Structure-Preserving Signatures on Equivalence Classes From Standard Assumptions*

Mojtaba Khalili[1,**], Daniel Slamanig[2], and Mohammad Dakhilalian[1]

[1] Isfahan University of Technology, Iran
{m.khalili,mdalian}@ec.iut.ac.ir
[2] AIT Austrian Institute of Technology, Vienna, Austria
daniel.slamanig@ait.ac.at

Abstract. Structure-preserving signatures on equivalence classes (SPS-EQ) introduced at ASIACRYPT 2014 are a variant of SPS where a message is considered as a projective equivalence class, and a new representative of the same class can be obtained by multiplying a vector by a scalar. Given a message and corresponding signature, anyone can produce an updated and randomized signature on an arbitrary representative from the same equivalence class. SPS-EQ have proven to be a very versatile building block for many cryptographic applications.
In this paper, we present the first EUF-CMA secure SPS-EQ scheme under standard assumptions. So far only constructions in the generic group model are known. One recent candidate under standard assumptions are the weakly secure equivalence class signatures by Fuchsbauer and Gay (PKC'18), a variant of SPS-EQ satisfying only a weaker unforgeability and adaption notion. Fuchsbauer and Gay show that this weaker unforgeability notion is sufficient for many known applications of SPS-EQ. Unfortunately, the weaker adaption notion is only proper for a semi-honest (passive) model and as we show in this paper, makes their scheme unusable in the current models for almost all of their advertised applications of SPS-EQ from the literature. We then present a new EUF-CMA secure SPS-EQ scheme with a tight security reduction under the SXDH assumption providing the notion of perfect adaption (under malicious keys). To achieve the strongest notion of perfect adaption under malicious keys, we require a common reference string (CRS), which seems inherent for constructions under standard assumptions. However, for most known applications of SPS-EQ we do not require a trusted CRS (as the CRS can be generated by the signer during key generation). Technically, our construction is inspired by a recent work of Gay et al. (EUROCRYPT'18), who construct a tightly secure message authentication code and translate it to an SPS scheme adapting techniques due to Bellare and Goldwasser (CRYPTO'89).

1 Introduction

Structure-preserving signatures (SPS) [AFG+10] are signatures where the messages, public keys and signatures only consists of elements of groups equipped with an efficient bilinear map, and the verification algorithm just consists of group membership checks and evaluation of pairing product equations (PPEs). SPS schemes [AFG+10, AGHO11, ACD+12,

* This is the full version of the article with the same title which appears at ASIACRYPT 2019.
** Work partly done while visiting Universitat Pompeu Fabra, Barcelona, Spain.

AGOT14, KPW15, Gha16, JR17, Gha17, AHN+17, JOR18, GHKP18, AJOR18] are compatible with efficient pairing-based NIZK proofs [GS08], and are a useful building-block for many cryptographic applications, such as blind signatures [AFG+10, FHS15], group signatures [AFG+10, LPY15], traceable signatures [ACHO11], group encryption [CLY09], homomorphic signatures [LPJY13], delegatable anonymous credentials [Fuc11], compact verifiable shuffles [CKLM12], network coding [ALP12], oblivious transfer [GH08], tightly secure encryption [HJ16] and anonymous e-cash [BCF+11]. SPS schemes come in various different flavors such as being able to sign elements in either one or both source groups of the bilinear group or requiring certain conditions for messages (e.g., messages need to be Diffie-Hellman tuples [Fuc09, Gha17]). They come with different provable security guarantees, ranging from ones that are directly analyzed in the generic group model (GGM) to ones that can be constructed from standard assumptions such as SXDH or SXDLin (typically within the Matrix-Diffie-Hellman assumption framework [EHK+17]) and under different qualities of the reduction (from very loose to tight reductions). A desirable goal is to construct schemes with tight security reductions from standard assumptions which are at the same time highly efficient. Some SPS schemes are also randomizable (e.g., [AFG+10, AGOT14]), meaning that a signature can be randomized to another unlinkable valid signature on the same message.

Structure-preserving signatures on equivalence classes (SPS-EQ) [HS14, FHS14, FHS19] are a variant of SPS where anyone can randomize not only signatures, but a message-signature pair publicly, i.e., in addition to randomizing the signature also the message can be randomized. They have proven to be useful in many applications such as attribute-based anonymous credentials [HS14, DHS15, FHS19], delegatable anonymous credentials [CL19], self-blindable certificates [BHKS18], blind signatures [FHS15, FHKS16], group signatures [DS18, BHKS18, CS18, BHS18], sanitizable signatures [BLL+19], verifiably encrypted signatures [HRS15], access control encryption [FGKO17] or proving the correctness of a shuffle in mix-nets (i.e., for anonymous communication or electronic voting) [HPP19]. In many of these applications, the idea of randomizing signatures and messages offers the same functionality as when using SPS schemes combined with a NIZK proof, but without the need for any NIZK. Consequently, this allows for the design of more efficient constructions.

More concretely, in an SPS-EQ scheme, given a signature on an equivalence class defined over the message space, anyone can update the signature to another representative of the same class. Defined on $(\mathbb{G}^*)^\ell$ (where $\mathbb{G}$ is of prime order p), this equivalence relation $\sim_{\mathcal{R}}$ is as follows ($\ell > 1$):

$$\mathbf{M} \in (\mathbb{G}^*)^\ell \sim_{\mathcal{R}} \mathbf{N} \in (\mathbb{G}^*)^\ell \Leftrightarrow \exists \mu \in \mathbb{Z}_p^* : \mathbf{M} = \mu\mathbf{N}$$

An SPS-EQ scheme signs an equivalence class $[\mathbf{M}]_{\mathcal{R}}$ for $\mathbf{M} \in (\mathbb{G}_i^*)^\ell$ by signing a representative $\mathbf{M}$ of $[\mathbf{M}]_{\mathcal{R}}$. It then allows for switching to other representatives of $[\mathbf{M}]_{\mathcal{R}}$ and updating the signature without access to the secret key. Two important properties of SPS-EQ are *unforgeability* (EUF-CMA security) defined on equivalence classes and *perfect adaption* (potentially even under malicious signing keys), where the latter requires that updated signatures (output by the algorithm ChgRep) are distributed identically to new signatures on the respective representative (if signatures or even if signing keys are computed maliciously). Latter together with the DDH assumption on the message space then yields a notion of unlinkability, i.e., that original signatures and those output by ChgRep cannot be linked. As it turns out, coming up with constructions that achieve *both notions simultaneously* is a challenging task.

We note that, as observed in [FHS15], every SPS-EQ yields a (randomizable) SPS scheme by appending some fixed group element to the message vector before signing and which is checked on verification, to allow only one single representative of each class. Recently, the concept of SPS-EQ has even been further extended to consider also equivalence classes on the public keys, denoted as signatures with flexible public key [BHKS18] and equivalence classes on messages and public keys simultaneously, denoted as mercurial signatures [CL19]. This further extends the scope of applications.

Prior approaches to construct SPS-EQ. The first instantiation of SPS-EQ in [HS14] was secure only against random message attacks, and later Fuchsbauer et al. [FHS14, FHS19] presented a revised scheme that achieves EUF-CMA security in the generic group model (GGM). In [FHS15], Fuchsbauer et al. present another EUF-CMA secure scheme under a q-type assumption, which by construction does not provide the perfect adaption notion and thus is not interesting for existing applications of SPS-EQ. Recently, Fuchsbauer and Gay [FG18], presented a version of SPS-EQ (called equivalence class signatures or EQS) which can be proven secure under standard assumptions, i.e., in the Matrix-Diffie-Hellman assumption framework [EHK+17]. In order to prove their scheme secure, they have introduced a weakened unforgeability notion called existential unforgeability under chosen open message attacks (EUF-CoMA), in which the adversary does not send group element vectors to the signing oracle but vectors of $\mathbb{Z}_p^*$ elements. Moreover, in contrast to the original definition of SPS-EQ in [HS14] and the scheme of Fuchsbauer et al. [FHS14, FHS19], which allows to randomize a given signature (change the representative) an arbitrary number of times, the scheme of Fuchsbauer and Gay [FG18] distinguishes two types of signatures. The first type comes from the signing algorithm and when randomized yields a signature of the second type, which cannot be randomized any further. As argued by Fuchsbauer and Gay in [FG18], for most of the known applications of SPS-EQ the combination of EUF-CoMA notion and the one-time randomizability is sufficient. Actually, as argued in [FG18], it is sufficient for all applications in the literature, except for the one to round-optimal blind signatures from SPS-EQ [FHS15].

The construction of Fuchsbauer and Gay in [FG18] does also rely on a weakened notion of adaption (weaker than the original one from [FHS15] in that it only considers honestly generated keys and honestly computed signatures). We will show that even though their weaker unforgeability notion is sufficient for applications, the weaker adaption notion makes the scheme suitable only for restricted applications, i.e., access control encryption (ACE) or attribute-based credentials (ABCs) with an honest credential issuer. Moreover, the application to verifiably encrypted signatures in [HRS15] requires another notion called perfect composition, which [FG18] seem to assume implicitly. Unfortunately, their scheme does not satisfy this notion. Consequently, for the interesting schemes providing the perfect adaption notion from [FHS15], the current state of affairs is that there is only the EUF-CMA secure scheme from [FHS14, FHS19] secure in the GGM.

Tight security for SPS-EQ schemes. Tight security allows to choose cryptographic parameters of a scheme in a way that is supported by a security proof, without the need to sacrifice efficiency by compensating the security loss of a reduction with larger parameters. Latter can be significant if the reduction is very loose. In case of SPS, quite some progress has been made in recent years on constructing tightly-secure SPS [HJ12, AHN+17, JOR18, AJOR18, GHKP18], though the state-of-the-art tightly-secure schemes under standard assumptions are still less efficient than for instance schemes proven secure in the generic group

model (GGM). While tight security is quite well studied within SPS (and other primitives such as encryption [HJ12, GHKW16, Hof17], signatures [HJ12, CW13, Hof17, GJ18], identity-based encryption [CW13, HKS15, HJP18], key exchange [BHJ+15, GJ18, HHK18], or zero-knowledge proofs [HJ12, GHKW16]), there are no such results for SPS-EQ schemes so far.

1.1 Our Contributions

Our contributions in this paper can be summarized as follows:

Analysis of FG18: Firstly, we revisit the concrete approach to construct EUF-CoMA secure EQS from Fuchsbauer and Gay in [FG18], representing the only known candidate towards perfectly adapting SPS-EQ under standard assumptions so far. Thereby, we identify various problems with the applications of the scheme presented in [FG18]. We stress that we do not present attacks on the scheme itself (which is secure in their model), but show that their adaption notion is too weak for most applications claimed in [FG18] (apart from access control encryption (ACE) [FGKO17]). Briefly summarizing, we first show that their scheme cannot be used for the application to attribute-based credentials (ABCs) [FHS14, FHS19]. We demonstrate an attack based on a trapdoor in the signing key that invalidates the anonymity proof for ABCs. Secondly, we show an attack that demonstrates that the scheme in [FG18] cannot be used even for applications that assume honest generation of signing keys and in particular for ABCs under honest-keys [HS14] and dynamic group signatures [DS18]. We stress that due to this too weak adaption notion concrete instantiations presented in follow up works by Backes et al. [BHKS18, BHS18], that rely on the FG18 scheme from [FG18], are invalidated and need to be reconsidered. Our results allow to repair their now broken claims in part.[3] Thirdly, we show that the FG18 scheme does not satisfy another notion called perfect composition [HRS15], invalidating the use of their scheme for application to verifiably encrypted signatures as discussed in [FG18]. Consequently, this means that contrary to their claim, the EQS framework and scheme in [FG18] can only be used for the construction of access control encryption (ACE) in [FGKO17] and for all other applications no instantiations under standard assumptions remain. We stress that one could relax the security models of the applications to make [FG18] usable again, but such models where signatures and keys are assumed to be generated honestly, i.e., that only guarantee semi-honest (passive) security, limits the practical applications. For example, one could consider ABCs with anonymity against honest credential issuers and use the EQS from [FG18].

