} \in \mathcal{M}$, a signature σ (and possibly a tag τ), returns a bit indicated acceptance.

Sign and ChgRep must generate valid signatures, as defined next.

Definition 1. *An EQS scheme is* ***correct*** *if for all $\lambda \in \mathbb{N}$, $\ell > 1$, any $par \in [\mathsf{ParGen}(1^\lambda)]$, $(sk, pk) \in [\mathsf{KeyGen}(par, 1^\ell)]$, $\boldsymbol{M} \in \mathcal{M}$ and $\mu \in \mathbb{Z}_p^*$:*

$$\Pr\big[\mathsf{Verify}\big(pk, \boldsymbol{M}, \mathsf{Sign}(sk, \boldsymbol{M})\big) = 1\big] = 1 \qquad \textit{and}$$
$$\Pr\big[\mathsf{Verify}\big(pk, \mu\cdot\boldsymbol{M}, \mathsf{ChgRep}(pk, \boldsymbol{M}, \mathsf{Sign}(sk, \boldsymbol{M}), \mu)\big) = 1\big] = 1.$$

Unforgeability requires that after receiving the public key and signatures (and tags) on messages of its choice, the adversary cannot produce a valid signature on a message that is not contained in any of the classes of the queried signatures.

Definition 2. *An EQS scheme Σ with message length $\ell > 1$ is* ***existentially unforgeable under chosen-message attack*** *if*

$$\mathsf{Adv}^{\mathrm{UNF}}_{\Sigma,\mathcal{A}}(\lambda) := \Pr[\mathrm{UNF}_{\Sigma,\mathcal{A}}(\lambda) = 1]$$

is negligible for all p.p.t. adversaries $\mathcal{A}$, where game UNF *is defined as follows:*

$\mathrm{UNF}_{\Sigma,\mathcal{A}}(\lambda)$

$par \leftarrow \mathsf{ParGen}(1^\lambda)$
$(sk, pk) \leftarrow \mathsf{KeyGen}(par, 1^\ell)$
$Q := \emptyset$
$(\boldsymbol{M}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(pk)$
$\texttt{return}\ \big(\boldsymbol{M}^* \notin Q \wedge \mathsf{Verify}(pk, \boldsymbol{M}^*, \sigma^*)\big)$

$\mathcal{O}(\boldsymbol{M})$

$Q := Q \cup [\boldsymbol{M}]_\sim$
$\texttt{return}\ \mathsf{Sign}(sk, \boldsymbol{M})$

where $[\boldsymbol{M}]_\sim := \{\boldsymbol{M'} \in \mathcal{M} \mid \boldsymbol{M} \sim \boldsymbol{M'}\}$ is the equivalence class of $\boldsymbol{M}$ for $\sim$ defined in (1).

A further security requirement is that signatures generated by ChgRep should either be indistinguishable from signatures output by Sign or uniformly random in the space of all valid signatures. As these notions are not relevant for our results, we refrain from stating them and refer to the original work [FHS19].

3 A Flaw in the Security Proofs of KSD19 and CLP22

The proof of unforgeability [KSD19] defines Game 0 as the game UNF from Definition 2 instantiated with their construction as Σ, and, in a series of "hops", the games are gradually modified until Game 6 can only be won with probability $1/p$, even by an unbounded adversary. The difference between the adversary's advantage $\mathbf{Adv}_i$ in winning Game i and its advantage $\mathbf{Adv}_{i+1}$ in winning Game $(i+1)$ is then bounded. Of these bounds, two depend on the hardness of a computational problem.

Define event N_i as $\boldsymbol{M}^* \notin Q$ when running Game i (where $\boldsymbol{M}^*$ is from $\mathcal{A}$'s output and Q is the union of all classes of queried messages). Moreover, let V_i be the event that when running Game i, we have $\mathsf{Verify}_i(pk, \boldsymbol{M}^*, \sigma^*)$, where Verify_i is how verification of $\mathcal{A}$'s signature is defined in Game i. (The details of Verify_i are not relevant here.) We thus have $\mathbf{Adv}_i = \Pr[\mathrm{N}_i \wedge \mathrm{V}_i]$.

The first hop. In Game 0 and Game 1 the adversary's view remains the same, and we therefore have $\mathrm{N}_0 = \mathrm{N}_1$. The only thing that changes is that when verifying $\mathcal{A}$'s forgery, which contains group-element vectors $[\mathbf{u}_1^*]_1$ and $[\mathbf{t}^*]_1$, against $pk = ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$, instead of checking

$$e([\mathbf{u}_1^*]_1^\top, [\mathbf{A}]_2) - e([\mathbf{t}^*]_1^\top, [\mathbf{K}_0\mathbf{A}]_2) - e([\mathbf{m}^*]_1^\top, [\mathbf{K}\mathbf{A}]_2) = 0,$$

one checks if $\boldsymbol{S} := [\mathbf{u}_1^*]_1 - \mathbf{K}_0^\top[\mathbf{t}^*]_1 - \mathbf{K}^\top[\mathbf{m}^*]_1 = 0$, which implies the above.

We thus have $\mathrm{V}_1 \subseteq \mathrm{V}_0$ and if V_0 occurs but V_1 does not, then $\mathcal{A}$ has found a non-zero vector $\boldsymbol{S}$ in the kernel of $\mathbf{A}$. The authors construct a reduction $\mathcal{B}$ which uses this to break KerMDH [MRV16] in $\mathbb{G}_2$. We have

$$\begin{aligned}\mathbf{Adv}_0 - \mathbf{Adv}_1 &= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0] - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1] \\ &= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \mathrm{V}_1] + \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \neg\mathrm{V}_1] \\ &\qquad\qquad - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1 \wedge \mathrm{V}_0] - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1 \wedge \neg\mathrm{V}_0] \\ &= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \neg\mathrm{V}_1] \quad (\text{since } \mathrm{N}_0 = \mathrm{N}_1 \text{ and } \mathrm{V}_1 \subseteq \mathrm{V}_0) \\ &\leq \Pr[\mathrm{V}_0 \wedge \neg\mathrm{V}_1] \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{KerMDH}}.\end{aligned}$$

Note that for this argument it was essential that N_0, N_1, V_0 and V_1 are all events in the same probability space (which will not be the case in the hop from Game 2 to Game 3).

The bad hop. In the hop from Game 2 to Game 3, the distribution of the game changes and thus we do not have $\mathrm{N}_2 = \mathrm{N}_3$ (which is also syntactically meaningless). The authors construct a reduction $\mathcal{B}_1$ which bounds $\Pr[\mathrm{V}_2] - \Pr[\mathrm{V}_3] \leq \mathbf{Adv}_{\mathcal{B}_1}^{\mathrm{core}}$, where the latter is $\mathcal{B}_1$'s probability in winning the game from their "core lemma" [KSD19, Sect. 4.1], which is bounded by breaking another computational problem (Matrix-DDH [EHK+17]). However, it is not clear how to use this to bound the change in advantage from Game 2 to Game 3. We have

$$\begin{aligned}\mathbf{Adv}_2 - \mathbf{Adv}_3 &= \Pr[\mathrm{N}_2 \wedge \mathrm{V}_2] - \Pr[\mathrm{N}_3 \wedge \mathrm{V}_3] \\ &= \Pr[\mathrm{N}_2 \,|\, \mathrm{V}_2] \cdot \big(\underbrace{\Pr[\mathrm{V}_2] - \Pr[\mathrm{V}_3]}_{(1)}\big) + \big(\underbrace{\Pr[\mathrm{N}_2 \,|\, \mathrm{V}_2] - \Pr[\mathrm{N}_3 \,|\, \mathrm{V}_3]}_{(2)}\big) \cdot \Pr[\mathrm{V}_3].\end{aligned}$$

So while we can bound (1) by $\mathcal{B}_1$'s advantage of breaking the "core lemma", it is unclear how to bound (2). In particular, N_i is an event that cannot be efficiently checked, and moreover, in contrast to N_0 and N_1, the events N_2 and N_3 are not equivalent, since the adversary's view is different on Game 2 and Game 3.

To show this, we spell out Game i for $i \in \{2,3\}$ in Figure 1, where Verify_i denotes how verification is defined in Game i (both Verify_2 and Verify_3 are efficient, but their details not relevant here). Moreover, $\mathcal{D}_1$ is a distribution of matrices from $\mathbb{Z}_p^{2\times 1}$ for which the MDDH assumption must hold; PGen and PPro belong to a proof system for statements $([\mathbf{t}]_1, [\mathbf{w}]_1)$ which are true if $[\mathbf{t}]_1 = [\mathbf{A}_b]_1 r_1$ and $[\mathbf{w}]_1 = [\mathbf{A}_b]_1 r_2$ for some $b \in \{0,1\}$ and $r_1, r_2 \in \mathbb{Z}_p$ (again, the details are not relevant here); and $\mathbf{F}\colon \mathbb{Z}_p \to \mathbb{Z}_p^2$ is a random function.

To argue that $\mathcal{A}$'s view changes from Game 2 to Game 3, an easy way is to have $\mathcal{A}$ query the signing oracle $\mathcal{O}$ twice on the same (arbitrary) message. For the i-th query, let $r_1^{(i)}$ and $r_2^{(i)}$ be the randomness sampled by $\mathcal{O}$ and let $\mathbf{u}_1^{(i)}, \mathbf{t}^{(i)}, \mathbf{u}_2^{(i)}, \mathbf{w}^{(i)} \in \mathbb{Z}_p^2$ be the logarithms of the respective components returned by $\mathcal{O}$.

Since $\mathbf{A}_0 \in \mathbb{Z}_p^{2\times 1}$ is from a "matrix distribution" [KSD19, Definition 1], it has full rank and is thus non-zero. The value $\mathbf{t}^{(i)} = \mathbf{A}_0 r_1^{(i)}$ thus uniquely

Game $(2+\beta)$

$grp \leftarrow \mathsf{BGGen}(1^\lambda)$; $ctr := 0$
$\mathbf{A}_0 \leftarrow_\$ \mathcal{D}_1$; $\mathbf{A}_1 \leftarrow_\$ \mathcal{D}_1$
$crs \leftarrow \mathsf{PGen}(grp, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1)$
$par := (grp, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1, crs)$
$\mathbf{A} \leftarrow_\$ \mathcal{D}_1$
$\mathbf{K}_0 \leftarrow_\$ \mathbb{Z}_p^{2\times 2}$; $\mathbf{K} \leftarrow_\$ \mathbb{Z}_p^{\ell\times 2}$
$\mathbf{a}^\perp \leftarrow_\$ \{\mathbf{a}^\perp \in \mathbb{Z}_p^2 \mid (\mathbf{a}^\perp)^\top \mathbf{A} = 0\}$
$\mathbf{k}_0 \leftarrow_\$ \mathbb{Z}_p^2$; $\mathbf{k}_1 \leftarrow_\$ \mathbb{Z}_p^2$
$\mathbf{K}_0 := \mathbf{K}_0 + \mathbf{k}_0(\mathbf{a}^\perp)^\top$
$pk := ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$
$Q := \emptyset$
$([\mathbf{m}^*]_1, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(par, pk)$
return $\big([\mathbf{m}^*]_1 \notin Q$
$\quad \wedge \mathsf{Verify}_i(pk, [\mathbf{m}^*]_1, \sigma^*)\big)$

$\mathcal{O}([\mathbf{m}]_1)$

$Q := Q \cup [[\mathbf{m}]_1]_\sim$
$r_1, r_2 \leftarrow_\$ \mathbb{Z}_p$
$[\mathbf{t}]_1 := [\mathbf{A}_0]_1 r_1$; $[\mathbf{w}]_1 := [\mathbf{A}_0]_1 r_2$
$\Omega \leftarrow \mathsf{PPro}(crs, [\mathbf{t}]_1, r_1, [\mathbf{w}]_1, r_2)$
$(\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi) := \Omega$
$ctr := ctr + 1$
$[\mathbf{u}_1]_1 := \mathbf{K}_0^\top [\mathbf{t}]_1 + \mathbf{K}^\top [\mathbf{m}]_1$
$\quad + \mathbf{a}^\perp \big(\mathbf{k}_0 + \beta \cdot \mathbf{F}(ctr)\big)^\top [\mathbf{t}]_1$
$[\mathbf{u}_2]_1 := \mathbf{K}_0^\top [\mathbf{w}]_1$
$\quad + \mathbf{a}^\perp \big(\mathbf{k}_0 + \beta \cdot \mathbf{k}_1\big)^\top [\mathbf{w}]_1$
$\sigma := ([\mathbf{u}_1]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$
$\tau := ([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1)$
return (σ, τ)

Fig. 1. Games 2 and 3 in the unforgeability proof of [KSD19]. Changes w.r.t. game UNF are denoted in gray, the differences between Games 2 and 3 are highlighted in blue. The line in red is our interpretation, since the distribution of $\mathbf{a}^\perp$ is not specified.