SPS-EQ from standard assumptions and applications: As our main contribution, we provide the first construction of SPS-EQ under standard assumptions and in particular the Matrix-Diffie-Hellman assumption framework. We therefore have to revise the model of SPS-EQ in some aspects: (1) we introduce tags, where the signing algorithm outputs a signature and a tag, randomization (i.e., ChgRep) requires a signature and a tag, whereas for verification only the signature is required; signatures that have been randomized using a tag can not further be randomized, i.e., only a single randomization is possible. This definition is comparable to the one in [FG18], apart that FG18 does not use tags. We stress that as demonstrated in [FG18], this restriction does not affect existing applications of SPS-EQ. (2) we require that signers generate their signing keys with respect to a common reference

[3] For the group signatures in [BHS18] it will only work with our construction when relying on a CRS, or by using the construction secure in the GGM in [FHS14].

string (CRS) for achieving the perfect adaption notion in the malicious setting (prior works on SPS-EQ did not consider having a CRS). We will show that this does not impact the applications discussed in [FG18] with the exception of anonymous credentials in the malicious key model, as the security models in all other applications assume honest generation of the signing keys and thus every signer can produce its own CRS as part of the signing key. As we, however, cannot avoid a CRS in the malicious key setting, we are not able to instantiate round-optimal blind signatures in the standard model from SPS-EQ [FHS15] under standard assumptions, which [FG18] could not achieve either. On the positive side, however, it allows us to obtain the most efficient round-optimal blind signatures in the CRS model from standard assumptions.

On the use of a CRS. Although our scheme does not require a CRS for nearly all of the applications of SPS-EQ, avoiding a CRS in the malicious setting would be good. The use of a CRS in general seems to be debatable, as it needs to be generated by some trusted third party that is hard to find in the real world. Within recent years, we have seen a number of deployed real-world applications that require a CRS when using zk-SNARKS (e.g., Zcash[4] being probably the most prominent one) and which have used multi-party computation ceremonies to construct the CRS in a way that no entity provably knows the trapdoor. A number of such ceremonies has been run in real-world[5] and various works discuss approaches to achieve it [BCG+15, BGM17, BGG19]. In the light of this, we do not consider it unrealistic to generate a CRS for the use within practical applications of SPS-EQ that require security under malicious keys, especially since the CRS does not depend on the message length ℓ and so a single CRS can be used for all types of SPS-EQ keys for different applications. Furthermore, it seems interesting to investigate the application of recent approaches towards subversion resistant (QA)-NIZK [BFS16, ALSZ18] or updatable CRS [GKM+18, Lip19], though this typically comes at the cost of rather strong knowledge assumptions. Clearly, ultimately it would be good to find SPS-EQ in the malicious key model without a CRS, which we leave as a challenging open problem.

1.2 Outline of our Construction

Fuchsbauer and Gay [FG18] modify an affine MAC of Blazy et al. [BKP14] to obtain a linear structure-preserving MAC. Then, they make the scheme publicly verifiable using a known technique from Kiltz and Wee [KW15] already used previously in context of SPS [KPW15]. Unfortunately, the structure-preserving MAC has an inherent problem in the security game, where both messages and Matrix Decision Diffie-Hellman (MDDH) challenges belong to the same source group of the bilinear group. This forces them to use the weaker EUF-CoMA instead of EUF-CMA security. Consequently, as we are interested in EUF-CMA security, we need to look for a different framework when trying to construct EUF-CMA secure SPS-EQ schemes.

Therefore, we borrow a central idea from the recent work of Gay et al. [GHKP18]. In particular, they use a specific OR-proof [Ràf15] to then construct tightly secure structure-preserving MACs based on the key encapsulation mechanism of Gay et al. in [GHK17]. More precisely, they make use of adaptive partitioning [Hof17] to randomize all tags in their MAC.

[4] https://z.cash/

[5] see e.g., https://z.cash/blog/the-design-of-the-ceremony/ or https://www.zfnd.org/blog/conclusion-of-powers-of-tau/.

Their work is based on the observation (core lemma in [GHKP18]) that for all $[\mathbf{t}]_1 = [\mathbf{A_0}]_1\mathbf{r}$ with $\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^k$ chosen freshly for each instance, fixed matrices $\mathbf{A_0}, \mathbf{A_1} \xleftarrow{R} \mathcal{D}_{2k,k}$, and a NIZK proof π for $\mathbf{t} \in \mathrm{span}(\mathbf{A_0}) \cup \mathrm{span}(\mathbf{A_1})$, the following values

$$\mathbf{k_0}^\top[\mathbf{t}]_1 \ , \qquad (\mathbf{k_0}^\top + \mathbf{s}^\top)[\mathbf{t}]_1 \tag{1}$$

are indistinguishable under the MDDH assumption, where $\mathbf{k_0} \leftarrow \mathbb{Z}_p^{2k}$ is a key, and $\mathbf{s} \in \mathbb{Z}_p^{2k}$ is a fresh random value for each instance. Actually, they show that $[\mathbf{k_0}^\top\mathbf{t}]_1$ is pseudorandom.

In this paper, we are going to present an approach to obtain malleability for this pseudorandom function, which we use as one part of our signature, and the NIZK proof as another part. Therefore, we first add a tag (to allow a homomorphism on the pseudorandom part) to our signature, such that everyone who knows it can re-randomize the pseudorandom part. Second, we revise the NIZK proof and give a proof for well-formedness of both the pseudorandom part and the tag, such that it can be re-randomized and that we finally get a fresh signature, including fresh pseudorandom part and a proof for it. More precisely, we first show that for all $[\mathbf{t}]_1 = [\mathbf{A_0}]_1\mathbf{r}_1$ and $[\mathbf{w}]_1 = [\mathbf{A_0}]_1\mathbf{r}_2$ for $\mathbf{r}_1, \mathbf{r}_2 \xleftarrow{R} \mathbb{Z}_p^k$ chosen freshly for each instance, and a NIZK proof π for $\mathbf{t}, \mathbf{w} \in \mathrm{span}(\mathbf{A_0}) \cup \mathrm{span}(\mathbf{A_1})$ (to be discussed later), the following tuples are indistinguishable under the MDDH assumption

$$(\mathbf{k_0}^\top[\mathbf{t}]_1, \mathbf{k_0}^\top[\mathbf{w}]_1) \ , \qquad ((\mathbf{k_0}^\top + \mathbf{s}^\top)[\mathbf{t}]_1, \mathbf{k_0}^\top[\mathbf{w}]_1). \tag{2}$$

We then use this MAC (for $k = 1$)[6] to construct an SPS-EQ scheme on a message $[\mathbf{m}]_1 \in (\mathbb{G}_1^*)^\ell$. Our signature has a basic form like $\sigma = \mathbf{k_0}^\top[\mathbf{t}]_1 + \mathbf{k}^\top[\mathbf{m}]_1$, with a tag $\tau = \mathbf{k}_0^\top[\mathbf{w}]_1$ (which is only required for randomization), where $\mathbf{k_0} \xleftarrow{R} \mathbb{Z}_p^2$ and $\mathbf{k} \xleftarrow{R} \mathbb{Z}_p^\ell$. We can use (2) to add some randomness to the signature as $\sigma = \mathbf{k_0}^\top[\mathbf{t}]_1 + \mathbf{k}^\top[\mathbf{m}]_1 + \zeta$ for $\zeta \xleftarrow{R} \mathbb{Z}_p$. At a high level, by adding randomness to each signature, we can make every signature independent of each other. So, we completely hide the values $\mathbf{k}$, and an adversary has negligible chance to compute a valid forgery. On the other hand, everyone can obtain a fresh tag, using previous tag τ, and add it to the signature to obtain a fresh pseudorandom part. From a high level perspective, we have a basic MAC which is additively homomorphic and our signatures and tags are two instances of it, one on message $[\mathbf{m}]_1$ and another one on message zero. This allows deriving a signature on $\mu[\mathbf{m}]_1$ for $\mu \xleftarrow{R} \mathbb{Z}_p^*$, i.e., to adapt the signature part to representative $\mu[\mathbf{m}]_1$, using a multiplication of the signature part with μ and then add it to the fresh tag. Note that, in our scheme we do not need to have access to the tag τ in the verification algorithm, but it is required for randomizing messages and signatures (changing representatives in the language of SPS-EQ). We note that in the EUF-CMA game, we model it in a way that on a signature query the challenger returns both the signature and the tag, while the adversary only needs to output a signature without the tag as its forgery attempt.

Now, we will discuss how to randomize the NIZK proof. At this point, there is an obvious problem with the OR-proof used in [GHKP18] and we need to revise their approach such that the proof is randomizable (proofs can be re-randomized to look like fresh proofs) and malleable (statements for given proofs can be updated), where latter is required to switch between representatives of a class. In particular, to obtain these properties we change a part

[6] We note that we can only instantiate our construction for $k = 1$, i.e., under the SXDH assumption, and leave the construction of SPS-EQ under the more general Matrix Decision Diffie-Hellman assumption as an interesting open problem.

of the OR-proof and replace it with a QA-NIZK. In the NIZK proof of [GHKP18], we have a permanent CRS including $[\mathbf{D}]_2 \in \mathbb{G}_2^2$ and $[\mathbf{z}]_2 \in \mathbb{G}_2^2$, where $\mathbf{z} \notin \text{span}(\mathbf{D})$ be parameters of the system. On the other hand, their scheme has an updatable CRS including $[\mathbf{z}_0]_2$ and $[\mathbf{z}_1]_2$. Now, given the permanent CRS, the complements of the parts of the updatable CRS are computed in each instance. The idea is that exactly these CRS generate a sound system (i.e., one of the parts of the updatable CRS is outside the span of $[\mathbf{D}]_2$) and in the other case we have a simulatable system (i.e., both parts of the updatable CRS are in the span of $[\mathbf{D}]_2$). As the public parameter $[\mathbf{z}]_2$ is not in the span of $[\mathbf{D}]_2$, we can obtain soundness by letting $[\mathbf{z}_0]_2 = [\mathbf{D}]_2 v$ and $[\mathbf{z}_1]_2 = [\mathbf{z}]_2 - [\mathbf{z}_0]_2$, for $v \xleftarrow{R} \mathbb{Z}_p$, where the sum of them is equal to the value $[\mathbf{z}]_2$, i.e., $[\mathbf{z}_0]_2 + [\mathbf{z}_1]_2 = [\mathbf{z}]_2$. So, it proves that at least one of $[\mathbf{z}_0]_2$ and $[\mathbf{z}_1]_2$ has a part in the span($\mathbf{z}$). The fact that this sum of the updatable CRS is a fixed value is of course not good to enable the randomization of the updatable CRS. To circumvent this state of affairs and obtain malleability, we need to compute a NIZK proof π for $\mathbf{t}, \mathbf{w} \in \text{span}(\mathbf{A_0}) \cup \text{span}(\mathbf{A}_1)$ with the shared updatable CRS, for $\mathbf{t}$ and $\mathbf{w}$, and adapt other proof parts, while we remain sound. Our approach is to set $[\mathbf{z}_0]_2 = [\mathbf{D}]_2 v$ and $[\mathbf{z}_1]_2 = [\mathbf{z}]_2 v$, and give a proof using a one-time homomorphic QA-NIZK due to Jutla and Roy [JR14] that $\mathbf{z}_0 + \mathbf{z}_1$ is in the linear subspace of $\mathbf{D} + \mathbf{z}$. This means that at least one of $[\mathbf{z}_0]_2$ and $[\mathbf{z}_1]_2$ has a part in span($\mathbf{z}$). Fortunately, after this change other parts of the proof adapt properly, and only moving to using a QA-NIZK comes at the cost of having computationally soundness instead of perfect soundness.[7]

For realizing the change representative algorithm ChgRep, our Prove algorithm of the OR-proof computes two proofs with shared randomness and QA-NIZK (where the second proof is part of the tag), which allows to randomize the first proof and update its word. This yields to have randomized signatures output by ChgRep to be distributed identical to a fresh signature for the new representative, i.e., we obtain perfect adaption. As explained above, we use a NIZK OR-proof and a QA-NIZK proof in the construction of the SPS-EQ. In order to guarantee perfect adaption even in front of a signer that generates the keys in a potentially malicious way (i.e., remembers a trapdoor), we need to have a CRS for these proof systems.[8] Consequently, the perfect adaption of our SPS-EQ is guaranteed in the common parameter model where the parameters include a common reference string. However, we stress again that for most applications the CRS generation can simply be part of the key generation and no trusted setup is required.