determines $r_1^{(i)}$ and $\mathbf{w}^{(i)} = \mathbf{A}_0 r_2^{(i)}$ uniquely determines $r_2^{(i)}$. Let $r_1' := r_1^{(1)} - r_1^{(2)}$ and $r_2' := r_2^{(1)} - r_2^{(2)}$, and thus $\mathbf{t}^{(1)} - \mathbf{t}^{(2)} = \mathbf{A}_0 r_1'$ and $\mathbf{w}^{(1)} - \mathbf{w}^{(2)} = \mathbf{A}_0 r_2'$, and consider these further differences:

$$\mathbf{u}_1' := \mathbf{u}_1^{(1)} - \mathbf{u}_1^{(2)} = \mathbf{K}_0^\top \mathbf{A}_0 r_1' + \mathbf{a}^\perp \mathbf{k}_0^\top \mathbf{A}_0 r_1' + \beta \cdot \mathbf{a}^\perp \big(\mathbf{F}(1)^\top \mathbf{A}_0 r_1^{(1)} - \mathbf{F}(2)^\top \mathbf{A}_0 r_1^{(2)}\big)$$
$$\mathbf{u}_2' := \mathbf{u}_2^{(1)} - \mathbf{u}_2^{(2)} = \mathbf{K}_0^\top \mathbf{A}_0 r_2' + \mathbf{a}^\perp \mathbf{k}_0^\top \mathbf{A}_0 r_2' + \beta \cdot \mathbf{a}^\perp \mathbf{k}_1^\top \mathbf{A}_0 r_2'$$

In Game 2, where $\beta = 0$, we thus have

$$\mathbf{u}_1' r_2' = \mathbf{u}_2' r_1'. \tag{2}$$

On the other hand, for (2) to hold in Game 3, we would have to have

$$\mathbf{a}^\perp \big(\mathbf{F}(1)^\top \mathbf{A}_0 r_1^{(1)} - \mathbf{F}(2)^\top \mathbf{A}_0 r_1^{(2)}\big) r_2' = \mathbf{a}^\perp \mathbf{k}_1^\top \mathbf{A}_0 r_2' (r_1^{(1)} - r_1^{(2)}),$$

or equivalently

$$\mathbf{a}^\perp \big(\underbrace{\mathbf{F}(1)^\top r_1^{(1)} - \mathbf{F}(2)^\top r_1^{(2)} - \mathbf{k}_1^\top (r_1^{(1)} - r_1^{(2)})}_{=:\mathbf{U}^\top}\big) \mathbf{A}_0 r_2' = \mathbf{0}. \tag{3}$$

Since $\mathbf{F}(1)$ is independent and uniformly distributed in $\mathbb{Z}_p^2$, the term $\mathbf{U}$ is uniform in $\mathbb{Z}_p^2$, except with negligible probability (when $r_1^{(1)} = 0$). As argued above, $\mathbf{A}_0$ is non-zero and thus $\mathbf{U}^\top \mathbf{A}_0$ is uniform in $\mathbb{Z}_p$ (except with negligible probability). The authors [GHKP18, KSD19] do not specify how $\mathbf{a}^\perp$ is distributed, but for their last argument in the proof to work, namely that Game 6 can only be won with probability $1/p$ (or with negligible probability), we must have $\mathbf{a}^\perp \neq \mathbf{0}$ (with overwhelming probability). Thus for (3) (and thus (2)) to hold, we must either have $\mathbf{a}^\perp = \mathbf{0}$ or $\mathbf{U}^\top \mathbf{A}_0 = 0$ or $r_2' = 0$, which happens with negligible probability only.

Thus, the view of the adversary changes between Games 2 and 3, and therefore so can its probability of returning a messages that is in the class of a queried message, i.e., we can have that $\Pr[\mathrm{N}_2]$ and $\Pr[\mathrm{N}_3]$ differ by a non-negligible amount. The argument which worked for bounding $\mathbf{Adv}_0 - \mathbf{Adv}_1$ (a reduction that only considers the events V_0 and V_1), and which the authors also apply to bound $\mathbf{Adv}_2 - \mathbf{Adv}_3$, can thus not be made again.

4 The Security of FHS in the AGM

With the FHS EQS scheme remaining the only scheme with some security proof [FHS19], we will strengthen its security guarantees by giving a proof in the *algebraic group model* (AGM) under a parametrized hardness assumption. We start with defining the scheme.

Definition 3 ([FHS19]). *Let* $grp = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G, \hat{G}, e)$ *be a bilinear group output by* $\mathsf{BGGen} = \mathsf{ParGen}$. *Let* $\ell > 1$ *and* $\mathcal{M} := (\mathbb{G}_1^*)^\ell$. *The EQS scheme* ***FHS*** *is defined as follows:*

- $\mathsf{KeyGen}(grp, 1^\ell)$*: sample* $\boldsymbol{x} \leftarrow_\$ (\mathbb{Z}_p^*)^\ell$*, set* $sk := \boldsymbol{x}$*,* $pk := \hat{\boldsymbol{X}} = \big(x_1\hat{G}, \ldots, x_\ell\hat{G}\big)$.
- $\mathsf{Sign}(\boldsymbol{x}, \boldsymbol{M})$*: sample* $r \leftarrow_\$ \mathbb{Z}_p^*$ *and return* $\sigma := \Big(r\sum_{i=1}^\ell x_i M_i, \frac{1}{r}G, \frac{1}{r}\hat{G}\Big)$.
- $\mathsf{ChgRep}(\hat{\boldsymbol{X}}, \boldsymbol{M}, (Z, R, \hat{R}), \mu)$ *sample* $r \leftarrow_\$ \mathbb{Z}_p^*$ *and return* $\sigma' := \big(\mu r Z, \frac{1}{r}R, \frac{1}{r}\hat{R}\big)$
- $\mathsf{Verify}(\hat{\boldsymbol{X}}, \boldsymbol{M}, (Z, R, \hat{R}))$*: return* 1 *if and only if*

$$\sum\nolimits_{i=1}^{\ell} e\big(M_i, \hat{X}_i\big) = e\big(Z, \hat{R}\big) \qquad \text{and} \tag{4}$$

$$e\big(R, \hat{G}\big) = e\big(G, \hat{R}\big)\ . \tag{5}$$

Correctness is immediate (cf. [FHS19]). While, so far, the scheme has only been proven secure in the generic group model, we will give a proof in the AGM.

Definition 4 (EQS-unforgeability in the AGM). *The algebraic unforgeability game* $\mathrm{UNF}^{\mathrm{AGM}}$ *is obtained from the UNF game from Definition 2 with the following changes: whenever the adversary* $\mathcal{A}$ *outputs an element* Y *of a group* $\mathbb{G}_t$*, for* $t \in \{1, 2\}$*, it also provides a* representation $\boldsymbol{\alpha}$ *s.t.* $Y = \sum \alpha_i Y_i$*, where* $\{Y_i\}$ *is the set of previously received elements from* $\mathbb{G}_t$.

The (q_1, q_2)-DL assumption [Lip12] in a bilinear group $grp = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G, \hat{G}, e)$ states that for a randomly sampled $y \leftarrow_\$ \mathbb{Z}_p$, no efficient adversary, that is given grp as well as $y^i G$ for $i \in [q_1]$ and $y^i\hat{G}$ for $i \in [q_2]$, can find y.

We introduce a variant of this assumption, where in addition to powers of the challenge value y^i (in the form $y^i G_t$), the adversary receives denominators $1/(y + c_i)$ for random known values c_i. This is reminiscent of the assumption corresponding to the *weakly secure* Boneh-Boyen signatures [BB04], which is implied by their *strong Diffie-Hellman* assumption. Analogously, we show that, under similar conditions, our assumption is implied by the standard (q_1, q_2)-DL assumption for appropriate q_1 and q_2.

Definition 5. *The* q***-PowDenDL assumption*** *holds with respect to* BGGen *if* $\mathsf{Adv}^{q\text{-PowDenDL}}_{\mathsf{BGGen},\mathcal{A}}(\lambda) := \Pr[q\text{-PowDenDL}_{\mathsf{BGGen},\mathcal{A}}(\lambda) = 1]$ *is negligible for all p.p.t. adversaries* $\mathcal{A}$*, where game* q-PowDenDL *is defined as follows:*

$q\text{-PowDenDL}_{\mathsf{BGGen},\mathcal{A}}(\lambda)$

$grp = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G, \hat{G}, e) \leftarrow \mathsf{BGGen}(1^\lambda)$

$y \leftarrow\!\!\$\ \mathbb{Z}_p\ ;\ (c_1, \dots, c_q) \leftarrow\!\!\$\ \mathbb{Z}_p^q$

$\texttt{if}\ (-y \bmod p) \in \{c_1, \dots, c_q\}\ \texttt{then return}\ 1$

$y' \leftarrow \mathcal{A}\Big(grp, \big(y^i G\big)_{i=1}^{2q}, y\hat{G}, \big(\tfrac{1}{y+c_i}G, \tfrac{1}{y+c_i}\hat{G}, c_i\big)_{i=1}^{q}\Big)$

$\texttt{return}\ y = y'$

We show that, assuming that BGGen returns random generators, q-PowDenDL is implied by (q_1, q_2)-DL for $q_1 := 3q$ and $q_2 := q{+}1$; we follow Boneh and Boyen's proof [BB04] (who for their scheme also assume that generators are randomly sampled).

Lemma 3. *Let* q *be arbitrary and* BGGen *be such that* G *and* $\hat{G}$ *are uniformly random. If* $(3q, q+1)$*-DL holds then* q*-PowDenDL holds; concretely, for every* $\mathcal{A}$ *there exists* $\mathcal{B}$ *with essentially the same running time such that*

$$\mathsf{Adv}^{(3q,q+1)\text{-DL}}_{\mathsf{BGGen},\mathcal{B}}(\lambda) \geq \mathsf{Adv}^{q\text{-PowDenDL}}_{\mathsf{BGGen},\mathcal{A}}(\lambda)\ .$$

Proof. Let $\mathcal{A}$ be an adversary against q-PowDenDL. We construct an adversary $\mathcal{B}$ against $(3q, q+1)$-DL. Let

$$\big(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G, \hat{G}, e, X^{(1)}, \dots, X^{(3q)}, \hat{X}^{(1)}, \dots, \hat{X}^{(q+1)}\big)$$

be an instance of $(3q, q+1)$-DL, that is, for some x, we have $X^{(i)} = x^i G$ and $\hat{X}^{(i)} = x^i \hat{G}$. Reduction $\mathcal{B}$ chooses $c_1, \dots, c_q \leftarrow\!\!\$\ \mathbb{Z}_p$; if for any $i \in [q] : -c_i G = X^{(1)}$ then $\mathcal{B}$ stops and returns $-c_i$.

Otherwise, $\mathcal{B}$ defines the polynomial

$$\prod_{j=1}^{q} (\mathrm{X} + c_j) = \sum_{j=0}^{q} \gamma_j \mathrm{X}^j =: \mathsf{P}(\mathrm{X})$$

for some $\gamma_0, \dots, \gamma_q \in \mathbb{Z}_p$. It defines new generators $H := \sum_{j=0}^{q} \gamma_j X^{(j)} = \big(\prod_{j=1}^{q}(x + c_j)\big)G$ and $\hat{H} := \sum_{j=0}^{q} \gamma_j \hat{X}^{(j)}$. If $H = 0_1$ then $\mathcal{B}$ factors $\mathsf{P}(\mathrm{X})$ and returns the root x that satisfies $xG = X^{(1)}$. Since G and $\hat{G}$ were uniform, so are H and $\hat{H}$. The reduction then completes a q-PowDenDL challenge

$$\big(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, H, \hat{H}, e, Y^{(1)}, \ldots, Y^{(2q)}, \hat{Y}^{(1)}, Y_1, \ldots, Y_q, \hat{Y}_1, \ldots, \hat{Y}_q, c_1, \ldots c_1\big)$$

for secret x as follows:

- for $i \in [2q]$: $Y^{(i)} := \sum_{j=0}^{q} \gamma_j X^{(j+i)} = \big(x^i \prod_{j=1}^{q}(x + c_j)\big)G = x^i H$; and analogously $\hat{Y}^{(1)} = \big(x \prod_{j=1}^{q}(x + c_j)\big)\hat{G} = x\hat{H}$;
- for $i \in [q]$: let $\delta_{i,j}$ be such that $\sum_{j=0}^{q-1} \delta_{i,j} \mathrm{X}^j = \prod_{j=1, j \neq i}^{q}(\mathrm{X} + c_j)$; set $Y_i := \sum_{j=0}^{q-1} \delta_{i,j} X^{(j)} = \big(\prod_{j=1,j\neq i}^{q}(x + c_j)\big)G = \frac{1}{x+c_i} H$ and, likewise, $\hat{Y}_i := \sum_{j=0}^{q-1} \delta_{i,j} \hat{X}^{(j)}$.