Comparison with other schemes. In the following Table 1 we provide a comparison of previous SPS-EQ schemes with the one proposed in this paper. We only consider schemes satisfying some reasonable adaption notion, i.e., we exclude the one under q-type assumptions in [FHS15]. We note that while for [FHS14] original and randomized signatures are identical, for [FG18] and our scheme presented in this paper we only consider sizes of randomized signatures, i.e., those output by ChgRep and signatures without the tag respectively. For [FG18] we consider a concrete setting where $\mathcal{U}_{4,2}$-MDDH reduces to the SXDLin assumption [ACD+12], i.e., assuming DLin in $\mathbb{G}_1$ and $\mathbb{G}_2$, and $\mathcal{D}_1$-KerMDH in $\mathbb{G}_2$ reduces to the

[7] Thus, we will formally have a NIZK argument, but in the text we will usually not make a distinction between NIZK proofs and arguments.

[8] Even if all involved proof systems provide zero-knowledge definitions in the style of composable zero-knowledge [GS08], i.e., even if the adversary knows the trapdoor and still simulated and honestly computed proofs cannot be distinguished, we still have the problem of maliciously generated proofs and thus we cannot avoid a CRS.

Scheme	|Signature|	|PK|	Model	Ass.	Loss	A
[FHS14]	$2\|\mathbb{G}_1\| + 1\|\mathbb{G}_2\|$	$\ell\|\mathbb{G}_2\|$	EUF-CMA (strong)	GGM	–	✓✓
[FG18]	$(4\ell+2)\|\mathbb{G}_1\| + 4\|\mathbb{G}_2\|$	$(4\ell+2)\|\mathbb{G}_2\|$	EUF-CoMA (weak)	$\mathcal{D}_{4,2}$-MDDH, $\mathcal{D}_1$-KerMDH	$\mathcal{O}(Q)$	≈
Section 5	$8\|\mathbb{G}_1\| + 9\|\mathbb{G}_2\|$	$3\ell\|\mathbb{G}_2\|$	EUF-CMA (strong)	SXDH	$\mathcal{O}(\log Q)$	✓

Table 1. Comparison of SPS-EQ and EQS Schemes when signing vectors of length ℓ and Q is the number of queries to the signing oracle. **A** means adaption. ✓✓ means perfect adaption under honest and malicious keys; ✓ means perfect adaption under honest keys and under malicious keys in the honest parameters model (i.e., using a CRS); ≈ means adaption under honest keys and honest signatures.

DDH assumption in $\mathbb{G}_2$. For our scheme $k = 1$ and thus we have the $\mathcal{L}_1$-MDDH assumption in $\mathbb{G}_1$ and the $\mathcal{L}_1$-KerMDH assumption in $\mathbb{G}_2$. Latter representing the 1-KerLin assumption which by Lemma 1 is implied by DDH. Consequently, our scheme is secure under SXDH, i.e., assuming DDH in $\mathbb{G}_1$ and $\mathbb{G}_2$.

2 Preliminaries

Notation. Let GGen be a probabilistic polynomial time (PPT) algorithm that on input 1^λ returns a description $\mathcal{G} = (\mathbb{G}, p, P)$ of an additive cyclic group $\mathbb{G}$ of order p for a λ-bit prime p, whose generator is P. We use implicit representation of group elements as introduced in [EHK+17]. For $a \in \mathbb{Z}_p$, define $[a] = aP \in \mathbb{G}$ as the implicit representation of a in $\mathbb{G}$. We will always use this implicit notation of elements in $\mathbb{G}$, i.e., we let $[a] \in \mathbb{G}$ be an element in $\mathbb{G}$, and note that from $[a] \in \mathbb{G}$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}$).

Let BGGen be a PPT algorithm that returns a description $\mathsf{BG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, P_1, P_2, e)$ of an asymmetric bilinear group where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of order p , P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable (non-degenerate) bilinear map and for $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_p$, analogous to above, we write $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$. For two matrices (vectors) $\mathbf{A}, \mathbf{B}$ define $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T \in \mathbb{G}_T$. With $\overline{\mathbf{B}}$ we denote the upper square matrix of $\mathbf{B}$. Let $r \xleftarrow{R} \mathcal{S}$ denotes sampling r from set $\mathcal{S}$ uniformly at random. We denote by λ the security parameter, and by ϵ any negligible function of λ.

Assumptions. We recall the definition of the Matrix Decision Diffie-Hellman assumption [EHK+17] and a natural computational analogue of it, called the Kernel-Diffie-Hellman assumption [MRV16].

Definition 1 (Matrix Distribution). *Let $k \in \mathbb{N}$. We call $\mathcal{D}_k$ a matrix distribution if it outputs matrices in $\mathbb{Z}_q^{(k+1)\times k}$ of full rank k in polynomial time.*

Definition 2 ($\mathcal{D}_k$-Matrix Decision Diffie-Hellman Assumption). *Let $\mathcal{D}_k$ be a matrix distribution. We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-MDDH) Assumption holds relative to* BGGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, we have:*

$$\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) := |\mathsf{Pr}\big[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1\big] - \mathsf{Pr}\big[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1\big]| \leq \epsilon(\lambda)$$

where the probability is taken over $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda), \mathbf{A} \leftarrow \mathcal{D}_k, \mathbf{w} \leftarrow \mathbb{Z}_q^k, \mathbf{u} \leftarrow \mathbb{Z}_q^{k+1}$

Definition 3 (Kernel Matrix Diffie-Hellman Assumption). *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2\}$. We say that the $\mathcal{D}_k$-Kernel Diffie-Hellman Assumption ($\mathcal{D}_k$-KerMDH) holds relative to* BGGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) = \quad \mathsf{Pr}\Big[[\mathbf{c}]_{3-s} \leftarrow \mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s) : \mathbf{c}^\top \mathbf{A} = \mathbf{0} \wedge \mathbf{c} \neq \mathbf{0}\Big] \leq \epsilon(\lambda)$$

where $\mathbf{A} \xleftarrow{R} \mathcal{D}_k$.

Lemma 1 ($\mathcal{D}_k$-MDDH $\implies$ $\mathcal{D}_k$-KerMDH [MRV16]). *Let $k \in \mathbb{N}$ and let $\mathcal{D}_k$ be a matrix distribution. For any PPT adversary $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that* $\mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{B})$.

2.1 Structure-Preserving Signatures on Equivalence Classes

In this section, we recall the definition and the security model of SPS-EQ scheme, as introduced in [HS14]. We note that in order to cover a broader range of potential constructions, we rename the algorithm BGGen that generates the bilinear group BG to ParGen generating public parameters par, i.e., now the parameters par can potentially include additional values such as a common reference string. Moreover, our construction is tag-based where the tag output by Sign is just used as input to ChgRep, where no new tag is output, and required for randomization (for normal SPS-EQ, every occurrence of the tag τ is just ignored).

Definition 4 (SPS-EQ). *A SPS-EQ scheme is tuple of PPT algorithms:*

- $\mathsf{ParGen}(1^\lambda)$. *On security parameter λ and returns* par *including an asymmetric bilinear group* BG. par *is implicitly used as input by all of the algorithms.*
- $\mathsf{KeyGen}(\mathsf{par}, \ell)$*: This algorithm takes* pp *and vector length $\ell > 1$ as input and outputs a key pair* $(\mathsf{sk}, \mathsf{pk})$.
- $\mathsf{Sign}([\mathbf{m}]_i, \mathsf{sk})$*: This algorithm given a representative $[\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell$ for class $[\mathbf{m}]_\mathcal{R}$ and a secret key* sk *outputs a signature $\sigma' = (\sigma, \tau)$ (potentially including a tag τ).*
- $\mathsf{ChgRep}([\mathbf{m}]_i, (\sigma, \tau), \mu, \mathsf{pk})$*: This algorithm on input a representative $[\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell$ and signature σ (and potentially a tag τ), a scalar μ and* pk *as public key, computes an updated signature σ' on new representative $[\mathbf{m}']_i = [\mu\mathbf{m}]_i$ and returns $([\mathbf{m}']_i, \sigma')$.*
- $\mathsf{Verify}([\mathbf{m}]_i, (\sigma, \tau), \mathsf{pk})$*: This verification algorithm when given a representative $[\mathbf{m}]_i$, a signature σ (potentially including a tag τ) and public key* pk*, outputs 1 if it accepts and 0 otherwise.*
- $\mathsf{VKey}(\mathsf{sk}, \mathsf{pk})$*: This algorithm on input key pair* $(\mathsf{sk}, \mathsf{pk})$ *outputs 1 if secret key and public key are consistent and 0 otherwise.*

We recall correctness, EUF-CMA security and the notion of perfect adaption (latter being a stronger notion than the original class-hiding notion which we omit here).

Definition 5 (Correctness). *An* SPS-EQ *over* $(\mathbb{G}_i^*)^\ell$ *correct if for any* $\lambda \in N$*, any* $\ell > 1$*, any* $\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$*, any pair* $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(\mathsf{par}, \ell)$*, any message* $[\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell$ *and any* $\mu \in \mathbb{Z}_p$ *the following holds:*

$$\begin{aligned}&\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1, \text{ and}\\ &\Pr[\mathsf{Verify}([\mathbf{m}]_i, \mathsf{Sign}([\mathbf{m}]_i, \mathsf{sk}), \mathsf{pk}) = 1] = 1, \text{ and}\\ &\Pr[\mathsf{Verify}(\mathsf{ChgRep}([\mathbf{m}]_i, \mathsf{Sign}([\mathbf{m}]_i, \mathsf{sk}), \mu, \mathsf{pk}), \mathsf{pk}) = 1] = 1.\end{aligned}$$

Definition 6 (EU-CMA). *An* SPS-EQ *over* $(\mathbb{G}_i^*)^\ell$ *is* existentially unforgeable under adaptively chosen-message attacks*, if for all* $\ell > 1$ *and PPT adversaries* $\mathcal{A}$ *with access to a signing oracle* $\mathcal{O}^{\mathsf{Sign}}$*, there is a negligible function* $\epsilon(\cdot)$*:*

$$\Pr\left[\begin{array}{l}\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda),\\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(\mathsf{par}, \ell),\\ ([\mathbf{m}]_i^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}}(\mathsf{pk})\end{array} : \begin{array}{r}[\mathbf{m}^*]_\mathcal{R} \neq [\mathbf{m}]_\mathcal{R} \quad \forall [\mathbf{m}]_i \in Q^{\mathsf{Sign}} \quad \wedge\\ \mathsf{Verify}([\mathbf{m}]_i^*, \sigma^*, \mathsf{pk}) = 1\end{array}\right] \leq \epsilon(\lambda),$$

where $Q^{\mathsf{Sign}_\mathcal{R}}$ *is the set of queries that* $\mathcal{A}$ *has issued to the signing oracle* $\mathcal{O}^{\mathsf{Sign}}$*. Note that in the tag-based case this oracle returns* (σ_i, τ_i)*.*

Perfect adaption introduced in [FHS15] by Fuchsbauer et al. requires signatures output by ChgRep are distributed like fresh signatures on the new representative. We present both variants here, as we will require them later. We do not yet adapt them to the tag-based variant of SPS-EQ (this is done afterwards). Note that in the following variant signatures are only required to verify (so may be maliciously computed) while we only consider keys need to satisfy VKey.

Definition 7 (Perfect adaption of signatures). *An* SPS-EQ *over* $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures if for all tuples* $(\mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \mu)$ *with:*

$$\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad \mathsf{Verify}([\mathbf{m}]_i, \sigma, \mathsf{pk}) = 1 \qquad [\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

we have that $\mathsf{ChgRep}([\mathbf{m}]_i, \sigma, \mu, \mathsf{pk})$ *and* $([\mu \cdot \mathbf{m}]_i, \mathsf{Sign}([\mu \cdot \mathbf{m}]_i, \mathsf{sk}))$ *are identically distributed.*

In the subsequent definition, the strongest adaption notion, one in addition to potentially maliciously generated signatures one also considers maliciously generated keys (i.e., does not require that VKey needs to hold).

Definition 8 (Perfect adaption of signatures under malicious keys). *An* SPS-EQ *over* $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures under malicious keys if for all tuples* $(\mathsf{pk}, [\mathbf{m}]_i, \sigma, \mu)$ *with:*

$$[\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mathsf{Verify}([\mathbf{m}]_i, \sigma, \mathsf{pk}) = 1 \qquad \mu \in \mathbb{Z}_p^*$$

we have that ChgRep *outputs* $([\mu \cdot \mathbf{m}]_i, \sigma')$ *such that* σ' *is a random element in the space of signatures, conditioned on* $\mathsf{Verify}([\mu \cdot \mathbf{m}]_i, \sigma', \mathsf{pk}) = 1$*.*

Perfect adaption in context of a CRS and for tag-based SPS-EQ. If par contains a CRS (as in the case of our construction), we need to consider this in the adaption notion. For Definition 7 we just replace $(\mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \mu)$ with $(\mathsf{par}, \mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \mu)$ where $\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$ is honestly generated. We introduce it subsequently, for completeness.

Definition 9 (Perfect adaption in the honest parameter model). *An SPS-EQ scheme* $(\mathsf{ParGen}, \mathsf{Sign}, \mathsf{ChgRep}, \mathsf{Verify}, \mathsf{VKey})$ *perfectly adapts signatures if for all* $(\mathsf{par}, \mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \tau, \mu)$ *with*

$$\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad \mathsf{Verify}([\mathbf{m}]_i, (\sigma, \tau), \mathsf{pk}) = 1 \qquad [\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$
$$\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$$

the following are identically distributed:

$$(\sigma, \mathsf{ChgRep}([\mathbf{m}]_i, \sigma, \tau, \mu, \mathsf{pk})) \text{ and}$$

$$((\sigma', \cdot) \leftarrow \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_i), \mathsf{ChgRep}([\mathbf{m}]_i, \mathsf{Sign}(\mathsf{sk}, [\mu \cdot \mathbf{m}]_i), 1, \mathsf{pk}))$$

Definition 8 does not change and also considers a potentially malicious generation of the parameters which may include a CRS (which is not satisfied by our construction). Moreover, we introduce an intermediate notion, where keys may be generated maliciously, but par is generated honestly. We formally define it in the following for completeness (this is satisfied by our construction).

Definition 10 (Perfect adaption of signatures under malicious keys in the honest parameters model). *An* SPS-EQ *over* $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures under malicious keys in the honest parameter model if for all tuples* $(\mathsf{par}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \tau, \mu)$ *with:*

$$[\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mathsf{Verify}([\mathbf{m}]_i, (\sigma, \tau), \mathsf{pk}) = 1 \qquad \mu \in \mathbb{Z}_p^* \qquad \mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$$

we have that ChgRep *outputs* $([\mu \cdot \mathbf{m}]_i, \sigma')$ *such that* σ' *is a random element in the space of signatures, conditioned on* $\mathsf{Verify}([\mu \cdot \mathbf{m}]_i, \sigma', \mathsf{pk}) = 1$.

2.2 Non-Interactive Zero-Knowledge Proofs

Let $\mathcal{R}_\mathcal{L}$ be an efficiently computable relation of pairs (x, w) of words and witnesses. Let $\mathcal{L}$ be the language defined as $\mathcal{L} = \{x | \exists w : \mathcal{R}_\mathcal{L}(x, w) = 1\}$. We recall the definition of a NIZK proof system [BFM88] for a relation $\mathcal{R}_\mathcal{L}$, where we use the formalization in [GHKP18] (based on [GS08]) for the sake of consistency. We note that we focus on NIZK argument systems, where soundness only holds for computationally bounded adversaries.

- $\mathsf{PGen}(1^\lambda, \mathsf{par})$: On input a security parameter λ and parameters par outputs a common reference string crs.
- $\mathsf{PTGen}(1^\lambda, \mathsf{par})$: On input a security parameter λ and parameters par outputs a common reference string crs and a trapdoor td.
- $\mathsf{PPro}(\mathsf{crs}, x, w)$: On input a common reference string crs, a statement x, and a witness w such that $\mathcal{R}_\mathcal{L}(x, w) = 1$, returns a proof Ω.
- $\mathsf{PVer}(\mathsf{crs}, x, \Omega)$: On input a reference string crs and a proof Ω, Returns accept if Ω is valid and reject otherwise.

– $\mathsf{PSim}(\mathsf{crs}, \mathsf{td}, x)$: On input common reference string crs, and the trapdoor td and word x and outputs a simulated proof Ω.

A NIZK argument system needs to satisfy the following properties:

– **Perfect Completeness:** For all possible public parameters par, all $\lambda \in \mathbb{N}$, all words $x \in \mathcal{L}$, and all witnesses w such that $\mathcal{R}_{\mathcal{L}}(x, w) = 1$, we have

$$\mathsf{Pr}\left[\begin{array}{l}\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\kappa}, \mathsf{par}),\\ \Omega \leftarrow \mathsf{PPro}(\mathsf{crs}, x, w)\end{array} \;:\; \mathsf{PVer}(\mathsf{crs}, x, \Omega) = 1\right] = 1.$$

– **Computational Soundness:** For all PPT adversaries $\mathcal{A}$ and for all words $x \notin \mathcal{L}$ we have:

$$\mathsf{Pr}\left[\begin{array}{l}\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\kappa}, \mathsf{par}),\\ \Omega \leftarrow \mathcal{A}(\mathsf{crs}, x)\end{array} \;:\; \mathsf{PVer}(\mathsf{crs}, x, \Omega) = 0\right] \approx 1.$$

– **Composable Zero-Knowledge:** For all PPT adversaries $\mathcal{A}$, we have

$$\mathsf{Pr}\left[\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\lambda}, \mathsf{par}) \,:\, \mathcal{A}(1^{\lambda}, \mathsf{crs}) = 1\right] \approx$$

$$\mathsf{Pr}\left[(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{PTGen}(1^{\lambda}, \mathsf{par}) \,:\, \mathcal{A}(1^{\lambda}, \mathsf{crs}) = 1\right].$$

Furthermore, for all for all $x \in \mathcal{L}$ with witness w such that $\mathcal{R}_{\mathcal{L}}(x, w) = 1$, the following are identically distributed:

$$\mathsf{PPro}(\mathsf{crs}, x, w) \quad \text{and} \quad \mathsf{PSim}(\mathsf{crs}, \mathsf{td}, x)$$

where $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{PTGen}(1^{\lambda}, \mathsf{par})$. Note that the composable zero knowledge requires indistinguishability even for adversaries that get access to $(\mathsf{crs}, \mathsf{trap})$.

Quasi-Adaptive NIZK proofs. Quasi-Adaptive NIZK (QA-NIZK) proofs [JR13, LPJY14, JR14, KW15, GHR15, AJOR18, DGP+19] are NIZK proofs where the generation of the common reference string (CRS), for a class of languages $\mathcal{L}_\rho$, parametrized by ρ, is allowed to depend on the language parameter ρ. Moreover the common CRS includes a fixed part par, generated by an algorithm pargen. Here, we recall the definitions QA-NIZK proofs, as presented in [KW15].

Definition 11 (QA-NIZK). A non-interactive proof system $(\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prove}, \mathsf{verify}, \mathsf{sim})$ is said to be a QA-NIZK proof system for an ensemble of distributions $\{\mathcal{D}_{\mathsf{par}}\}$ on collection of witness-relations $\mathcal{R} = \{\mathcal{R}_\rho\}$ with associated language parameter ρ if the following holds (cf. [KW15]):

Perfect Completeness: For all λ, all par output by $\mathsf{pargen}(1^\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all (x, y) with $\mathcal{R}_\rho(x, y) = 1$, we have

$$\mathsf{Pr}\left[\begin{array}{l}(\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{crsgen}(\mathsf{par}, \rho),\\ \pi \leftarrow \mathsf{prove}(\mathsf{crs}, x, w)\end{array} \;:\; \mathsf{verify}(\mathsf{crs}, x, \pi) = 1\right] = 1$$

Computational Adaptive Soundness: For all PPT adversaries $\mathcal{A}$,

$$\mathsf{Pr}\left[\begin{array}{l}\rho \leftarrow \mathcal{D}_{\mathsf{par}}, \mathsf{par} \leftarrow \mathsf{pargen}(1^\lambda),\\ \mathsf{crs} \leftarrow \mathsf{crsgen}(\mathsf{par}, \rho),\\ (x, \pi) \leftarrow \mathcal{A}_1(\mathsf{crs}, \mathsf{par}, \rho)\end{array} \;:\; \begin{array}{c}\mathsf{verify}(\mathsf{crs}, x, \pi) = 1 \wedge\\ x \notin \mathcal{L}_\rho\end{array}\right] \leq \epsilon(\lambda)$$

Perfect Zero-Knowledge: For all λ, all par output by $\mathsf{pargen}(1^\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all $(\mathsf{crs}, \mathsf{trap})$ output by $\mathsf{crsgen}(\mathsf{par}, \rho)$, all (x, y) with $\mathcal{R}_\rho(x, y) = 1$, the distributions

$$\mathsf{prove}(\mathsf{crs}, x, w) \quad \text{and} \quad \mathsf{sim}(\mathsf{crs}, \mathsf{td}, x)$$

are identical. Note that the formalization of perfect zero-knowledge is similar to that of composable zero knowledge in [GS08] and requires indistinguishability even for adversaries that get access to $(\mathsf{crs}, \mathsf{trap})$.