Reduction $\mathcal{B}$ runs $\mathcal{A}$ on the (correctly distributed) q-PowDenDL instance and forwards the solution x if $\mathcal{A}$ finds it. Whenever $\mathcal{A}$ finds it, $\mathcal{B}$ also solves its $(3q, q + 1)$-DL challenge. □

Theorem 1. *Let $q \in \mathbb{N}$ and let $\mathcal{A}$ be an algebraic adversary attacking* $\mathrm{UNF}^{\mathrm{AGM}}$ *of FHS that makes q signing queries. Then there exists a reduction $\mathcal{B}$ against q-PowDenDL for* BGGen *such that*

$$\mathsf{Adv}^{q\text{-PowDenDL}}_{\mathsf{BGGen},\mathcal{B}} \geq \mathsf{Adv}^{\mathrm{UNF}^{\mathrm{AGM}}}_{\mathrm{FHS},\mathcal{A}} - \frac{4q+1}{p-1}.$$

Proof Idea. We will construct a reduction that essentially views the discrete logarithm z of any group element Z as a polynomial $\mathsf{Z}(\mathrm{Y})$ in indeterminate Y, such that when evaluated on the solution y of the given q-PowDenDL challenge, we have $\mathsf{Z}(y) = z$. In particular, the reduction embeds y into the public key $\hat{\boldsymbol{X}}$ given to the adversary, as well as into the randomness r_i that is sampled for the i-th signing query.

In order to guarantee independence of the adversary's behavior from y, we hide y by both multiplying with and adding a uniform element from $\mathbb{Z}_p$. In particular, components of the secret key will have the form $x_j y + x'_j$ for random x_j, x'_j. This ensures that even an unbounded adversary that can compute discrete logarithms is unable to reason about y, since it is information-theoretically hidden (the values x_j and x'_j are not used anywhere else). Using the element $\hat{Y}^{(1)} = y\hat{G}$ from its q-PowDenDL instance, the reduction can compute the public key elements $\hat{X}_j = x_j \hat{Y}^{(1)} + x'_j \hat{G}$.

Analogously, y will be embedded into the randomness r_i of each signing query. We now show how the reduction answers its i-th signing query. Let $(Z_k, R_k, \hat{R}_k)$, $k < i$, be the signatures given to the adversary $\mathcal{A}$ so far, for which the reduction knows the polynomials representing their discrete logarithms. When $\mathcal{A}$ queries the signing oracle on a message $\boldsymbol{M}$, since $\mathcal{A}$ is algebraic, it accompanies each M_j with a representation $(\mu^{(j)}, \mu^{(j)}_{z,1}, \ldots, \mu^{(j)}_{z,i-1}, \mu^{(j)}_{r,1}, \ldots, \mu^{(j)}_{r,i-1})$ such that

$$M_j := \mu^{(j)} G + \sum_{k=1}^{i-1} \mu^{(j)}_{z,k} Z_k + \sum_{k=1}^{i-1} \mu^{(j)}_{r,k} R_k \ , \tag{6}$$

since $G, Z_1, \dots, Z_{i-1}, R_1, \dots, R_{i-1}$ are all the $\mathbb{G}_1$ elements that $\mathcal{A}$ has seen so far. As the reduction knows the polynomials associated to these group elements, from (6) it can compute the polynomial associated to M_j, and, from this, the polynomial associated to the signature element $Z = r \sum (x_i y + x'_i) M_i$. Even though the reduction does not know y, it can evaluate these polynomials on y "in the exponent" by performing group operations in $\mathbb{G}_1$ on the elements given in the q-PowDenDL challenge and thereby compute Z (and analogously R and $\hat{R}$).

Once the adversary submits its forgery $(Z, R, \hat{R}), M$, the reduction considers the two EQS verification equations (4) and (5) "in the exponent", and represents them in the "homogenious" form $e(R, \hat{G}) - e(G, \hat{R}) = 0$ (for (5)). The algebraic adversary $\mathcal{A}$ accompanies its forgery with representations, from which the reduction can compute the polynomials associated to each element. Plugging these into the verification equations, $\mathcal{B}$ computes two "verification polynomials" Q_1 and Q_2, which evaluate to 0 at y if and only if $\mathcal{A}$'s forgery satisfies the corresponding equation.

If the adversary succeeds, there are two cases: (1) At least one of the verification polynomials is not the zero polynomial: $\mathsf{Q}_i \not\equiv 0$. Then the q-PowDenDL solution y is a root of Q_i. By factoring Q_i, we therefore obtain the solution y. (2) Both polynomials are identically zero: we show that in this case the message on which the adversary provided a forgery was in fact a multiple of a previously asked query. This contradicts that the adversary wins the game. This will be accomplished by reasoning about the coefficients that the algebraic adversary provides by equating coefficients of the verification polynomial.

Proof. Consider the $\mathrm{UNF}^{\mathrm{AGM}}$ game instantiated with FHS as shown in Figure 2. (We omit the group elements from $\mathcal{A}$'s outputs, since they are determined by their representations.) We follow the convention that for an uppercase Latin letter A the coefficients will be represented by its greek lowercase analog α, where subscripts like $\alpha_{z,k}$ are to be read as "the coefficient that gets multiplied with Z_k". The elements Z_i, R_i and $\hat{R}_i$ are the answers to the i-th signing query. For example, the element Z is represented by the coefficients $\zeta, \zeta_{z,k}$ and $\zeta_{r,k}$ for $k \in [q]$, as can be seen in Figure 2 on Line 7.

We will construct a reduction $\mathcal{B}$ in Figure 3 that breaks q-PowDenDL using an algebraic adversary $\mathcal{A}$ against $\mathrm{UNF}^{\mathrm{AGM}}$ that makes up to q queries to the signing oracle. The reduction works as follows: it gets the q-PowDenDL challenge

$$\left(Y^{(i)}\right)_{i=1}^{2q}, \hat{Y}^{(1)}, \left(Y_i, \hat{Y}_i, c_i\right)_{i=1}^{q}$$

with the aim of computing the discrete logarithm y of $Y^{(1)}$. For the sake of convenience define $Y^{(0)} := G$. Sampling uniform vectors $\boldsymbol{x}, \boldsymbol{x}'$ the reduction embeds y into the secret key by setting the public key elements $\hat{X}_j := x_j \hat{Y}^{(1)} + x'_j \hat{G}$. If for any j we have $\hat{X}_j = 0_2$ then $\mathcal{B}$ stops and returns $y = -x_j^{-1} x'_j \mod p$. Note that the public key elements are distributed correctly, since the reduction $\mathcal{B}$ essentially implements rejection sampling. The secret key elements, which correspond to the discrete logarithm of the public key, are thus of the form $x_j y + x'_j$.

$\mathrm{UNF}^{\mathrm{AGM}}_{\mathrm{FHS},\mathcal{A}}(\lambda)$

$grp \leftarrow \mathsf{ParGen}(1^\lambda)$

$(sk, pk := \hat{\boldsymbol{X}}) \leftarrow \mathsf{KeyGen}(grp, 1^\ell)$

$Q := \emptyset$

$\Big(\big(\mu^{(j)}, \big(\mu^{(j)}_{z,k}\big)_{k=1}^{q}, \big(\mu^{(j)}_{r,k}\big)_{k=1}^{q}\big)_{j=1}^{\ell},$
$\big(\zeta, \big(\zeta_{z,k}\big)_{k=1}^{q}, \big(\zeta_{r,k}\big)_{k=1}^{q}\big), \big(\rho, \big(\rho_{z,k}\big)_{k=1}^{q}, \big(\rho_{r,k}\big)_{k=1}^{q}\big),$
$\big(\hat{\rho}, \big(\hat{\rho}_{x,k}\big)_{k=1}^{\ell}, \big(\hat{\rho}_{r,k}\big)_{k=1}^{q}\big)\Big) \leftarrow \mathcal{A}^{\mathcal{O}}(grp, pk)$

`For` $j \in [\ell] : M^*_j := \mu^{(j)} G + \sum_{k=1}^{q} \mu^{(j)}_{z,k} Z_k + \sum_{k=1}^{q} \mu^{(j)}_{r,k} R_k$

`if` $\boldsymbol{M}^* \in Q :$ `return` 0

$Z := \zeta G + \sum_{k=1}^{q} \zeta_{z,k} Z_k + \sum_{k=1}^{q} \zeta_{r,k} R_k$

$R := \rho G + \sum_{k=1}^{q} \rho_{z,k} Z_k + \sum_{k=1}^{q} \rho_{r,k} R_k$

$\hat{R} := \hat{\rho}\hat{G} + \sum_{k=1}^{\ell} \hat{\rho}_{x,k} \hat{X}_k + \sum_{k=1}^{q} \hat{\rho}_{r,k} \hat{R}_k$

`return` $\sum_j e(M_j, \hat{X}_j) = e(Z, \hat{R}) \ \wedge\ e(R, \hat{G}) = e(G, \hat{R})$

$\mathcal{O}\Big(\Big(\mu^{(i,j)}, \big(\mu^{(i,j)}_{z,k}\big)_{k=1}^{i-1}, \big(\mu^{(i,j)}_{r,k}\big)_{k=1}^{i-1}\Big)_{j=1}^{\ell}\Big)$ // the i-th query

`For` $j \in [\ell] : M_j := \mu^{(i,j)} G + \sum_{k=1}^{i-1} \mu^{(i,j)}_{z,k} Z_k + \sum_{k=1}^{i-1} \mu^{(i,j)}_{r,k} R_k$

$Q := Q \cup [(M_j)_j]_\sim$

$r \leftarrow\!\!\$\ \mathbb{Z}_p^*$

`return` $\Big(Z_i := r \sum_j x_j M_j, R_i := \frac{1}{r} G, \hat{R}_i := \frac{1}{r}\hat{G}\Big)$

Fig. 2. The game $\mathrm{UNF}^{\mathrm{AGM}}$ for the EQS scheme FHS.

The reduction can therefore, without knowing y, evaluate a polynomial at y "in the exponent" by using the elements of the q-PowDenDL challenge. These polynomials will be represented in sans-serif font, e.g. M_j, and their indeterminates in Roman font, e.g. Y.

The vectors $\boldsymbol{x}$ and $\boldsymbol{x}'$ are required so the adversary's behavior is independent of y. Even if it is unbounded and is able to obtain discrete logarithms of elements, since y is hidden information-theoretically, it cannot reason about y. Similarly, y is embedded in the randomness r that gets introduced during a signing query. The signing randomness will be of the form as $r_i(y + c_i)$ where r_i gets drawn uniformly and c_i is part of the q-PowDenDL challenge. Due to the randomness r appearing both as r and its reciprocal $\frac{1}{r}$, the reduction will in fact consider Laurent polynomials. The elements Y_i and $\hat{Y}_i$ from its challenge enable the reduction to also evaluate (very specific) Laurent polynomials "in the exponent" at y and compute corresponding group elements. Since y is embedded in both the secret key and the signature randomness, the reduction considers *multivariate* Laurent polynomials in indeterminates $\mathbf{X}$ and $\mathbf{R}$, which models the adversary's view more closely and simplifies our reasoning. Only at a later stage these multivariate Laurent polynomials will be transformed into univariate polynomials in Y.

When $\mathcal{A}$ makes the i-th signing query, for $j \in [\ell]$ the reduction will receive coefficients

$$\mu^{(i,j)}, \big(\mu_{z,k}^{(i,j)}\big)_{k=1}^{i-1}, \big(\mu_{r,k}^{(i,j)}\big)_{k=1}^{i-1}$$

that represent the j-th component of the queried message

$$M_j := \mu^{(i,j)} G + \sum_{k=1}^{i-1} \mu_{z,k}^{(i,j)} Z_k + \sum_{k=1}^{i-1} \mu_{r,k}^{(i,j)} R_k.$$

Since Z_k and R_k were the answers to previous signing queries, the reduction has Laurent polynomials that represent their respective logarithms. This fact will be used to find a Laurent polynomial that represents the logarithm of the answer to the i-th query Z_i. The following lemma will give a detailed description on how the reduction answers the adversaries signing queries.

Lemma 4. *There exist coefficients $a_k^{(i)}$, $k \in \{0, \ldots, 2i\}$, and $b_k^{(i)}$, $k \in [i-1]$, such that the polynomial Z_i representing the signature element Z_i from the i-th signing query is of the form*

$$\mathsf{Z}_i(\mathrm{Y}) = \sum_{k=0}^{2i} a_k^{(i)} \mathrm{Y}^k + \sum_{k=1}^{i-1} b_k^{(i)} \frac{1}{r_k(\mathrm{Y} + c_k)}.$$

Moreover $\mathcal{B}$ can compute these coefficients efficiently.

Proof. We will prove this by induction on the signing queries. Consider $i = 1$, the first signing query. As the previously seen $\mathbb{G}_1$ element is G, for the message we have $M_j^{(1)} = \mu^{(1,j)} G$ for some $\mu^{(1,j)}$, which we represent as a polynomial

$\mathcal{B}^{\mathcal{A}}\Big(grp, \big(Y^{(i)}\big)_{i=1}^{2q}, \hat{Y}^{(1)}, \big(Y_i, \hat{Y}_i, c_i\big)_{i=1}^{q}\Big)$

$r_1, \ldots, r_q, x_1, \ldots, x_\ell \leftarrow\!\!\$\ \mathbb{Z}_p^*; x_1', \ldots, x_\ell' \leftarrow\!\!\$\ \mathbb{Z}_p$

$pk := \Big(x_1 \hat{Y}^{(1)} + x_1'\hat{G}, \ldots, x_\ell \hat{Y}^{(1)} + x_\ell'\hat{G}\Big)$

$\texttt{if } \exists j \texttt{ s.t. } x_j\hat{Y}^{(1)} + x_j'\hat{G} = 0 : \texttt{return } y := -x_j^{-1}x_j' \mod p$

$$\Big(\Big(\mu^{(j)}, \big(\mu_{z,k}^{(j)}\big)_{k=1}^{q}, \big(\mu_{r,k}^{(j)}\big)_{k=1}^{q}\Big)_{j=1}^{\ell}, \Big(\big(\zeta, (\zeta_{z,k})_{k=1}^q, (\zeta_{r,k})_{k=1}^q\big), \big(\rho, (\rho_{z,k})_{k=1}^q, (\rho_{r,k})_{k=1}^q\big), \big(\hat{\rho}, (\hat{\rho}_{x,k})_{k=1}^{\ell}, (\hat{\rho}_{r,k})_{k=1}^q\big)\Big)\Big) \leftarrow \mathcal{A}^{\mathtt{OSign}}(grp, pk)$$

$$\texttt{For } j \in [\ell] : \mathsf{M}_j(\mathbf{X}, \mathbf{R}) := \mu^{(j)} + \sum_{k=1}^{q} \mu_{z,k}^{(j)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k=1}^{q} \mu_{r,k}^{(j)} \mathrm{R}_k^{-1}$$

$$\mathsf{R}(\mathbf{X}, \mathbf{R}) := \rho + \sum_{k=1}^{q} \rho_{z,k} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k=1}^{q} \rho_{r,k} \mathrm{R}_k^{-1}$$

$$\hat{\mathsf{R}}(\mathbf{X}, \mathbf{R}) := \hat{\rho} + \sum_{k=1}^{\ell} \hat{\rho}_{x,k} \mathrm{X}_k + \sum_{k=1}^{q} \hat{\rho}_{r,k} \mathrm{R}_k^{-1}$$

$$\mathsf{V}_1 := \Big(\prod_{i=1}^{q} \mathrm{R_i}\Big)\Big(\mathsf{R}(\mathbf{X}, \mathbf{R}) - \hat{\mathsf{R}}(\mathbf{X}, \mathbf{R})\Big)$$

$$\mathsf{V}_2 := \Big(\prod_{i=1}^{q} \mathrm{R}_i^2\Big)\Big(\Big(\sum_{j=1}^{\ell} \mathrm{X_j}\mathsf{M_j}\Big) - \hat{\mathsf{R}}(\mathbf{X}, \mathbf{R})\Big(\zeta + \sum_{k=1}^{q} \zeta_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k=1}^{q} \zeta_{r,k}\mathrm{R}_k^{-1}\Big)\Big)$$

$$\texttt{For } t \in [2] : \mathsf{Q}_t := \mathsf{V}_t\Big(\big(x_i\mathrm{Y} + x_i'\big)_{i=1}^{\ell}, \big(r_i\,(\mathrm{Y} + c_i)\big)_{i=1}^{q}\Big)$$

$S := \emptyset; \quad \texttt{if } \mathsf{Q}_1 \not\equiv 0 : S := S \cup \mathsf{Roots}(\mathsf{Q}_1); \quad \texttt{if } \mathsf{Q}_2 \not\equiv 0 : S := S \cup \mathsf{Roots}(\mathsf{Q}_2)$

$\texttt{if } \exists y \in S \texttt{ s.t. } yG = Y^{(1)} : \texttt{return } y$

$\mathtt{OSign}\Big(\Big(\mu^{(i,j)}, \big(\mu_{z,k}^{(i,j)}\big)_{k=1}^{i-1}, \big(\mu_{r,k}^{(i,j)}\big)_{k=1}^{i-1}\Big)_{j=1}^{\ell}\Big)$ // describing the i-th signing query

---

$$\texttt{For } j \in [\ell] : \quad \mathsf{M}_j^{(i)}(\mathbf{X}, \mathbf{R}) := \mu^{(i,j)} + \sum_{k=1}^{i-1} \mu_{z,k}^{(i,j)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k=1}^{i-1} \mu_{r,k}^{(i,j)} \mathrm{R}_k^{-1}$$

$$\mathsf{Z}_i(\mathbf{X}, \mathbf{R}) := \mathrm{R}_i \sum_{j=1}^{\ell} \mathrm{X}_j \mathsf{M}_j^{(i)}(\mathbf{X}, \mathbf{R})$$

$$\texttt{Parse } \mathsf{Z}_i\Big(\big(x_j\mathrm{Y} + x_j'\big)_{j=1}^{\ell}, \big(r_j\,(\mathrm{Y} + c_j)\big)_{j=1}^{i-1}\Big) \texttt{ as } \mathsf{Z}_i = \sum_{j=0}^{2i} a_j^{(i)} \mathrm{Y}^i + \sum_{j=1}^{i-1} b_j^{(i)} \frac{1}{r_j(\mathrm{Y} + c_j)}$$

$$Z_i := \sum_{j=0}^{2i} a_j^{(i)} Y^{(i)} + \sum_{j=1}^{i-1} b_j^{(i)} Y_j$$

$$\texttt{return } \Big(Z_i, R_i := \tfrac{1}{r_i} Y_i, \hat{R}_i := \tfrac{1}{r_i} \hat{Y}_i\Big)$$

Fig. 3. Reduction from FHS unforgeability in the AGM to q-PowDenDL

$\mathsf{M}_j^{(1)} = \mu^{(1,j)}$ for $j \in [\ell]$. Therefore the reduction will consider the Laurent polynomial

$$\mathsf{Z}_1(\mathbf{X}, \mathbf{R}) = \mathrm{R}_1 \sum_{j=1}^{\ell} \mu^{(1,j)} \mathrm{X}_j$$

evaluated on $\mathrm{X}_j = x_j \mathrm{Y} + x'_j$ for $j \in [\ell]$ and $\mathrm{R}_1 = r_1(\mathrm{Y} + c_1)$, which can be parsed as (recall that $\odot$ denotes componentwise multiplication)

$$\begin{aligned}
\mathsf{Z}_1(\boldsymbol{x}\mathrm{Y} + \boldsymbol{x}', \boldsymbol{r}\mathrm{Y} + \boldsymbol{r} \odot \boldsymbol{c}) &= r_1(\mathrm{Y} + c_1) \sum_j \mu^{(1,j)}(x_j \mathrm{Y} + x'_j) \\
&= \mathrm{Y}^2 \sum_j \mu^{(1,j)} r_1 x_j + \mathrm{Y} \sum_j \mu^{(1,j)} r_1 \left(x_j c_1 + x'_j\right) + \sum_j \mu^{(1,j)} r_1 c_1 x'_j \\
&= \sum_{k=0}^{2} a_k^{(1)} \mathrm{Y}^k,
\end{aligned}$$

for appropriate coefficients $a_k^{(1)}$. Observe that $\deg_{\mathrm{Y}} \mathsf{Z}_1 \leq 2$. The reduction then sends the group elements $Z_1 := \sum_{k=0}^{2} a_k^{(1)} Y^{(k)}$ and $R_1 := \frac{1}{r_1} Y_1 = \frac{1}{r_1(y+c_1)} G$ and $\hat{R}_1 := \frac{1}{r_1} \hat{Y}_1$ answering the query. Note that the fractional part of Z_1 being zero is in accordance with the statement of this lemma, since $\sum_{k=1}^{0} b_k^{(1)} (r_k(\mathrm{Y} + c_k))^{-1} = 0$ holds for the empty sum.

Now consider the i-th query, after the reduction has answered all queries $k < i$ represented by polynomials Z_k for which $\deg_{\mathrm{Y}} \mathsf{Z}_k \leq 2k$ holds. The previously seen $\mathbb{G}_1$ elements additionally contain Z_k and R_k for $k < i$, therefore the message is provided with coefficients such that for $j \in [\ell]$ its polynomial representation is

$$\mathsf{M}_j^{(i)} = \mu^{(i,j)} + \sum_{k}^{i-1} \mu_{z,k}^{(i,j)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k}^{i-1} \mu_{r,k}^{(i,j)} \mathrm{R}_k^{-1}.$$

The reduction then considers the Laurent polynomial

$$\mathsf{Z}_i(\mathbf{X}, \mathbf{R}) = \mathrm{R}_i \sum_j \mathrm{X}_j \left(\mu^{(i,j)} + \sum_{k}^{i-1} \mu_{z,k}^{(i,j)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k}^{i-1} \mu_{r,k}^{(i,j)} \mathrm{R}_k^{-1} \right)$$

and evaluates it on $\mathrm{X}_j = x_j \mathrm{Y} + x'_j$ for $j \in [\ell]$ and $\mathrm{R}_i = r_i(\mathrm{Y} + c_i)$ for $i \in [q]$. By the induction hypothesis we know that for $k < i$ there exist coefficients $a_j^{(k)}$ and $b_j^{(k)}$ such that

$$\mathsf{Z}_k(\boldsymbol{x}\mathrm{Y} + \boldsymbol{x}', \boldsymbol{r}\mathrm{Y} + \boldsymbol{r} \odot \boldsymbol{c}) = \sum_{j=0}^{2k} a_j^{(k)} \mathrm{Y}^j + \sum_{j=1}^{k-1} b_j^{(k)} \frac{1}{r_j(\mathrm{Y} + c_j)}.$$

The reduction now considers $\mathsf{Z}_i(\boldsymbol{x}\mathrm{Y} + \boldsymbol{x}', \boldsymbol{r}\mathrm{Y} + \boldsymbol{r} \odot \boldsymbol{c}) = \mathsf{P}(\mathrm{Y}) + \mathsf{F}(\mathrm{Y})$ where P denotes the polynomial part, while F denotes the fractional part of Z_i. The polynomial part can be parsed as

$$\mathsf{P}(\mathrm{Y}) = r_i(\mathrm{Y}+c_i)\sum_j (x_j\mathrm{Y}+x'_j)\left(\mu^{(i,j)} + \sum_k^{i-1}\mu_{z,k}^{(i,j)}\sum_{j=0}^{2k} a_j^{(k)}\mathrm{Y}^j\right) = \sum_{j=0}^{2i} p_j\mathrm{Y}^j,$$

for appropriate coefficients p_j. For the fractional part

$$\begin{aligned}\mathsf{F}(\mathrm{Y}) = r_i(\mathrm{Y}+c_i)\sum_j (x_j\mathrm{Y}+x'_j)\Bigg(&\sum_k^{i-1}\mu_{z,k}^{(i,j)}\sum_m^{k-1} b_m^{(k)}\frac{1}{r_m(\mathrm{Y}+c_m)}\\ &+\sum_k^{i-1}\mu_{r,k}^{(i,j)}\frac{1}{r_k(\mathrm{Y}+c_k)}\Bigg),\end{aligned}$$

the reduction can find coefficients f_j for $j \in \{1, 0, \ldots, -i+1\}$ via partial fraction decomposition such that

$$\mathsf{F}(\mathrm{Y}) = f_1\mathrm{Y} + f_0 + \sum_{j=1}^{i-1} f_{-j}\frac{1}{r_j(\mathrm{Y}+c_j)}.$$

Therefore

$$\begin{aligned}\mathsf{Z}_i(\boldsymbol{x}\mathrm{Y}+\boldsymbol{x}', \boldsymbol{r}\mathrm{Y}+\boldsymbol{r}\odot\boldsymbol{c}) &= \mathsf{P}(\mathrm{Y}) + \mathsf{F}(\mathrm{Y})\\ &= \sum_{j=0}^{2i} p_j\mathrm{Y}^j + f_1\mathrm{Y} + f_0 + \sum_{j=1}^{i-1} f_{-j}\frac{1}{r_j(\mathrm{Y}+c_j)}\\ &= \sum_{j=0}^{2i} a_j^{(i)}\mathrm{Y}^j + \sum_{j=1}^{i-1} b_j^{(i)}\frac{1}{r_j(\mathrm{Y}+c_j)},\end{aligned}$$

for appropriate $a_j^{(i)}$, $b_j^{(i)}$. The reduction answers the signing query with $Z_i := \sum_{j=0}^{2i} a_j^{(i)}Y^{(j)} + \sum_{j=1}^{i-1} b_j^{(i)}Y_j$ and $R_i := \frac{1}{r_i}Y_i$ and $\hat{R}_i := \frac{1}{r_i}\hat{Y}_i$. Note that since

$$\begin{aligned}Z_i &= \sum_{j=0}^{2i} a_j^{(i)}Y^{(j)} + \sum_{j=1}^{i-1} b_j^{(i)}Y_j\\ &= \mathsf{Z}_i(\boldsymbol{x}y+\boldsymbol{x}', \boldsymbol{r}y+\boldsymbol{r}\odot\boldsymbol{c})G\\ &= (r_iy + r_ic_i)\sum_j M_j^{(i)}(x_jy+x'_j)\\ &= \tilde{r}\sum_j \tilde{x}_jM_j^{(i)},\end{aligned}$$

with $\tilde{r}$ being uniform in $\mathbb{Z}_p^*$, $\tilde{x}_j$ being consistent with $\hat{\boldsymbol{X}}$, and $R_i = \frac{1}{\tilde{r}}G$, the signatures are distributed identically to signatures from FHS. □

Since the q-PowDenDL challenge contains "powers" up to $2q$ and q different "denominators" we obtain the following corollary.