2.3 Malleable Proof Systems

Let $\mathcal{R}_\mathcal{L}$ be the witness relation associated to language $\mathcal{L}$, then a controlled malleable proof system [CKLM12] is accompanied by a family of efficiently computable n-ary transformations $T = (T_x, T_w)$ such that for any n-tuple $\{(x_1, w_1), \ldots, (x_n, w_n)\} \in \mathcal{R}^n_\mathcal{L}$ it holds that $(T_x(x_1, \ldots, x_n), T_w(w_1, \ldots, w_n)) \in \mathcal{R}_\mathcal{L}$ (the family of admissible transformations is denoted by $\mathcal{T}$). Intuitively, such a proof system allows when given valid proofs $\{\Omega_i\}_{i\in[n]}$ for words $\{x_i\}_{i\in[n]}$ with associated witnesses $\{w_i\}_{i\in[n]}$ to publicly compute a valid proof Ω for word $x := T_x(x_1, \ldots, x_n)$ corresponding to witness $w := T_w(w_1, \ldots, w_n)$ using an additional algorithm denoted as ZKEval. More formally, the additional algorithms is defined as follows:

- $\mathsf{ZKEval}(\mathsf{crs}, T, (x_i, \Omega_i)_{i\in[n]})$: takes as input common reference string crs, a transformation $T \in \mathcal{T}$, words $x_1, \ldots x_n$ and corresponding proofs $\Omega_1, \ldots, \Omega_2$, and outputs a new word $x' := T_x(x_1, \ldots, x_n)$ and proof Ω'.

It is desirable that proofs computed by applying ZKEval are indistinguishable from freshly computed proofs for the resulting word $x' := T_x(x_1, \ldots, x_n)$ and corresponding witness $w' := T_w(w_1, \ldots, w_n)$ (this property is called (strong) derivation privacy). We recall the weaker notion of derivation privacy below.

Definition 12 (Derivation Privacy [CKLM12]). *A NIZK proof system* $\{\mathsf{PGen}, \mathsf{PTGen}, \mathsf{PPro}, \mathsf{PVer}, \mathsf{PSim}, \mathsf{ZKEval}\}$ *being malleable with respect to a set of transformations* $\mathcal{T}$ *defined on some relation* $\mathcal{R}$ *is derivation private, if for all PPT adversaries* $\mathcal{A}$*,*

$$\Pr\left[\begin{array}{l} \mathsf{crs} \leftarrow \mathsf{PGen}(1^\kappa), b \xleftarrow{R} \{0,1\}, \\ (\mathsf{st}, ((x_i, w_i), \Omega_i)_{i\in[q]}, T) \leftarrow \mathcal{A}(\mathsf{crs}), \\ \mathsf{Return}\ \bot\ \mathsf{if}\ (T \notin \mathcal{T}\ \vee\ \exists i \in [q] : (\mathsf{PVer}(\mathsf{crs}, x_i, \Omega_i) = 0\ \vee \\ (x_i, w_i) \notin \mathcal{R}), \\ \mathsf{Else\ if}\ b = 0 : \Omega \leftarrow \mathsf{PPro}(\mathsf{crs}, T_x((x_i)_{i\in[q]}), T_w((w_i)_{i\in[q]}), \quad : b = b^* \\ \mathsf{Else\ if}\ b = 1 : \Omega \leftarrow \mathsf{ZKEval}(\mathsf{crs}, T, (x_i, \pi_i)_{i\in[q]}), \\ b^* \leftarrow \mathcal{A}(\mathsf{st}, \Omega) \end{array}\right] \leq \epsilon(\lambda)$$

3 Revisiting the FG18 Model and Applications

In this section we recall the construction in [FG18] (denoted FG18 henceforth) and point out some issues regarding their signature adaption notion and the implicitly assumed notion of perfect composition from [HRS15] for concrete applications. We again stress that FG18 scheme is secure in FG18 model (honestly signature and key generation or semi-honest), but

we are going to show its problems in the stronger model, which is current acceptable model. In order to make it more convenient for the reader we adapt the notion used in [FG18] to the original SPS-EQ notion (but keep their name EQS).

First, we recall that their scheme has a one-time randomizability property and therefore FG18 need to modify the perfect adaption notion from [FHS15] (Definition 7 in Section 2.1) to exclude trivial distinguishers, i.e., they always consider the pairs of original and adapted signatures in their distributions. We recall their version in Definition 13. The most important difference[9] is that while the original notion in Definition 7 considers maliciously generated signatures, the definition in [FG18] is restricted to *honestly generated* signatures.

Definition 13 (Signature Adaption [FG18]). *An EQS scheme* $(\mathsf{ParGen}, \mathsf{Sign}, \mathsf{ChgRep}, \mathsf{Verify}, \mathsf{VKey})$ *perfectly adapts signatures if for all* $(\mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \mu)$ *with*

$$\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad [\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

the following are identically distributed:

$$(\rho := \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_i), \mathsf{ChgRep}(\mathsf{pk}, \rho, \mu)) \text{ and}$$

$$(\rho := \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_i), \mathsf{ChgRep}(\mathsf{pk}, \mathsf{Sign}(\mathsf{sk}, [\mu \cdot \mathbf{m}]_i), 1))$$

In Figure 1 we recall the FG18 scheme and then proceed to discuss problems of Definition 13 and their scheme in context of applications.

$\mathsf{Setup}(\mathcal{PG})$:

$\mathbf{A} \xleftarrow{R} \mathcal{D}_{2k,k}, \mathbf{B} \xleftarrow{R} \mathcal{D}_{k'}$
for $i \in [\ell]$ **do**
  $\mathbf{K}_i \xleftarrow{R} \mathbb{Z}_p^{2k \times (k'+1)}$
endfor
$\mathsf{pk} := ([\mathbf{B}]_2, \{[\mathbf{K}_i\mathbf{B}]_2\}_{i\in[\ell]})$
$\mathsf{sk} := (\mathbf{A}, \{\mathbf{K}_i\}_{i\in[\ell]})$
return (pk,sk)

$\mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_1 \in (\mathbb{G}_1^\ell)^*)$:

$\mathbf{U} \xleftarrow{R} \mathsf{GL}_k, \mathbf{S} = \mathbf{AU}$
for $i \in [\ell]$ **do**
  $[\mathbf{S}_i]_1 = [m_i]_1\mathbf{S}$
endfor
$[\mathbf{S}_{\ell+1}]_1 = \sum_{i=1}^{\ell} [m_i]_1\mathbf{K}_i^\top\mathbf{S}$
return $\rho = (\{[\mathbf{S}_i]_1\}_{i\in[\ell+1]}, [\mathbf{S}]_2)$

$\mathsf{ChgRep}(\mathsf{pk}, \rho = (\{[\mathbf{S}_i]_1\}_{i\in[\ell+1]}, [\mathbf{S}]_2), \mu)$:

$\mathbf{r} \xleftarrow{R} (\mathbb{Z}_p^k)^*, [\mathbf{s}]_2 = [\mathbf{S}]_2\mathbf{r}$
for $i \in [\ell+1]$ **do**
  $[\mathbf{s}_i]_1 = \mu[\mathbf{S}_i]_1\mathbf{r}$
endfor
return $\sigma = (\{[\mathbf{s}_i]_1\}_{i\in[\ell+1]}, [\mathbf{s}]_2)$

$\mathsf{Ver}(\mathsf{pk}, [\mathbf{m}]_1, \sigma = (\{[\mathbf{s}_i]_1\}_{i\in[\ell+1]}, [\mathbf{s}]_2)$:

if $[\mathbf{s}]_2 \neq [\mathbf{0}]_2$
  and $\forall i \in [\ell] : [\mathbf{s}_i]_1 \cdot [1]_2 = [m_i]_1 \cdot [\mathbf{s}]_2$
    and $\sum_{i=1}^{\ell} [\mathbf{s}_i^\top]_1 \cdot [\mathbf{K}_i\mathbf{B}]_2 = [\mathbf{s}_{\ell+1}^\top]_1 \cdot [\mathbf{B}]_2$
      return 1
else return 0

Fig. 1. EQS Scheme from [FG18].

[9] One syntactical difference is that for EQS they do not input the message $[\mathbf{m}]_i$ in their ChgRep algorithm, but this does not matter for our discussion.

3.1 Problem With Key Verification and the Need for a CRS

Fuchsbauer and Gay require for signature adaption that the respective EQS scheme provides a VKey algorithm that checks consistency of keys sk and pk. When looking at their keys $\mathsf{pk} := ([\mathbf{B}]_2, \{[\mathbf{K}_i\mathbf{B}]_2\}_{i\in[\ell]})$ and $\mathsf{sk} := (\mathbf{A}, \{\mathbf{K}_i\}_{i\in\ell})$, a potential VKey algorithm can check the consistency of pk with the part of the secret key $\{\mathbf{K}_i\}_{i\in\ell}$. They did not specify the VKey algorithm, but any reasonable VKey would check if sk contains the trapdoor $\mathbf{B}$, as honest keys would not contain it. Now an interesting aspect is that this does not per se present a problem in their definition, as they do not consider perfect adaption under malicious keys (in the vein of Definition 8; cf. Section 2.1). However, the existence of the potential trapdoor $\mathbf{B}$ and no means to proving the absence of it represents a problem with the application of the FG18 scheme to attribute-based credentials (ABCs) (cf. Section 5 in [FG18]).

In the ABC construction from [FHS19], the issuer generates an SPS-EQ key pair and in the Issue protocol, the issuer needs to provide a ZKPoK that $\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1$. Note that for FG18 no realization of this ZKPoK can prove the absence of $\mathbf{B}$ (as the issuer could simply pretend to not knowing it and the ZKPoK cannot cover this) and a malicious issuer may remember $\mathbf{B}$. Now in the anonymity proof of the ABC scheme (Theorem 8 in [FHS19]), the reduction can extract the signing key sk from the ZKPoK and in the transition from $\mathbf{Game}_1$ to $\mathbf{Game}_2$, for all calls to the oracle $\mathcal{O}_{LoR}$ the computation of ChgRep is replaced with Sign of the SPS-EQ, i.e., instead of adapting existing signatures fresh signatures are computed. Now, this is argued under their signature adaption notion. However, without additional means, by the strategy we discuss below (i.e., a way to construct malicious signatures that verify), an adversary can detect with overwhelming probability that the simulation deviates from the original anonymity game and thus this proof breaks down when instantiated with EQS in [FG18]. The reason is, that their adaption notion in Definition 13 is too weak to be useful to constructing ABCs following the approach in [FHS19].