Corollary 1. *Using the q-PowDenDL challenge, the reduction can answer q queries to the signing oracle.*

The following observation directly follows from the definition of Z_i, and noting that there do not exist reciprocal terms in $\mathbf{X}$ in any of the Laurent polynomials that we consider.

Remark 1. Let $i \in [q]$. Then for every monomial m of Z_i there exists a $j \in [q]$ such that X_j divides m.

At some point the adversary $\mathcal{A}$ will output coefficients that represent a forgery consisting of a message $\boldsymbol{M}$ and the signature $(Z, R, \hat{R})$. Figure 2 describes how these coefficients relate to the elements. $\mathcal{B}$ then defines polynomials V_1 and V_2 that correspond to the two verification equations in the $\mathrm{UNF}^{\mathrm{AGM}}$ game. If the verification equation (5) $e(G, \hat{R}) = e(R, \hat{G})$ holds, then the logarithms of R and $\hat{R}$ are equivalent. Therefore the polynomial V_1 has y as a zero if R and $\hat{R}$ satisfy that verification equation of the game.

Recall the definitions of the Laurent polynomials (Figure 3, lines 5 and 6):

$$\mathsf{R}(\mathbf{X}, \mathbf{R}) := \rho + \sum_{k=1}^{q} \rho_{z,k} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{k=1}^{q} \rho_{r,k} \mathrm{R}_k^{-1}$$

$$\hat{\mathsf{R}}(\mathbf{X}, \mathbf{R}) := \hat{\rho} + \sum_{k=1}^{\ell} \hat{\rho}_{x,k} \mathrm{X}_k + \sum_{k=1}^{q} \hat{\rho}_{r,k} \mathrm{R}_k^{-1},$$

clearly, $\hat{\mathsf{R}}$ has denominators of maximum degree 1. Recall also that every Laurent polynomial we consider only has reciprocal terms in $\mathbf{R}$. Consider how Z_i is formed inductively, then Z_1 does not have any reciprocal terms (and insofar denominators with a maximum degree of 1), while when Z_i is formed from the previous Z_k for $k < i$, there might be reciprocal terms of degree 1 that are added. Therefore Z_i only has denominators with a maximum degree of 1, and so R only has denominators with a maximum degree of 1. Therefore, the factor $\prod_i \mathrm{R_i}$ ensures that V_1 is a polynomial.

Analogously, V_2 has y as a root if and only if the verification equation (4) $\sum_j e(M_j, \hat{X}_j) = e(Z, \hat{R})$ holds. Since multiplying $\hat{\mathsf{R}}$ by R_k^{-1} potentially contained in the polynomial associated with Z creates denominators of degree 2, the factor $\prod_i \mathrm{R}_i^2$ ensures that V_2 is a polynomial. Observing that $\mathsf{Z_k}$ has a total degree upper-bounded by $2k$, the following corollary summarizes this argument.

Corollary 2. *Both* V_1 *and* V_2 *are polynomials of total degree upper-bounded by* $4q + 1$.

The following convention will simplify the remainder of the proof.

Remark 2. Since for fixed k the coefficient $\zeta_{z,k}$ only occurs as a factor of Z_k, whenever $\mathsf{Z}_k \equiv 0$ the adversary $\mathcal{A}$ can choose $\zeta_{z,k}$ arbitrarily. Since this choice does not change the system of equations, the reduction will set $\zeta_{z,k} := 0$ whenever $\mathsf{Z}_k \equiv 0$.

Note that this remark is not limited to $\zeta_{z,k}$ but also applies to other coefficients for example $\rho_{z,k}$ among others.

We will briefly discuss the technique used in the following proofs. Recall that if $\mathcal{R}$ is a ring, then an ideal $\mathfrak{I}$ is an additive subgroup of $\mathcal{R}$ such that for $\mathsf{P} \in \mathcal{R}$ and $\mathsf{Q} \in \mathfrak{I}$ it holds that $\mathsf{PQ} \in \mathfrak{I} \ni \mathsf{QP}$. For a subset S of $\mathcal{R}$, the ideal *generated by* S is defined as the smallest ideal $\mathfrak{I}$ such that $S \subseteq \mathfrak{I}$. If $\mathfrak{I}$ is an ideal then $\mathcal{R}/\mathfrak{I}$ is a ring, the so-called quotient ring or factor ring. Conceptually, the ideal "defines" which elements we identify with 0 in the quotient ring. Since we consider $\mathsf{V}_1 \equiv 0$, that is, for all inputs it vanishes, viewing this equation in the quotient ring corresponds to fixing specific terms (the ones in the ideal) to zero. This greatly simplifies notation when we equate coefficients of polynomials.

The following lemma states that given polynomials P_j in $\mathbf{X}$ such that (7) holds, then all P_j must vanish. Since we will apply this lemma to polynomials P_j of degree less than two, this means that they must be the zero polynomial. Equations of the form (7) emerge in the proof by considering $\mathsf{V}_t \equiv 0$, for $t \in [2]$, in an appropriate quotient ring. Remark 2 motivates that we merely need to consider the non-zero polynomials Z_j.

Lemma 5. *Let $J := \{j \mid \mathsf{Z}_j \not\equiv 0\} \subseteq [q]$ be the set of indices such that Z_j is a non-zero Laurent polynomial, and for $j \in J$ let $\mathsf{P}_j \in \mathbb{Z}_p[\mathbf{X}]$ be arbitrary polynomials. Then whenever*

$$\Big(\prod_k \mathrm{R}_k\Big) \sum_{j \in J} \mathsf{P}_j \mathsf{Z}_j \equiv 0, \tag{7}$$

as a polynomial in $\mathbf{X}$ and $\mathbf{R}$, we have $\mathsf{P}_j \equiv 0$ for all $j \in J$.

Proof. For $j \in J$ let $\mathfrak{K}_j$ be the ideal generated by $\{\mathrm{R}_i^2 \mid j < i \leq q\}$. We will consider equations in the factor rings $\mathbb{Z}_p[\mathbf{X}, \mathbf{R}]/\mathfrak{K}_j$, where we will denote equality by $\equiv_{\mathfrak{K}_j}$.

We will prove the claim inductively on the size of J. Assume $J \neq \emptyset$ and let $j := \min J$. Consider (7) modulo $\mathfrak{K}_j$. Since R_i divides Z_i, and thus R_i^2 divides $\big(\prod_k \mathrm{R}_k\big)\mathsf{Z}_i$, all the summands $\mathsf{P}_i\mathsf{Z}_i$ for $i > j$ vanish:

$$\Big(\prod_k \mathrm{R}_k\Big)\mathsf{P}_j\mathsf{Z}_j \equiv_{\mathfrak{K}_j} 0. \tag{8}$$

Now since $\mathsf{Z}_j \not\equiv 0$, and Z_j does not contain any R_i for $i > j$, we get

$$\deg_{\mathrm{R}_i} \Big(\prod_k \mathrm{R}_k\Big)\mathsf{Z}_j = 1.$$

Since P_j does not depend on $\mathbf{R}$, the only way that the left-hand side of (8) always vanishes is for $\mathsf{P}_j \equiv 0$. Considering $J' := J \setminus \{j\}$ we can inductively apply this reasoning eventually yielding the statement. $\square$

We will now consider what it means if either verification polynomial V_t is the zero polynomial. This essentially models an adversary that tries to "outsmart" the reduction, by choosing coefficients in a way such that the polynomials V_1 and V_2 leak no information about y. In particular, if $\mathsf{V}_1 \equiv 0$ then $\mathcal{A}$ was (partly) successful in forging a signature but our reduction cannot obtain the q-PowDenDL solution y from the corresponding equation. The following lemma captures that the only way for $\mathcal{A}$ to enforce $\mathsf{V}_1 \equiv 0$ is to respresent both R and $\hat{\mathsf{R}}$ by the same coefficients.

Lemma 6. *If $\mathsf{V}_1 \equiv 0$, then the following holds for the coefficients of R and $\hat{\mathsf{R}}$:*

$$\begin{aligned} \rho &= \hat{\rho}, \\ \rho_{z,j} &= \hat{\rho}_{x,j} = 0 \quad \forall j \in [q], \\ \rho_{r,j} &= \hat{\rho}_{r,j} \qquad\quad \forall j \in [q]. \end{aligned}$$

Proof. Let $j \in [q]$ and let $\mathfrak{J}$ denote the ideal generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell, \mathrm{R}_j\}$. We will look at V_1 in the quotient ring $\mathbb{Z}_p[\mathbf{X}, \mathbf{R}]/\mathfrak{J}$. By $\equiv_{\mathfrak{J}}$ we denote equivalence in the quotient ring. Recall that

$$\begin{aligned} \mathsf{V}_1(\mathbf{X}, \mathbf{R}) &= \Big(\prod_i \mathrm{R}_i\Big)\Big(\mathsf{R}(\mathbf{X}, \mathbf{R}) - \hat{\mathsf{R}}(\mathbf{X}, \mathbf{R})\Big) \\ &= \Big(\prod_i \mathrm{R}_i\Big)\Big(\rho + \sum_k \rho_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_k \rho_{r,k}\mathrm{R}_k^{-1} \\ &\qquad\qquad - \hat{\rho} - \sum_k \hat{\rho}_{x,k}\mathrm{X}_k - \sum_k \hat{\rho}_{r,k}\mathrm{R}_k^{-1}\Big). \end{aligned}$$

Now since $\rho \prod_i \mathrm{R}_i \equiv_{\mathfrak{J}} 0$ and $\hat{\rho} \prod_i \mathrm{R}_i \equiv_{\mathfrak{J}} 0$, and all monomials of Z_k contain some X_j (as noted in Remark 1), which implies $\mathsf{Z}_k = \mathrm{R}_k \sum_j \mathrm{X}_j \mathsf{M}_j^{(k)} \equiv_{\mathfrak{J}} 0$, we get

$$\begin{aligned} 0 \equiv \mathsf{V}_1(\mathbf{X}, \mathbf{R}) &\equiv_{\mathfrak{J}} \Big(\prod_i \mathrm{R}_i\Big)\Big(\sum_k (\rho_{r,k} - \hat{\rho}_{r,k})\mathrm{R}_k^{-1}\Big) \\ &\equiv_{\mathfrak{J}} \big(\prod_{i \neq j} \mathrm{R}_i\big)(\rho_{r,j} - \hat{\rho}_{r,j}), \end{aligned}$$

where the second equivalence follows from $\mathrm{R}_j \equiv_{\mathfrak{J}} 0$. Equating coefficients yields $\rho_{r,j} = \hat{\rho}_{r,j}$. As j was arbitrary, this result holds for every $j \in [q]$.

Since $\mathsf{V}_1 \equiv 0$ implies that $\mathsf{V}_1 / \prod_i \mathrm{R}_i \equiv 0$ where it is defined, viewing this equation in the factor ring obtained by factoring the ideal $\mathfrak{X}$ generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell\}$ and using what we deduced about $\rho_{r,j}$ and $\hat{\rho}_{r,j}$ we get

$$\begin{aligned} \frac{\mathsf{V}_1(\mathbf{X}, \mathbf{R})}{\prod_i \mathrm{R}_i} &\equiv \rho - \hat{\rho} + \sum_k \rho_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}) - \sum_k \hat{\rho}_{x,k}\mathrm{X}_k \\ &\equiv_{\mathfrak{X}} \rho - \hat{\rho}, \end{aligned}$$

where by Remark 1 we have $\mathsf{Z}_k = \mathrm{R}_k \sum_j \mathrm{X}_j \mathsf{M}_j^{(k)} \equiv_{\mathfrak{X}} 0$. We thus obtain $\rho = \hat{\rho}$.