Attack strategy. Let us assume that the adversary who generates the key-pair $\mathsf{pk} = ([\mathbf{B}]_2, \{[\mathbf{K}_i\mathbf{B}]_2\}_{i\in[\ell]})$ and $\mathsf{sk} = (\mathbf{A}, \{\mathbf{K}_i\}_{i\in[\ell]})$ remembers the trapdoor $\mathbf{B}$. For simplicity we set $k = 2$ and $k' = 1$ in Scheme 1 and so we have $\mathbf{B} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$. Let us for the sake of exposition assume that the signer (credential issuer) wants to track a specific instance of signing (issuing) and generates all signatures honestly, except for the one instance (lets say Alice's credential). Latter signature is computed differently by the issuer, but in a way that it is indistinguishable for verifiers, i.e., it still verifies correctly. Actually, instead of computing $\mathbf{S}_{\ell+1} = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix}$ as dictated by the Sign algorithm (cf. Figure 1), he uses $\mathbf{S}_{\ell+1}$ (as in Sign) but also his trapdoor $\mathbf{B}$ to compute $\mathbf{S}'_{\ell+1} = \begin{pmatrix} S_1 - b_2 & S_2 + b_2 \\ S_3 + b_1 & S_4 - b_1 \end{pmatrix}$. Then, he includes $\mathbf{S}'_{\ell+1}$ instead of $\mathbf{S}_{\ell+1}$ in the first part of the signature ρ. Note that we have $\mathbf{S}_{\ell+1}^\top\mathbf{B} = \mathbf{S}_{\ell+1}'^\top\mathbf{B}$, and for a verifier this alternative signature computation is not noticeable. When Alice wants to randomize ρ (i.e., run ChgRep in Figure 1), she chooses $\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^2$ and obtains $\mathbf{s}'_{\ell+1} = \mu\mathbf{S}'_{\ell+1}\mathbf{r} = \mu \begin{pmatrix} (S_1 - b_2)r_1 + (S_2 + b_2)r_2 \\ (S_3 + b_1)r_1 + (S_4 - b_1)r_2 \end{pmatrix}$. Note that the signer knows $\mathbf{K}_i$, and so he can check for any given randomized signature the following:

$$\sum_{i=1}^{\ell} [\mathbf{s}_i^\top]_1 \mathbf{K}_i = [\mathbf{s}_{\ell+1}^\top]_1 \tag{3}$$

which does not use pairing evaluations and thus does not eliminate $\mathbf{B}$. Now it is easy to see that all randomized signatures including the randomized signature issued for Alice pass the original verification using Ver. However, the randomized signature of Alice has an additional part (i.e., $\mathbf{B}$) and so Equation (3) cannot be satisfied. So, the signer can easily distinguish the signature issued to Alice from all other honestly computed signatures.

Trying to fix the problem. A modification of the FG18 scheme to prevent this attack would be to put $[\mathbf{B}]_2$ in a common reference string (CRS) used by all signers when generating their keys so that no signer knows $\mathbf{B}$. As we show subsequently, however, the adaption notion in Definition 13 used for FG18 still remains too weak for ABCs and group signatures.

3.2 Distinguishing Signatures

Now, we show how a malicious signer can distinguish signatures even if keys are generated honestly. In the case of dynamic group signatures (GS) in [DS18] (or ABCs under honest keys), the adversary in the anonymity game is allowed to compute signatures on its own and we will show how this enables the adversary to track signatures, which breaks the anonymity proof. We stress that this attack works independently of whether there is a trapdoor in the secret key, as the GS in [DS18] rely on the BSZ model [BSZ05] and thus assume honest key generation (mitigating the attack in Section 3.1 by construction).

Attack strategy. First we show how a signer who remembers $\mathbf{S}$ during running Sign can obtain the value of $[\mathbf{r}]_2$, which was used as a randomizer for the signature during ChgRep, and then how he can use it to distinguish two signatures. Again, let us set $k = 2$ and $k' = 1$. So, we have $\mathbf{S} = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \\ S_5 & S_6 \\ S_7 & S_8 \end{pmatrix}$, and when ChgRep multiplies $[\mathbf{S}]_2$ on $\mathbf{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, we receive $[\mathbf{s}]_2 = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}_2 = \begin{bmatrix} r_1 S_1 + r_2 S_2 \\ r_1 S_3 + r_2 S_4 \\ r_1 S_5 + r_2 S_6 \\ r_1 S_7 + r_2 S_8 \end{bmatrix}_2$. Taking $[\mathbf{s}]_2$ and $\mathbf{S}$, we compute $[\frac{s_1}{S_1}]_2 - [\frac{s_2}{S_3}]$, and then multiply it to $(\frac{S_2}{S_1} - \frac{S_4}{S_3})^{-1}$ to obtain $[r_2]_2$. Now, we also can recover $[r_1]_2$ and so we obtain $[\mathbf{r}]_2$.

Now, let the signer generate two signatures, say for Alice and Bob, where he later wants to link the received randomized signature to one of them.

The signer picks $\mathbf{S} = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \\ S_5 & S_6 \\ S_7 & S_8 \end{pmatrix}$ for Alice, and picks different S'_5, S'_6, S'_7, S'_8, and sets $\mathbf{S}' = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \\ S'_5 & S'_6 \\ S'_7 & S'_8 \end{pmatrix}$ for Bob in their respective signatures. When the signer receives $[\mathbf{s}]_2$, a candidate for a signature obtained from ChgRep, based on the approach discussed above he obtains $[\mathbf{r}]_2$. Now he checks whether $[s_3]_2 = [r_1 S_5 + r_2 S_6]_2$ holds, in which case the randomized signature is related to Alice. On the other hand, if $[s_3]_2 = [r_1 S'_5 + r_2 S'_6]_2$ holds, then the randomized signature is related to Bob.

3.3 No Perfect Composition

Subsequently, in Definition 14 we recall the perfect composition notion from [HRS15] required to construct VES from SPS-EQ. This notion intuitively requires that ChgRep executed with random coins fixed to 1 updates only the parts of the given signature that are affected by updating the representative from $[\mathbf{m}]_i$ to $\mu[\mathbf{m}]_i$ and not changing the randomness ω previously used by Sign.

Definition 14 (Perfect Composition [HRS15]). *An SPS-EQ scheme* $(\mathsf{ParGen}, \mathsf{Sign}, \mathsf{ChgRep}, \mathsf{Verify}, \mathsf{VKey})$ *allows perfect composition if for all random tapes* ω *and tuples* $(\mathsf{sk}, \mathsf{pk}, [\mathbf{m}]_i, \sigma, \mu)$*:*

$$\mathsf{VKey}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad \sigma \leftarrow \mathsf{Sign}([\mathbf{m}]_i, \mathsf{sk}; \omega) \qquad [\mathbf{m}]_i \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

it holds that $(\mu[\mathbf{m}]_i, \mathsf{Sign}(\mu[\mathbf{m}]_i, \mathsf{sk}; \omega)) = \mathsf{ChgRep}([\mathbf{m}]_i, \sigma, \mu, \mathsf{pk}; 1)$.

Since this notion does not require any assumption on the distribution of original and adapted signatures, the issues discussed so far do not yield to any problem. However, it is quite easy to see that this notion is not satisfied by the FG18 scheme and this is actually an inherent problem for EQS (SPS-EQ) schemes where signatures output by Sign and ChgRep have different forms. To illustrate this for the FG18 scheme (cf. Figure 1), signatures resulting from Sign contain a matrix $[\mathbf{S}]_2$, whereas signatures output by ChgRep contain the vector $[\mathbf{s}]_2 := [\mathbf{S}]_2\mathbf{r}$ (where in context of Definition 14, $\mathbf{r}$ represents the all all-ones vector).

4 Our OR-Proof and Core Lemma

Subsequently, we present the concrete instantiation of our malleable OR-proof that we use for our SPS-EQ scheme. Firstly, PPro computes as a proof two copies Ω_1 and Ω_2 of an OR-proof for statements $[x_1]_1$ and $[x_2]_1$, which use the same randomness v and share a QA-NIZK proof π (denoted by Ω). Consequently, instead of ending up with two independent proofs, we end up with a single proof $\Omega = (\Omega_1 = ([\mathbf{C}_{1,i}]_2, [\mathbf{\Pi}_{1,i}]_1), \Omega_2 = ([\mathbf{C}_{2,i}]_2, [\mathbf{\Pi}_{2,i}]_1), [\mathbf{z}_i]_2, \pi)$ for $i = 0, 1$ where both proofs share $[\mathbf{z}_i]_2$ and π. We also have PVer and PSim which take two statements and proofs with shared randomness and QA-NIZK denoted by π as input. Our ZKEval is restricted to any two words $[\mathbf{x}_1]_1$ and $[\mathbf{x}_2]_1$ corresponding to witnesses r_1 and r_2 where the associated proofs Ω_1 and Ω_2 have been computed using the same randomness v and thus have shared $[\mathbf{z}_i]_2$ and π. The output of ZKEval is a proof $\Omega' = (\Omega_1', [\mathbf{z}_i']_2, \pi')$ for word $[\mathbf{x}_1']_1$ corresponding to witness $r' = r_1 + \psi r_2$ with $\psi \xleftarrow{R} \mathbb{Z}_p$ chosen by ZKEval (i.e., ψ indexes a concrete transformation in the family $\mathcal{T}$). Finally, we also provide a verification algorithm (PRVer) that verifies a single OR-proof (as we use it in the SPS-EQ).

Our OR-proof. Now, we present our malleable proof for OR language $\mathcal{L}^\vee_{\mathbf{A}_0, \mathbf{A}_1}$ based upon the one in [GHKP18]. We recall their NIZK proof as well as the QA-NIZK used by us in our NIZK proof in Appendix A.1. The language is

$$\mathcal{L}^\vee_{\mathbf{A_0}, \mathbf{A_1}} = \{[\mathbf{x}]_1 \in \mathbb{G}_1^{2k} | \exists \mathbf{r} \in \mathbb{Z}_p^k : [\mathbf{x}]_1 = [\mathbf{A_0}]_1 \cdot \mathbf{r} \vee [\mathbf{x}]_1 = [\mathbf{A_1}]_1 \cdot \mathbf{r}\}$$

and $\mathsf{par} := (\mathsf{BG}, [\mathbf{A_0}]_1, [\mathbf{A_1}]_1)$ with $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$ and $\mathbf{A_0}, \mathbf{A_1} \xleftarrow{R} \mathcal{D}_{2k,k}$ for $k \in \mathbb{N}$. We henceforth denote our proof by PS and set $k = 1$ and consider the class of admissible transformations $\mathcal{T} := \{(T_x^\psi, T_w^\psi)\}_{\psi \in \mathbb{Z}_p^*}$ and $T_x^\psi([\mathbf{x}_1]_1, [\mathbf{x}_2]_1) := [\mathbf{x}_1]_1 + \psi[\mathbf{x}_2]_1$ and

$T_w^{\psi}(r_1, r_2) := r_1 + \psi r_2$. Observe that the output of ZKEval is a proof with new randomness $v' = \alpha v$, $s'_0 = \alpha s_{1,0} + \alpha\psi s_{2,0} + \beta_0$ and $s'_1 = \alpha s_{1,1} + \alpha\psi s_{2,1} + \beta_1$ as well as new witness $r' = r_1 + \psi r_2$.

Below, we show that the protocol in Figure 2 is indeed a NIZK argument.

Theorem 1. *The protocol in Figure 2 is a malleable non-interactive zero-knowledge argument for the language $\mathcal{L}^{\vee}_{\mathbf{A}_0,\mathbf{A}_1}$ with respect to allowable transformations $\mathcal{T}$.*

Proof. We need to prove three properties, perfect completeness, composable zero-knowledge, computational soundness and derivation privacy.

Completeness: This is easy to verify.

Zero-Knowledge: The challenger sends an MDDH challenge $([\mathbf{D}]_2, [\mathbf{z}]_2)$ to the adversary $\mathcal{B}$. Then $\mathcal{B}$ picks $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{R} \mathcal{D}_{2,1}$, $\mathbf{A} \xleftarrow{R} \mathcal{D}_1$, $\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{2\times 1}$ and computes $[\mathbf{P}]_2 = [\mathbf{z}^\top + \mathbf{D}^\top]_2\mathbf{K}$ and $\mathbf{C} = \mathbf{K}\overline{\mathbf{A}}$.

Then $\mathcal{B}$ sends $([\mathbf{A}_0]_1, [\mathbf{A}_1]_1, [\mathbf{z}]_2, [\mathbf{D}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$ to $\mathcal{A}$ as crs. When $\mathcal{B}$ receives a real MDDH tuple, where $[\mathbf{z}]_2 = [\mathbf{D}u]_2$ for some $u \in \mathbb{Z}_p$, $\mathcal{B}$ simulates crs as PTGen. In the other case, where $[\mathbf{z}]_2 \xleftarrow{R} \mathbb{G}_2^2$, using the fact that the uniform distribution over $\mathbb{Z}_p^2$ and the uniform distribution over $\mathbb{Z}_p^2 \backslash \mathrm{span}(\mathbf{D})$ are $1/p$-statistically close distributions, since $\mathbf{D}$ is of rank 1, we can conclude that $\mathcal{B}$ simulates the crs as output by PGen, within a $1/p$ statistical distance. Now, note that PPro and PSim compute the vectors $[\mathbf{z}_0]_2$ and $[\mathbf{z}_1]_2$ in the exact same way, i.e., for all $b \in \{0,1\}$, $\mathbf{z}_b := \mathbf{D}v_b$ where v_0, v_1 are uniformly random over $\mathbb{Z}_p$ subject to $v_1 = v_0 u$ (recall $\mathbf{z} := \mathbf{D}u$).

Also for case $j = 1$, on input $[\mathbf{x}_1]_1 := [\mathbf{A}_b r_1]_1$, for some $b \in \{0,1\}$, $\mathsf{PPro}(\mathsf{crs}, [\mathbf{x}_1]_1, [\mathbf{x}_2]_1, r_1, r_2)$ computes $[\mathbf{C}_{1,1-b}]_2$ and $[\Pi_{1,1-b}]_1$ exactly as PSim, that is: $[C_{1,1-b}]_2 = s_{1,1-b}[\mathbf{D}]_2$ and $[\Pi_{1,1-b}]_1 = [\mathbf{A}_{1-b}]_1 s_{1,1-b} - [\mathbf{x}_1]_1 v_{1-b}$. The algorithm PPro additionally computes $[\mathbf{C}_{1,b}]_2 = s_{1,b}[\mathbf{D}]_2 + r_1[\mathbf{z}]_2$ and $[\Pi_{1,b}]_1 = [\mathbf{A}_b]_1 s_{1,b}$, with $s_{1,b} \xleftarrow{R} \mathbb{Z}_p$. Since the following are identically distributed:

$$s_{1,b} \qquad \text{and} \qquad s_{1,b} - r_1 v_b$$

for $s_{1,b} \xleftarrow{R} \mathbb{Z}_p$, we can re-write the commitment and proof computed by PPro as $[\mathbf{C}_{1,b}]_2 = s_{1,b}[\mathbf{D}]_2 - r_1 v_b[\mathbf{D}]_2 + r_1[\mathbf{z}_b]_2 = [s_{1,b}\mathbf{D}]_2$ and $[\Pi_{1,b}]_1 = [\mathbf{A}_b]_1 s_{1,b} - [\mathbf{A}_b r_1 v_b]_2 = [\mathbf{A}_b s_{1,b}]_1 - [\mathbf{x}_1 \mathbf{v}_b]_2$, which is exactly as the output of PSim.

For case $j = 2$ the argumentation is analogous.

Computational Soundness: Based on the computational soundness of the QA-NIZK proofs [KW15], we have $\mathbf{z}_0 + \mathbf{z}_1 \notin \mathit{span}(\mathbf{D})$. So, there is a $b \in \{0,1\}$ such that $\mathbf{z}_b \notin \mathit{span}(\mathbf{D})$. This implies that there exists a $\mathbf{d}^\perp \in \mathbb{Z}_p^2$ such that $\mathbf{D}^\top \mathbf{d}^\perp = 0$, and $\mathbf{z}_b^\top \mathbf{d}^\perp = 1$. Furthermore, as the row vectors of $\mathbf{D}$ together with $\mathbf{z}_b$ form a basis of $\mathbb{Z}_p^2$, we can write $[\mathbf{C}_{j,b}]_2 := [s_{j,b}\mathbf{D} + r_j \mathbf{z}_b]_2$ for some $s_{j,b}, r_j \xleftarrow{R} \mathbb{Z}_p$. Multiplying the verification equation by $\mathbf{d}$ thus yields $[\mathbf{A}_b r_j]_1 = [\mathbf{x}_j]_1$, which proves a successful forgery outside $\mathcal{L}^{\vee}_{\mathbf{A_0},\mathbf{A_1}}$ impossible.

$\mathsf{PGen}(\mathsf{par}, 1^\lambda)$:

$\mathbf{D}, \mathbf{A} \xleftarrow{R} \mathcal{D}_1, \mathbf{z} \xleftarrow{R} \mathbb{Z}_p^2 \setminus \mathrm{span}(\mathbf{D})$
$\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{2\times 1}$
$\mathbf{M} := \mathbf{D} + \mathbf{z}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}$
$\mathbf{C} := \mathbf{K}\overline{\mathbf{A}}$
$\mathsf{crs} = (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$
return crs

$\mathsf{PPro}(\mathsf{crs}, [\mathbf{x}_1]_1, r_1, [\mathbf{x}_2]_1, r_2)$:

Let $b \in \{0,1\}, j \in \{1,2\}$ **s.t.** $[\mathbf{x}_j]_1 = [\mathbf{A_b}]_1 r_j$
$v \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{z}_{1-b}]_2 := v[\mathbf{D}]_2$
$[\mathbf{z}_b]_2 := v[\mathbf{z}]_2$
$\pi := v[\mathbf{P}]_2$
$s_{1,0}, s_{1,1}, s_{2,0}, s_{2,1} \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{C}_{1,b}]_2 := s_{1,b}[\mathbf{D}]_2^\top + r_1[\mathbf{z}_b]_2$
$[\boldsymbol{\Pi}_{1,b}]_1 := [\mathbf{A}_b]_1^\top s_{1,b}$
$[\mathbf{C}_{1,1-b}]_2 := s_{1,1-b}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{1,1-b}]_1 := [\mathbf{A}_{1-b}]_1 \cdot s_{1,1-b} - [\mathbf{x}_1]_1 v$
$[\mathbf{C}_{2,b}]_2 := s_{2,b}[\mathbf{D}]_2^\top + r_2[\mathbf{z}_b]_2$
$[\boldsymbol{\Pi}_{2,b}]_1 := [\mathbf{A}_b]_1^\top s_{2,b}$
$[\mathbf{C}_{2,1-b}]_2 := s_{2,1-b}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{2,1-b}]_1 := [\mathbf{A}_{1-b}]_1 \cdot s_{2,1-b} - [\mathbf{x}_2]_1 v$
$\Omega := ([\mathbf{C}_{j,i}]_2, [\boldsymbol{\Pi}_{j,i}]_1, [\mathbf{z}_i]_2, \pi)_{j\in\{1,2\}, i\in\{0,1\}}$
return Ω

$\mathsf{PVer}(\mathsf{crs}, [\mathbf{x}_1]_1, [\mathbf{x}_2]_1, \Omega)$:

if $e([\overline{\mathbf{A}}]_1, \pi) = e([\mathbf{C}]_1, [\mathbf{z}_1]_2 + [\mathbf{z}_0]_2)$
and for all $i \in \{0,1\}, j \in \{1,2\}$ **it holds**
$e([\mathbf{A}_i]_1, [\mathbf{C}_{j,i}]_2)$
$e([\mathit{\Pi}_{j,i}]_1, [\mathbf{D}]_2^\top) + e([\mathbf{x}_j]_1, [\mathbf{z}_i]_2^\top)$
return 1
else return 0

$\mathsf{PRVer}(\mathsf{crs}, [\mathbf{x}'_1]_1, \Omega'_1)$:

if $e([\overline{\mathbf{A}}]_1, \pi') = e([\mathbf{C}]_1, [\mathbf{z}_1]_2 + [\mathbf{z}_0]_2)$
and for all $i \in \{0,1\}$ **it holds**
$e([\mathbf{A}_i]_1, [\mathbf{C}'_i]_2) =$
$e([\boldsymbol{\Pi}'_i]_1, [\mathbf{D}]_2^\top) + e([\mathbf{x}'_1]_1, [\mathbf{z}'_i]_2^\top)$
return 1
else return 0

$\mathsf{PTGen}(\mathsf{par}, 1^\lambda)$:

$\mathbf{D}, \mathbf{A} \xleftarrow{R} \mathcal{D}_1, u \xleftarrow{R} \mathbb{Z}_p$
$\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{2\times 1}$
$\mathbf{z} := \mathbf{D}u$
$\mathbf{M} := \mathbf{D} + \mathbf{z}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}$
$\mathbf{C} := \mathbf{K}\overline{\mathbf{A}}$
$\mathsf{crs} := (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$
$\mathsf{trap} := (u, \mathbf{K})$
return $(\mathsf{crs}, \mathsf{trap})$

$\mathsf{PSim}(\mathsf{crs}, \mathsf{trap}, [\mathbf{x}_1]_1, [\mathbf{x}_2]_1)$:

$v \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{z}_0]_2 := v[\mathbf{D}]_2$
$[\mathbf{z}_1]_2 := v[\mathbf{z}]_2$
$\pi := v[\mathbf{P}]_2$
$s_{1,0}, s_{1,1}, s_{2,0}, s_{2,1} \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{C}_{1,0}]_2 := s_{1,0}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{1,0}]_1 := [\mathbf{A}_0]_1^\top s_{1,0} - [\mathbf{x}_1]_1 v$
$[\mathbf{C}_{1,1}]_2 := s_{1,1}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{1,1}]_1 := [\mathbf{A}_1]_1 \cdot s_{1,1} - [\mathbf{x}_1]_1 (vu)$
$[\mathbf{C}_{2,0}]_2 := s_{2,0}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{2,0}]_1 := [\mathbf{A}_0]_1^\top s_{2,0} - [\mathbf{x}_2]_1 v$
$[\mathbf{C}_{2,1}]_2 := s_{2,1}[\mathbf{D}]_2^\top$
$[\boldsymbol{\Pi}_{2,1}]_1 := [\mathbf{A}_1]_1 \cdot s_{2,1} - [\mathbf{x}_2]_1 (vu)$
$\Omega := ([\mathbf{C}_{j,i}]_2, [\boldsymbol{\Pi}_{j,i}]_1, [\mathbf{z}_i]_2, \pi)_{j\in\{1,2\}, i\in\{0,1\}}$
return Ω

$\mathsf{ZKEval}(\mathsf{crs}, [\mathbf{x}_1]_1, [\mathbf{x}_2]_1, \Omega)$:

Parse $\Omega = (\Omega_1, \Omega_2, [\mathbf{z}_i]_2, \pi)$
if $\mathsf{PVer}(\mathsf{crs}, [\mathbf{x}_1]_1, [\mathbf{x}_2]_1, \Omega) = 0$
return $\perp$
else $\psi, \alpha, \beta_0, \beta_1 \xleftarrow{R} \mathbb{Z}_p^*$
and for all $b \in \{0,1\}$
$[\mathbf{z}'_b]_2 := \alpha[\mathbf{z}_b]_2$
$[\mathbf{C}'_b]_2 := \alpha[\mathbf{C}_{1,b}]_2 + \alpha\psi[\mathbf{C}_{2,b}]_2 + \beta_b[\mathbf{D}]_2$
$[\boldsymbol{\Pi}'_b]_1 := \alpha[\boldsymbol{\Pi}_{1,b}]_1 + \alpha\psi[\boldsymbol{\Pi}_{2,b}]_1 + \beta_b[\mathbf{A}_b]_1$
$\pi' := \alpha\pi$
$\Omega' := (\Omega'_1, [\mathbf{z}'_i]_2, \pi')$
return Ω'