Now consider the ideal $\mathfrak{R}$ generated by $\{\mathrm{R}_1, \ldots, \mathrm{R}_q\}$. Together with what we deduced so far we have

$$0 \equiv \frac{\mathsf{V}_1(\mathbf{X}, \mathbf{R})}{\prod_i \mathrm{R}_i} \equiv \sum_k \rho_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}) - \sum_k \hat{\rho}_{x,k}\mathrm{X}_k$$

$$
\begin{aligned}
&\equiv \sum_k \rho_{z,k} \mathrm{R}_k \sum_j \mathrm{X}_j \mathsf{M}_j^{(k)}(\mathbf{X}, \mathbf{R}) - \sum_k \hat{\rho}_{x,k} \mathrm{X}_k \\
&\equiv_{\mathfrak{R}} - \sum_k \hat{\rho}_{x,k} \mathrm{X}_k,
\end{aligned}
$$

where we used that $\mathrm{M}_j^{(k)}$ only depends on R_i for $i < k$, and thus does not contain any inverses of R_k. By equating coefficients for X_k we obtain $\hat{\rho}_{x,k} = 0$ for all $k \in [\ell]$. We therefore showed that

$$
\mathsf{V}_1(\mathbf{X}, \mathbf{R}) = \big(\prod_i \mathrm{R}_i\big) \sum_k \rho_{z,k} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}).
$$

Analogously to Remark 2, the reduction can set $\rho_{z,k} = 0$ whenever $\mathsf{Z}_k \equiv 0$ without loss of generality. Thus, applying Lemma 5 yields $\rho_{z,j} = 0$ for $j \in [q]$. This concludes the proof. □

The next lemma captures that if both polynomials representing the verification equations are zero, then $\mathcal{A}$ must have provided a forgery on a message that is a multiple of a previously queried message. The idea here is to consider $\mathsf{V}_2 \equiv 0$ and iteratively compare coefficients in various quotient rings to simplify the equation such that we can reason about the coefficients provided by $\mathcal{A}$.

Lemma 7. *If $\mathsf{V}_1 \equiv 0$ and $\mathsf{V}_2 \equiv 0$, then the message returned by $\mathcal{A}$ is a multiple of a message queried to the signing oracle, in particular*

$$
\exists i^* \in [q] \quad \forall j \in [\ell]: \quad M_j = \rho_{r,i^*} \zeta_{z,i^*} M_j^{(i^*)}.
$$

Proof. By Lemma 6 we have

$$
\hat{\mathsf{R}}(\mathbf{X}, \mathbf{R}) = \rho + \sum_k \rho_{r,k} \mathrm{R}_k^{-1},
$$

and therefore V_2 has the form

$$
\mathsf{V}_2(\mathbf{X}, \mathbf{R}) = \big(\prod_i \mathrm{R}_i^2\big)\Big(\sum_k \mathrm{X}_k \mathsf{M}_k(\mathbf{X}, \mathbf{R}) - \big(\rho + \sum_k \rho_{r,k} \mathrm{R}_k^{-1}\big) \cdot \mathsf{Z}(\mathbf{X}, \mathbf{R})\Big).
$$

Let $j \in [q]$ and denote by $\mathfrak{I}$ the ideal generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell, \mathrm{R}_j\}$. Recall

$$
\mathsf{Z}(\mathbf{X}, \mathbf{R}) = \zeta + \sum_i \zeta_{z,i} \mathsf{Z}_i(\mathbf{X}, \mathbf{R}) + \sum_i \zeta_{r,i} \mathrm{R}_i^{-1}.
$$

Viewing V_2 modulo $\mathfrak{I}$, all the terms containing X_k vanish (cf. Remark 1), and the only terms that remain are the ones where R_j^2 cancels. We obtain

$$
0 \equiv \mathsf{V}_2 \equiv_{\mathfrak{I}} -\rho_{r,j} \zeta_{r,j}, \tag{9}
$$

where j was arbitrary. We will start by showing that $\zeta_{r,k} = 0$ for all $k \in [q]$. Assume towards a contradiction that there exists $k \in [q]$ such that $\zeta_{r,k} \neq 0$.

Using this consider $j \neq k \in [q]$ and let $\mathfrak{J}$ denote the ideal generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell, \mathrm{R}_k, \mathrm{R}_j\}$. Then, analogously to the previous step where we considered the ideal $\mathfrak{I}$, all the terms containing X_k vanish, and the only terms that remain are ones that don't contain R_k or R_j either:

$$\begin{aligned} 0 \equiv \ \frac{-\mathsf{V}_2}{\prod_i \mathrm{R}_i} &\equiv_{\mathfrak{J}} \Big(\prod_i \mathrm{R}_i\Big)\Big(\sum_m \sum_{m' \neq m} \rho_{r,m}\zeta_{r,m'}\mathrm{R}_m^{-1}\mathrm{R}_{m'}^{-1}\Big) \\ &\equiv_{\mathfrak{J}} \Big(\prod_{i \neq k, i \neq j} \mathrm{R}_i\Big)\Big(\rho_{r,k}\zeta_{r,j} + \rho_{r,j}\zeta_{r,k}\Big), \end{aligned}$$

and thus

$$\rho_{r,k}\zeta_{r,j} + \rho_{r,j}\zeta_{r,k} = 0 \quad \text{for all} \quad j \in [q]. \tag{9a}$$

Now since we assumed $\zeta_{r,k} \neq 0$ from (9) we get $\rho_{r,k} = 0$, which with (9a) yields $\rho_{r,j}\zeta_{r,k} = 0$ and thus $\rho_{r,j} = 0$ for all $j \in [q]$. Again let $k \in [q]$ and denote by $\mathfrak{J}$ the ideal generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell, \mathrm{R}_k\}$. We have that

$$0 \equiv \frac{\mathsf{V}_2(\mathbf{X}, \mathbf{R})}{\prod_i \mathrm{R}_i} \equiv_{\mathfrak{J}} \Big(\prod_i \mathrm{R}_i\Big)\Big(-\rho\big(\zeta + \sum_j \zeta_{r,j}\mathrm{R}_j^{-1}\big)\Big) \equiv_{\mathfrak{J}} -\rho\zeta_{r,k}\prod_{i \neq k} \mathrm{R}_i,$$

and therefore $\rho = 0$. With $\rho_{r,j} = 0$ for all $j \in [q]$, Lemma 6 now implies $\mathsf{R} \equiv 0$, which contradicts $\mathcal{A}$ providing a valid forgery. Therefore $\zeta_{r,k} = 0$ for $k \in [q]$, and thus

$$\mathsf{Z}(\mathbf{X}, \mathbf{R}) = \zeta + \sum_k \zeta_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}). \tag{10}$$

Denote by $\mathfrak{L}$ the ideal generated by $\{\mathrm{X}_1, \ldots, \mathrm{X}_\ell\}$. Then, by Remark 1, we have $\mathsf{Z}(\mathbf{X}, \mathbf{R}) \equiv_{\mathfrak{L}} \zeta$ and therefore

$$0 \equiv \frac{-\mathsf{V}_2(\mathbf{X}, \mathbf{R})}{\prod_i \mathrm{R}_i} \equiv_{\mathfrak{L}} \big(\prod_i \mathrm{R}_i\big)\big(\zeta\rho + \sum_j \zeta\rho_{r,i}\mathrm{R}_j^{-1}\big) \equiv_{\mathfrak{L}} \big(\prod_i \mathrm{R}_i\big)\zeta\hat{\mathsf{R}}(\mathbf{X}, \mathbf{R}).$$

Since both $\hat{\mathsf{R}} \not\equiv 0$ and $\prod_k \mathrm{R}_k \not\equiv 0$ modulo $\mathfrak{L}$, we get $\zeta = 0$. We therefore showed that (10) has the form

$$\mathsf{Z}(\mathbf{X}, \mathbf{R}) = \sum_k \zeta_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R}).$$

We will now show that merely one summand is non-zero. Define $i^* := \max\{i \mid \zeta_{z,i} \neq 0\}$, and note that by Remark 2 we have $\mathsf{Z}_{i^*} \not\equiv 0$. Recall that we deduced

$$\mathsf{V}_2(\mathbf{X}, \mathbf{R}) = \big(\prod_i \mathrm{R}_i^2\big)\Big(\sum_k \mathsf{M}_k(\mathbf{X}, \mathbf{R})\mathrm{X}_k - \Big(\rho + \sum_k \rho_{r,k}\mathrm{R}_k^{-1}\Big)\sum_k^{i^*} \zeta_{z,k}\mathsf{Z}_k(\mathbf{X}, \mathbf{R})\Big)$$

and that M_k is defined as

$$\mathsf{M}_k(\mathbf{X}, \mathbf{R}) := \mu^{(k)} + \sum_j \mu_{z,j}^{(k)}\mathsf{Z}_j(\mathbf{X}, \mathbf{R}) + \sum_j \mu_{r,j}^{(k)}\mathrm{R}_j^{-1}. \tag{11}$$

We will show that $\mu_{z,j}^{(k)} = 0$ for $j > i^*$. Let $k^* := \sup\{k \mid \exists j : \mu_{z,k}^{(j)} \neq 0\}$. Again, similarly to Remark 2, we have $\mathsf{Z}_{k^*} \not\equiv 0$. Suppose $k^* > i^*$ and consider all the monomials of V_2 that are divisible by $\mathrm{R}_{k^*}^3$, that is, all the terms in which Z_{k^*} appears

$$\Big(\prod_i \mathrm{R}_i^2\Big)\Big(\sum_j \mu_{z,k^*}^{(j)} \mathsf{Z}_{k^*}(\mathbf{X},\mathbf{R})\mathrm{X}_j\Big) \equiv 0.$$

Since $\mathsf{Z}_{k^*} \not\equiv 0$, equating coefficients we obtain $\mu_{z,k^*}^{(j)} = 0$ for all j, therefore $k^* \leq i^*$.

Now consider all the monomials of V_2 that are divisible by $\mathrm{R}_{i^*}^3$, that is, all the terms in which Z_{i^*} appears, and equate coefficients with the zero polynomial:

$$\mathsf{Z}_{i^*}(\mathbf{X},\mathbf{R})\Big(\prod_i \mathrm{R}_i^2\Big)\left(\sum_j \mu_{z,i^*}^{(j)}\mathrm{X}_j - \Big(\rho + \sum_{k\neq i^*} \rho_{r,k}\mathrm{R}_k^{-1}\Big)\zeta_{z,i^*}\right) \equiv 0.$$

Since $\mathsf{Z}_{i^*} \not\equiv 0$, we can equate coefficients of X_j to obtain $\mu_{z,i^*}^{(j)} = 0$ for $j \in [\ell]$. This leaves us with the subtrahend, where due to $\zeta_{z,i^*} \neq 0$ equating coefficients yields $\rho = 0$ and $\rho_{r,k} = 0$ for $k \in [q] \setminus \{i^*\}$. Now since $\mathsf{R} \not\equiv 0$, we have $\rho_{r,i^*} \neq 0$. This leaves us with

$$\mathsf{V}_2(\mathbf{X},\mathbf{R}) = \Big(\prod_i \mathrm{R}_i^2\Big)\left(\sum_k \mathsf{M}_k(\mathbf{X},\mathbf{R})\mathrm{X}_k - \rho_{r,i^*}\mathrm{R}_{i^*}^{-1}\sum_k^{i^*} \zeta_{z,k}\mathsf{Z}_k(\mathbf{X},\mathbf{R})\right), \qquad (12)$$

and (11) becomes

$$\mathsf{M}_k(\mathbf{X},\mathbf{R}) = \mu^{(k)} + \sum_j^{i^*-1} \mu_{z,j}^{(k)}\mathsf{Z}_k(\mathbf{X},\mathbf{R}) + \sum_j \mu_{r,j}^{(k)}\mathrm{R}_j^{-1}.$$

Now consider the ideal $\mathfrak{I}$ generated by $\{\mathrm{R}_1^2, \ldots, \mathrm{R}_{i^*-1}^2, \mathrm{R}_{i^*}\}$. Recall that $\mathsf{Z}_k := \mathrm{R}_k \sum_j \mathsf{M}_j^{(k)}\mathrm{X}_j$, and that for $j \in [\ell]$ the Laurent polynomial $\mathsf{M}_j^{(k)}$ only has reciprocal terms in $\mathrm{R}_{k'}$ for $k > k'$. Then in this ideal the subtrahend of (12) vanishes, and the only remaining terms are those where R_{i^*} cancels:

$$0 \equiv \frac{\mathsf{V}_2(\mathbf{X},\mathbf{R})}{\prod_k \mathrm{R}_k} \equiv_{\mathfrak{I}} \Big(\prod_{k\neq i^*}\mathrm{R}_k\Big)\sum_j \mu_{r,i^*}^{(j)}\mathrm{X}_j.$$

Equating coefficients for X_j, we obtain $\mu_{r,i^*}^{(j)} = 0$ for $j \in [\ell]$.

Consider the ideal $\mathfrak{J}$ generated by R_{i^*}. Then in the corresponding factor ring the non-zero terms will be those where R_{i^*} cancels. Since we just showed that M_k does not contain any inverses of R_{i^*}, this can only happen in the subtrahend of (12) and thus

$$0 \equiv \frac{-\mathsf{V}_2(\mathbf{X},\mathbf{R})}{\prod_i \mathrm{R}_i} \equiv_{\mathfrak{J}} \Big(\prod_{i\neq i^*}\mathrm{R}_i\Big)\rho_{r,i^*}\sum_k^{i^*-1}\zeta_{z,k}\mathsf{Z}_k(\mathbf{X},\mathbf{R}).$$

Since $\rho_{r,i^*} \neq 0$ and the right-hand side is constant in R_{i^*}, multiplying by R_{i^*} yields

$$\Big(\prod_k \mathrm{R}_k\Big) \sum_j^{i^*-1} \zeta_{z,j} \mathsf{Z}_j(\mathbf{X}, \mathbf{R}) \equiv 0.$$

Now by Remark 2, Lemma 5 applies, and therefore $\zeta_{z,j} = 0$ for $j < i^*$. We therefore showed that there is exactly one index i^* such that $\zeta_{z,i^*} \neq 0$.

Now by expanding the representation of M_k, (12) simplifies to

$$\begin{aligned} \mathsf{V}_2(\mathbf{X}, \mathbf{R}) = \Big(\prod_i \mathrm{R}_i^2\Big)\Big(\sum_k \Big(\mu^{(k)} + \sum_j^{i^*-1} \mu_{z,j}^{(k)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_{j \neq i^*} \mu_{r,j}^{(k)} \mathrm{R}_j^{-1}\Big)\mathrm{X}_k \\ - \rho_{r,i^*} \mathrm{R}_{i^*}^{-1} \zeta_{z,i^*} \mathsf{Z}_{i^*}(\mathbf{X}, \mathbf{R})\Big). \quad (13) \end{aligned}$$

For $j > i^*$ consider this equation in the factor ring obtained by factoring the ideal $\mathfrak{J}$ generated by R_j^2. Then since for $k < j$ we have that $\deg_{\mathrm{R}_j} \mathsf{Z}_k = 0$, in this factor ring the only terms remaining are those of (13) that contain R_j^{-1}. We get

$$0 \equiv \mathsf{V}_2(\mathbf{X}, \mathbf{R}) \equiv_{\mathfrak{J}} \mathrm{R}_j \Big(\prod_{i \neq j} \mathrm{R}_i^2\Big) \sum_k \mu_{r,j}^{(k)} \mathrm{X}_k,$$

and equating coefficients yields $\mu_{r,j}^{(k)} = 0$ for $j > i^*$.

Denote by $\mathfrak{I}$ the ideal generated by $\{\mathrm{X}_i \mathrm{X}_j \mid 1 \leq i \leq j \leq \ell\}$. Recall the definition

$$\mathsf{Z}_{i^*}(\mathbf{X}, \mathbf{R}) := \mathrm{R}_{i^*} \sum_j \Big(\mu^{(i^*,j)} + \sum_k^{i^*-1} \mu_{z,k}^{(i^*,j)} \mathsf{Z}_k(\mathbf{X}, \mathbf{R}) + \sum_k^{i^*-1} \mu_{r,k}^{(i^*,j)} \mathrm{R}_k^{-1}\Big)\mathrm{X}_j.$$

Consider (13) $\equiv 0$ in the corresponding factor ring, where by Remark 1 the terms containing $\mathsf{Z}_k \mathrm{X}_j$ vanish:

$$\begin{aligned} 0 \equiv \mathsf{V}_2(\mathbf{X}, \mathbf{R}) \equiv_{\mathfrak{I}} & \Big(\prod_i \mathrm{R}_i^2\Big)\Big(\sum_j \Big(\mu^{(j)} + \sum_k^{i^*-1} \mu_{r,k}^{(j)} \mathrm{R}_k^{-1}\Big)\mathrm{X}_j \\ & - \rho_{r,i^*} \mathrm{R}_{i^*}^{-1} \zeta_{z,i^*} \sum_j \Big(\mu^{(i^*,j)} + \sum_k^{i^*-1} \mu_{r,k}^{(i^*,j)} \mathrm{R}_k^{-1}\Big)\mathrm{X}_j\Big) \\ \equiv_{\mathfrak{I}} & \Big(\prod_i \mathrm{R}_i^2\Big) \sum_j \mathrm{X}_j \Big(\mu^{(j)} - \rho_{r,i^*} \zeta_{z,i^*} \mu^{(i^*,j)} \\ & + \sum_k^{i^*-1} \Big(\mu_{r,k}^{(j)} - \rho_{r,i^*} \zeta_{z,i^*} \mu_{r,k}^{(i^*,j)}\Big) \mathrm{R}_k^{-1}\Big). \end{aligned}$$

Equating coefficients yields $\mu_{r,k}^{(j)} = \rho_{r,i^*}\zeta_{z,i^*}\mu_{r,k}^{(i^*,j)}$ for $j \in [\ell]$ and $k < i^*$, and $\mu^{(j)} = \rho_{r,i^*}\zeta_{z,i^*}\mu^{(i^*,j)}$ for $j \in [\ell]$. Therefore (13) simplifies to

$$\mathsf{V}_2(\mathbf{X}, \mathbf{R}) = \Big(\prod_i \mathrm{R}_i^2\Big)\left(\sum_k^{i^*-1}\left(\sum_j \left(\mu_{z,k}^{(j)} - \rho_{r,i^*}\zeta_{z,i^*}\mu_{z,k}^{(i^*,j)}\right)\mathrm{X}_j\right)\mathsf{Z}_k\right).$$

For $k < i^*$ define the polynomial

$$\mathsf{P}_k(\mathbf{X}) := \sum_j \left(\mu_{z,k}^{(j)} - \rho_{r,i^*}\zeta_{z,i^*}\mu_{z,k}^{(i^*,j)}\right)\mathrm{X}_j.$$

Whenever $\mathsf{Z}_k = 0$, similarly to Remark 2, we can suppose that $\mu_{z,k}^{(j)} = 0$ and $\mu_{z,k}^{(i^*,j)} = 0$ for all $j \in [\ell]$, which implies $\mathsf{P}_k = 0$. Lemma 5 is therefore applicable, yielding $\mathsf{P}_k \equiv 0$ for $k < i^*$. Equating coefficients yields $\mu_{z,k}^{(j)} = \rho_{r,i^*}\zeta_{z,i^*}\mu_{z,k}^{(i^*,j)}$ for $j \in [\ell]$ and $k < i^*$. Thus, for all $j \in [\ell]$ we derived

$$\begin{aligned}
M_j &= \mu^{(j)}G + \sum_k^{i^*-1}\mu_{z,k}^{(j)}Z_j + \sum_k^{i^*-1}\mu_{r,k}^{(j)}R_k \\
&= \rho_{r,i^*}\zeta_{z,i^*}\mu^{(i^*,j)}G + \sum_k^{i^*-1}\rho_{r,i^*}\zeta_{z,i^*}\mu_{z,k}^{(i^*,j)}Z_j + \sum_k^{i^*-1}\rho_{r,i^*}\zeta_{z,i^*}\mu_{r,k}^{(i^*,j)}R_k \\
&= \rho_{r,i^*}\zeta_{z,i^*}\left(\mu^{(i^*,j)}G + \sum_k^{i^*-1}\mu_{z,k}^{(i^*,j)}Z_j + \sum_k^{i^*-1}\mu_{r,k}^{(i^*,j)}R_k\right) \\
&= \rho_{r,i^*}\zeta_{z,i^*}M_j^{i^*}.
\end{aligned}$$

□

So far, we reasoned about the multivariate verification polynomials V_1 and V_2 where each indeterminate corresponds to one secret value that gets embedded. $\mathcal{B}$ transforms these multivariate verification polynomials into univariate polynomials in Y by evaluating the indeterminates by specifying how y was embedded. This yields the univariate polynomials Q_1 and Q_2 with indeterminate Y.

This transformation from multivariate to univariate polynomials might turn a non-zero polynomial into the zero polynomial. The following lemma will show that in our specific setting this is unlikely to occur.

Lemma 8. *Conditioned on $\mathcal{A}$ winning* $\mathrm{UNF}^{\mathrm{AGM}}$ *we have that the probability that one of the univariate polynomials Q_1 and Q_2 is non-zero is overwhelming:*

$$\Pr\left[\mathsf{Q}_1 \not\equiv 0 \vee \mathsf{Q}_2 \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] \geq 1 - \frac{4q+1}{p-1}.$$

Proof. Assuming that $\mathcal{A}$ wins $\mathrm{UNF}^{\mathrm{AGM}}$, Lemma 7 yields $\mathsf{V}_1 \not\equiv 0 \vee \mathsf{V}_2 \not\equiv 0$. Assume the case $\mathsf{V}_2 \not\equiv 0$. From Corollary 2 we have that V_2 is a polynomial of total degree upper-bounded by $4q+1$. We can therefore apply the BFL Lemma (Lemma 2) to conclude that given $\mathsf{V}_2 \not\equiv 0$, the leading coefficient in Y of

$$\mathsf{V}_2'(\mathbf{U}, \mathbf{V}, \mathbf{U}', \mathbf{V}', \mathrm{Y}) := \mathsf{V}_2(\mathbf{U}\mathrm{Y} + \mathbf{U}', \mathbf{V}\mathrm{Y} + \mathbf{V}')$$

is a polynomial in indeterminates $\mathbf{U}, \mathbf{V}$ of degree upper-bounded by $4q+1$. Call this polynomial $\mathsf{V}'_{2,\max} \in \mathbb{Z}_p[\mathbf{U}, \mathbf{V}]$. Recall that for $i \in [q]$, r_i and c_i are drawn uniformly from $\mathbb{Z}_p^*$ and $\mathbb{Z}_p$, respectively. Let $\mathbf{r}' := \mathbf{r} \odot \mathbf{c}$ and note that

$$\mathsf{Q}_2(\mathrm{Y}) = \mathsf{V}'_2\left(\mathbf{x}, \mathbf{r}, \mathbf{x}', \mathbf{r}', \mathrm{Y}\right). \tag{14}$$

Then by (14), it suffices to show $\mathsf{V}'_{2,\max} \not\equiv 0$ with overwhelming probability. Since $(\mathbb{Z}_p, +)$ and $(\mathbb{Z}_p^*, \cdot)$ are both cyclic, r'_i is uniformly distributed over $\mathbb{Z}_p$. Moreover, (r_i, r'_i) is uniformly distributed over $\mathbb{Z}_p^* \times \mathbb{Z}_p$ since the function

$$\begin{aligned} f \colon \mathbb{Z}_p^* \times \mathbb{Z}_p &\to \mathbb{Z}_p^* \times \mathbb{Z}_p \\ (x, y) &\mapsto (x, x \cdot y) \end{aligned}$$

is a bijection. This implies that the vector $\mathbf{r}' = (\mathbf{r} \odot \mathbf{c})$ is independent from the vector $\mathbf{r}$, and therefore $(\mathbf{x}', \mathbf{r}')$ is independent of $(\mathbf{x}, \mathbf{r})$.

Furthermore, since $(\mathbf{x}, \mathbf{r})$ is completely hidden from the adversary's view (due to the additive mask $(\mathbf{x}', \mathbf{r}')$ added after the multiplication), it is independent from the coefficients of V'_2 (determined by $\mathcal{A}$), and thus independent of the coefficients of $\mathsf{V}_{2,\max}$ (still fully determined by $\mathcal{A}$). Thus the Schwartz-Zippel Lemma (Lemma 1) applied to $\mathsf{V}_{2,\max}$ on uniform inputs $\boldsymbol{x}, \boldsymbol{r}$ yields

$$\Pr\left[\mathsf{V}_{2,\max} \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] \geq 1 - \frac{4q+1}{p-1}.$$

Overall, we get

$$\begin{aligned} \Pr\left[\mathsf{Q}_1 \not\equiv 0 \vee \mathsf{Q}_2 \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] &\geq \Pr\left[\mathsf{Q}_2 \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] \\ &= \Pr\left[\mathsf{V}_{2,\max} \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] \\ &\geq 1 - \frac{4q+1}{p-1}. \end{aligned}$$

Noticing that the case $\mathsf{V}_1 \not\equiv 0$ follows analogously concludes the proof. □

We will proceed with the proof of Theorem 1. We will show that reduction $\mathcal{B}$'s advantage is close to $\mathcal{A}$'s advantage.

We know that $\mathcal{B}$ wins if $\mathcal{A}$ wins and ($\mathsf{Q}_1 \not\equiv 0$ or $\mathsf{Q}_2 \not\equiv 0$), since $\mathcal{A}$ winning implies $\mathsf{Verify}(pk, \boldsymbol{M}, \sigma) = 1$, which means $e\big(R^*, G_2\big) = e\big(G, \hat{R}^*\big)$ and $\sum_{i=1}^{q} e\big(M_i^*, pk_i\big) = e\big(Z, \hat{R}^*\big)$. Therefore the logarithm y of $Y^{(1)}$ is a root of both Q_1 and Q_2. Since at least one of them is not identically zero, with its degree upper-bounded by $4q+1$, reduction $\mathcal{B}$ can efficiently factor the non-zero one to obtain y among its roots, and therefore solve q-PowDenDL. This yields

$$\begin{aligned} \mathsf{Adv}_{\mathsf{BGGen},\mathcal{B}}^{q\text{-PowDenDL}} &\geq \Pr\left[\mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1 \wedge (\mathsf{Q}_1 \not\equiv 0 \vee \mathsf{Q}_2 \not\equiv 0)\right] \\ &= \Pr\left[\mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right] \Pr\left[\mathsf{Q}_1 \not\equiv 0 \vee \mathsf{Q}_2 \not\equiv 0 \,\middle|\, \mathrm{UNF}_{\mathcal{A}}^{\mathrm{AGM}} = 1\right], \end{aligned}$$

and applying Lemma 8 yields

$$\geq \mathsf{Adv}_{\mathcal{A}}^{\mathrm{UNF}^{\mathrm{AGM}}}\left(1 - \frac{4q+1}{p-1}\right) \geq \mathsf{Adv}_{\mathcal{A}}^{\mathrm{UNF}^{\mathrm{AGM}}} - \frac{4q+1}{p-1}.$$

This concludes the proof of Theorem 1. □

Acknowledgments. The authors would like to thank the anonymous reviewers for ASIACRYPT 2024 for their very valuable comments. This work was funded by the Vienna Science and Technology Fund (WWTF) [10.47379/VRG18002] and by the Austrian Science Fund (FWF) [10.55776/F8515-N].

References

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.

[AGHO11] Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666. Springer, 2011.

[AGO11] Masayuki Abe, Jens Groth, and Miyako Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 628–646. Springer, 2011.

[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, 2004.

[BB08] Dan Boneh and Xavier Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177, 2008.

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, 2005.

[BCC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125. Springer, 2009.

[BEK+20] Jan Bobolz, Fabian Eidens, Stephan Krenn, Daniel Slamanig, and Christoph Striecks. Privacy-preserving incentive systems with highly efficient point-collection. In Hung-Min Sun, Shiuh-Pyng Shieh, Guofei Gu, and Giuseppe Ateniese, editors, *ASIACCS 20*, pages 319–333. ACM Press, 2020.

[BFL20] Balthazar Bauer, Georg Fuchsbauer, and Julian Loss. A classification of computational assumptions in the algebraic group model. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 121–151. Springer, 2020.

[BFP21] Balthazar Bauer, Georg Fuchsbauer, and Antoine Plouviez. The one-more discrete logarithm assumption in the generic group model. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 587–617. Springer, 2021.

[BFR24] Balthazar Bauer, Georg Fuchsbauer, and Fabian Regen. On proving equivalence class signatures secure from non-interactive assumptions. In Qiang Tang and Vanessa Teague, editors, *PKC 2024, Part I*, volume 14601 of *LNCS*, pages 3–36. Springer, 2024.

[BHKS18] Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Signatures with flexible public key: Introducing equivalence classes for public keys. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 405–434. Springer, 2018.

[BLL+19] Xavier Bultel, Pascal Lafourcade, Russell W. F. Lai, Giulio Malavolta, Dominique Schröder, and Sri Aravinda Krishnan Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 159–189. Springer, 2019.

[BLS04] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. On the selection of pairing-friendly groups. In Mitsuru Matsui and Robert J. Zuccherato, editors, *SAC 2003*, volume 3006 of *LNCS*, pages 17–25. Springer, 2004.

[BNPS03] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology*, 16(3):185–215, 2003.

[Bow17] Sean Bowe. BLS12-381: New zk-SNARK elliptic curve construction, 2017. https://electriccoin.co/blog/new-snark-curve/.

[BRS23] Fabrice Benhamouda, Mariana Raykova, and Karn Seth. Anonymous counting tokens. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part II*, volume 14439 of *LNCS*, pages 245–278. Springer, 2023.

[BSW23] Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner. Unlinkable policy-compliant signatures for compliant and decentralized anonymous payments. Cryptology ePrint Archive, Paper 2023/1070, 2023. https://eprint.iacr.org/2023/1070.

[CDLP22] Aisling Connolly, Jérôme Deschamps, Pascal Lafourcade, and Octavio Perez-Kempner. Protego: Efficient, revocable and auditable anonymous credentials with applications to Hyperledger Fabric. In Takanori Isobe and Santanu Sarkar, editors, *INDOCRYPT 2022*, volume 13774 of *LNCS*, pages 249–271. Springer, 2022.

[CFF+21] Matteo Campanelli, Antonio Faonio, Dario Fiore, Anaïs Querol, and Hadrián Rodríguez. Lunar: A toolbox for more efficient universal and updatable zkSNARKs and commit-and-prove extensions. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part III*, volume 13092 of *LNCS*, pages 3–33. Springer, 2021.

[CH20] Geoffroy Couteau and Dominik Hartmann. Shorter non-interactive zero-knowledge arguments and ZAPs for algebraic languages. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 768–798. Springer, 2020.

[CHM+20] Alessandro Chiesa, Yuncong Hu, Mary Maller, Pratyush Mishra, Psi Vesely, and Nicholas P. Ward. Marlin: Preprocessing zkSNARKs with universal and updatable SRS. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 738–768. Springer, 2020.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 268–289. Springer, 2003.

[CL19] Elizabeth C. Crites and Anna Lysyanskaya. Delegatable anonymous credentials from mercurial signatures. In Mitsuru Matsui, editor, *CT-RSA 2019*, volume 11405 of *LNCS*, pages 535–555. Springer, 2019.

[CL21] Elizabeth C. Crites and Anna Lysyanskaya. Mercurial signatures for variable-length messages. *PoPETs*, 2021(4):441–463, 2021.

[CLP22] Aisling Connolly, Pascal Lafourcade, and Octavio Perez-Kempner. Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part I*, volume 13177 of *LNCS*, pages 409–438. Springer, 2022.

[CS20] Remi Clarisse and Olivier Sanders. Group signature without random oracles from randomizable signatures. In Khoa Nguyen, Wenling Wu, Kwok-Yan Lam, and Huaxiong Wang, editors, *ProvSec 2020*, volume 12505 of *LNCS*, pages 3–23. Springer, 2020.

[DHS15] David Derler, Christian Hanser, and Daniel Slamanig. A new approach to efficient revocable attribute-based anonymous credentials. In Jens Groth, editor, *15th IMA International Conference on Cryptography and Coding*, volume 9496 of *LNCS*, pages 57–74. Springer, 2015.

[DS16] David Derler and Daniel Slamanig. Fully-anonymous short dynamic group signatures without encryption. Cryptology ePrint Archive, Report 2016/154, 2016. https://eprint.iacr.org/2016/154.

[DS18] David Derler and Daniel Slamanig. Highly-efficient fully-anonymous dynamic group signatures. In Jong Kim, Gail-Joon Ahn, Seungjoo Kim, Yongdae Kim, Javier López, and Taesoo Kim, editors, *ASIACCS 18*, pages 551–565. ACM Press, 2018.

[EHK+13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, 2013.

[EHK+17] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Luis Villar. An algebraic framework for Diffie-Hellman assumptions. *Journal of Cryptology*, 30(1):242–288, 2017.

[FG18] Georg Fuchsbauer and Romain Gay. Weakly secure equivalence-class signatures from standard assumptions. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 153–183. Springer, 2018.

[FGKO17] Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi. Access control encryption for equality, comparison, and more. In Serge Fehr, editor, *PKC 2017, Part II*, volume 10175 of *LNCS*, pages 88–118. Springer, 2017.

[FHKS16] Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model from weaker assumptions. In Vassilis Zikas and Roberto De Prisco, editors, *SCN 16*, volume 9841 of *LNCS*, pages 391–408. Springer, 2016.

[FHS15] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 233–253. Springer, 2015.

[FHS19] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *Journal of Cryptology*, 32(2):498–546, 2019.

[FKL18] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 33–62. Springer, 2018.

[FP09] Georg Fuchsbauer and David Pointcheval. Proofs on encrypted values in bilinear groups and an application to anonymity of signatures. In Hovav Shacham and Brent Waters, editors, *PAIRING 2009*, volume 5671 of *LNCS*, pages 132–149. Springer, 2009.

[Fuc11] Georg Fuchsbauer. Commuting signatures and verifiable encryption. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 224–245. Springer, 2011.

[Fuc14] Georg Fuchsbauer. Breaking existential unforgeability of a signature scheme from asiacrypt 2014. Cryptology ePrint Archive, Report 2014/892, 2014. https://eprint.iacr.org/2014/892.

[FV10] Georg Fuchsbauer and Damien Vergnaud. Fair blind signatures without random oracles. In Daniel J. Bernstein and Tanja Lange, editors, *AFRICACRYPT 10*, volume 6055 of *LNCS*, pages 16–33. Springer, 2010.

[GHKP18] Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan. More efficient (almost) tightly secure structure-preserving signatures. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 230–258. Springer, 2018.

[GL23] Scott Griffy and Anna Lysyanskaya. Pacific: Privacy-preserving automated contact tracing scheme featuring integrity against cloning. Cryptology ePrint Archive, Paper 2023/371, 2023. https://eprint.iacr.org/2023/371.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 99–108. ACM Press, 2011.

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive, Paper 2019/953, 2019.

[Han23] Lucjan Hanzlik. Non-interactive blind signatures for random messages. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 722–752. Springer, 2023.

[HPP20] Chloé Hébant, Duong Hieu Phan, and David Pointcheval. Linearly-homomorphic signatures and scalable mix-nets. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 597–627. Springer, 2020.

[HRS15] Christian Hanser, Max Rabkin, and Dominique Schröder. Verifiably encrypted signatures: Security revisited and a new construction. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *ESORICS 2015, Part I*, volume 9326 of *LNCS*, pages 146–164. Springer, 2015.

[HS14] Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 491–511. Springer, 2014.

[HS21] Lucjan Hanzlik and Daniel Slamanig. With a little help from my friends: Constructing practical anonymous credentials. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021*, pages 2004–2023. ACM Press, 2021.

[KSD19] Mojtaba Khalili, Daniel Slamanig, and Mohammad Dakhilalian. Structure-preserving signatures on equivalence classes from standard assumptions. In Steven D. Galbraith and Shiho Moriai, editors, *ASIA-*

CRYPT 2019, Part III, volume 11923 of *LNCS*, pages 63–93. Springer, 2019.

[Lip12] Helger Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 169–189. Springer, 2012.

[LSZ22] Helger Lipmaa, Janno Siim, and Michal Zajac. Counting vampires: From univariate sumcheck to updatable ZK-SNARK. Cryptology ePrint Archive, Paper 2022/406, 2022.

[Mau05] Ueli M. Maurer. Abstract models of computation in cryptography (invited paper). In Nigel P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12. Springer, 2005.

[MBG+23] Omid Mir, Balthazar Bauer, Scott Griffy, Anna Lysyanskaya, and Daniel Slamanig. Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *ACM CCS 2023*, pages 30–44. ACM Press, 2023.

[MBKM19] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. Sonic: Zero-knowledge SNARKs from linear-size universal and updatable structured reference strings. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019*, pages 2111–2128. ACM Press, 2019.

[MRV16] Paz Morillo, Carla Ràfols, and Jorge Luis Villar. The kernel matrix Diffie-Hellman assumption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758. Springer, 2016.

[MSBM23] Omid Mir, Daniel Slamanig, Balthazar Bauer, and Renérhofer. Practical delegatable anonymous credentials from equivalence class signatures. *Proc. Priv. Enhancing Technol.*, 2023(3):488–513, 2023.

[Nao03] Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109. Springer, 2003.

[Nec94] V. I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[PM23] Colin Putman and Keith M. Martin. Selective delegation of attributes in mercurial signature credentials. In Elizabeth A. Quaglia, editor, *IMACC 2023*, volume 14421 of *LNCS*, pages 181–196. Springer, 2023.

[Poi23] David Pointcheval. Linearly-homomorphic signatures for short randomizable proofs of subset membership. In *Eighth International Joint Conference on Electronic Voting (E-Vote-ID'23)*, 2023.

[Poi24] David Pointcheval. Efficient universally-verifiable electronic voting with everlasting privacy. *Cryptology ePrint Archive*, 2024.

[RZ21] Carla Ràfols and Arantxa Zapico. An algebraic framework for universal and updatable SNARKs. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 774–804, Virtual Event, Springer, 2021.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, 1997.

[SKSW22] Yumi Sakemi, Tetsutaro Kobayashi, Tsunekazu Saito, and Riad S. Wahby. Pairing-Friendly Curves. Internet-Draft draft-irtf-cfrg-pairing-friendly-curves-11, Internet Engineering Task Force, 2022. Work in Progress.

[SYF+23] Rui Shi, Yang Yang, Huamin Feng, Feng Yuan, Huiqin Xie, and Jianyi Zhang. Prirpt: Practical blockchain-based privacy-preserving reporting system with rewards. *Journal of Systems Architecture*, 143:102985, 2023.

[WTSD23] Eva Wisse, Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. A 2rid-anonymous direct authentication and remote identification of commercial drones. *IEEE Internet of Things Journal*, 2023.

[ZYY+23] Yonghua Zhan, Bixia Yi, Yang Yang, Rui Shi, Chen Dong, and Minming Huang. A privilege-constrained sanitizable signature scheme for e-health systems. *Journal of Systems Architecture*, 142:102939, 2023.