Fig. 2. Malleable NIZK argument for language $\mathcal{L}^\vee_{\mathbf{A_0}, \mathbf{A_1}}$

Derivation privacy: As can be seen, the algorithm ZKEval outputs a proof with new independent randomness. So, the algorithm ZKEval and the algorithm PPro, when only compute a single proof, have identical distribution, i.e., we have perfect derivation privacy. More precisely, under the CRS $([\mathbf{A}_0]_1, [\mathbf{A}_1]_1, [\mathbf{z}]_2, [\mathbf{D}]_2, [\mathbf{P}]_2)$, a proof $\Omega' = (\Omega'_1, [\mathbf{z}'_i]_2, \pi')$ for word $[\mathbf{x}'_1]_1$ corresponding to witness r' has form $[\mathbf{z}'_{1-b}]_2 = v'[\mathbf{D}]_2$, $[\mathbf{z}'_b]_2 = v'[\mathbf{z}]_2$ and $\pi = v'[\mathbf{P}]_2$, and $[\mathbf{C}'_b]_2 = s'_b[\mathbf{D}]_2^\top + r'[\mathbf{z}'_b]_2$, $[\mathbf{\Pi}'_b]_1 = [\mathbf{A}_b]_1^\top s'_b$, $[\mathbf{C}'_{1-b}]_2 = s'_{1-b}[\mathbf{D}]_2^\top$ and $[\mathbf{\Pi}'_{1-b}]_1 = [\mathbf{A}_{1-b}]_1 \cdot s'_{1-b} - [\mathbf{x}'_1]_1 v'$ for new independent randomness r', v', s'_b, s'_{1-b} and so is a random element in the space of all proofs. Concluding, the proof output by ZKEval is distributed identically to a fresh proof output by PPro. □

4.1 Our Core Lemma

We now give a new core lemma, which we denote by $\mathrm{Exp}^{\mathrm{core}}_\beta$. Note that we set $k = 1$, as it is sufficient for our construction of SPS-EQ. Consider following experiments (for two cases $\beta = 0$ and $\beta = 1$), where $\mathbf{F} : \mathbb{Z}_p \to \mathbb{Z}_p^2$ is a random function computed on the fly:

$\mathrm{Exp}^{\mathrm{core}}_\beta(\lambda), \beta \in \{0,1\}$:

$\mathsf{ctr} := 0$
$\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$
$\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{R} \mathcal{D}_1$
$\mathsf{par} := (\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1)$
$\mathsf{crs} \leftarrow \mathsf{PGen}(\mathsf{par}, 1^\lambda)$
$\mathbf{k}_0, \mathbf{k}_1 \xleftarrow{R} \mathbb{Z}_p^2$
$\mathsf{pp} := (\mathsf{BG}, [\mathbf{A}_0]_1, \mathsf{crs})$
$\mathsf{tag} \leftarrow \mathcal{A}^{\mathsf{TAGO}()}(\mathsf{pp})$
return $\mathsf{VERO}(\mathsf{tag})$

$\mathsf{TAGO}()$:

$\mathsf{ctr} := \mathsf{ctr} + 1$
$r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{t}]_1 := [\mathbf{A}_0]_1 r_1, [\mathbf{w}]_1 := [\mathbf{A}_0]_1 r_2$
$\Omega := (\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi) \leftarrow \mathsf{PPro}(\mathsf{crs}, [\mathbf{t}]_1, r_1, [\mathbf{w}]_1, r_2)$
$[u']_1 := (\mathbf{k}_0 + \beta \cdot \mathbf{F}(\mathsf{ctr}))^\top [\mathbf{t}]_1, [u'']_1 := (\mathbf{k}_0 + \beta \cdot \mathbf{k}_1)^\top [\mathbf{w}]_1$
$\mathsf{Tag} := ([\mathbf{t}]_1, [\mathbf{w}]_1, \Omega = (\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi), [u']_1, [u'']_1)$
return Tag

$\mathsf{VERO}(\mathsf{tag})$:

Parse $\mathsf{tag} = ([\mathbf{t}]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [u']_1)$
if $1 \leftarrow \mathsf{PVer}(\mathsf{crs}, [\mathbf{t}]_1, (\Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi))$
and $\exists \mathsf{ctr}' \leq \mathsf{ctr} : [u']_1 = (\mathbf{k}_0 + \beta \cdot \mathbf{F}(\mathsf{ctr}'))^\top [\mathbf{t}]_1$
return 1
else return 0

Lemma 2 (Core lemma). *If the $\mathcal{D}_1$-MDDH (DDH) assumption holds in $\mathbb{G}_1$ and the tuple of algorithms $(\mathsf{PGen}, \mathsf{PTGen}, \mathsf{PPro}, \mathsf{PVer})$ is a non-interactive zero-knowledge proof system for $\mathcal{L}^\vee_{\mathbf{A}_0, \mathbf{A}_1}$, then going from experiment Exp^{core}_0 to Exp^{core}_1 can (up to negligible terms) only increase the winning chance of an adversary. More precisely, for every adversary $\mathcal{A}$, there exist adversaries $\mathcal{B}$, $\mathcal{B}_1$ and $\mathcal{B}_2$ such that*

$$\mathbf{Adv}^{core}_0(\mathcal{A}) - \mathbf{Adv}^{core}_1(\mathcal{A}) \leq \Delta^{core}_{\mathcal{A}},$$

where

$$\Delta^{core}_{\mathcal{A}} = (2 + 2\lceil \log Q \rceil)\mathbf{Adv}^{\mathsf{zk}}_{\mathsf{PS}}(\mathcal{B}) + (8\lceil \log Q \rceil + 4)\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_1, \mathbb{G}_s}(\mathcal{B}_1)$$
$$2\lceil \log Q \rceil \mathbf{Adv}^{\mathsf{snd}}_{\mathsf{PS}}(\mathcal{B}_2) + \lceil \log Q \rceil \Delta_{\mathcal{D}_1} + \frac{(8\lceil \log Q \rceil + 4)}{p-1} + \frac{(\lceil \log Q \rceil)Q}{p}$$

and the term $\Delta_{\mathcal{D}_1}$ is statistically small.

Due to the lack of space and the similarity of the proof to the approach in [GHKP18] we present the full proof in Appendix B.

5 Our SPS-EQ Scheme

In Figure 3 we present our SPS-EQ scheme in the common parameter model under simple assumptions. We set $k = 1$ as we need randomizability and note that our scheme is based on the malleable OR-proof presented in Section 4. Observe that in ChgRep the new randomness is $v' = \alpha v$, $s'_0 = \alpha\mu s_{1,0} + \alpha\psi s_{2,0} + \beta_0$ and $s'_1 = \alpha\mu s_{1,1} + \alpha\psi s_{2,1} + \beta_1$ and the new witness is $r' = \mu r_1 + \psi r_2$.

$\mathsf{ParGen}(1^\lambda)$:

$\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\kappa)$
$\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{R} \mathcal{D}_1$
$\mathsf{crs} \leftarrow \mathsf{PGen}((\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1), 1^\lambda)$
$\mathsf{par} := (\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1, \mathsf{crs})$
return par

$\mathsf{Sign}([\mathbf{m}]_1, \mathsf{sk})$:

$r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$
$[\mathbf{t}]_1 := [\mathbf{A}_0]_1 r_1$
$[\mathbf{w}]_1 := [\mathbf{A}_0]_1 r_2$
$\Omega \leftarrow \mathsf{PPro}(\mathsf{crs}, [\mathbf{t}]_1, r_1, [\mathbf{w}]_1, r_2)$
Parse $\Omega = (\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi)$
$\mathbf{u}_1 := \mathbf{K}_0^\top [\mathbf{t}]_1 + \mathbf{K}^\top [\mathbf{m}]_1$
$\mathbf{u}_2 := \mathbf{K}_0^\top [\mathbf{w}]_1$
$\sigma := ([\mathbf{u}_1]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$
$\tau := ([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1)$
return (σ, τ)

$\mathsf{Verify}([\mathbf{m}]_1, (\sigma, \tau), \mathsf{pk})$:

Parse $\sigma = ([\mathbf{u}_1]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$
Parse $\tau \in \{([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1) \cup \bot\}$
1: **if** $1 = \mathsf{PVer}(\mathsf{crs}, [\mathbf{t}]_1, (\Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi))$
2: **if** $e([\mathbf{u}_1]_1^\top, [\mathbf{A}]_2) = e([\mathbf{t}]_1^\top, [\mathbf{K}_0\mathbf{A}]_2) + e([\mathbf{m}]_1^\top, [\mathbf{K}\mathbf{A}]_2)$
if $\tau \neq \bot$
3: **if** $1 \leftarrow \mathsf{PVer}(\mathsf{crs}, [\mathbf{w}]_1, (\Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi))$
4: **if** $e([\mathbf{u}_2]_1^\top, [\mathbf{A}]_2) = e([\mathbf{w}]_1^\top, [\mathbf{K}_0\mathbf{A}]_2)$
return 1
return 1
else return 0

$\mathsf{KeyGen}(\mathsf{par}, \ell)$:

$\mathbf{A} \xleftarrow{R} \mathcal{D}_1$
$\mathbf{K}_0 \xleftarrow{R} \mathbb{Z}_p^{2\times 2}$
$\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{\ell\times 2}$
$\mathsf{sk} := (\mathbf{K}_0, \mathbf{K})$
$\mathsf{pk} := ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$
return $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{ChgRep}([\mathbf{m}]_1, \sigma, \tau, \mu, \mathsf{pk})$:

Parse $\sigma = ([\mathbf{u}_1]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$
Parse $\tau = ([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1)$
$\Omega := (\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi)$
if $1 \neq \mathsf{PVer}(\mathsf{crs}, [\mathbf{t}]_1, [\mathbf{w}]_1, \Omega)$
or $e([\mathbf{u}_2]_1^\top, [\mathbf{A}]_2) \neq e([\mathbf{w}]_1^\top, [\mathbf{K}_0\mathbf{A}]_2)$
or $e([\mathbf{u}_1]_1^\top, [\mathbf{A}]_2) \neq e([\mathbf{t}]_1^\top, [\mathbf{K}_0\mathbf{A}]_2) + e([\mathbf{m}]_1^\top, [\mathbf{K}\mathbf{A}]_2)$
return $\bot$
else $\psi, \alpha, \beta_0, \beta_1 \xleftarrow{R} \mathbb{Z}_p^*$
$[\mathbf{u}_1]'_1 := \mu[\mathbf{u}_1]_1 + \psi[\mathbf{u}_2]_1$
$[\mathbf{t}']_1 := \mu[\mathbf{t}]_1 + \psi[\mathbf{w}]_1 = [\mathbf{A}_0]_1(\mu r_1 + \psi r_2)$
for all $b \in \{0, 1\}$
$[\mathbf{z}'_b]_2 := \alpha[\mathbf{z}_b]_2$
$[\mathbf{C}'_b]_2 := \alpha\mu[\mathbf{C}_{1,b}]_2 + \alpha\psi[\mathbf{C}_{2,b}]_2 + \beta_b[\mathbf{D}]_2$
$[\mathbf{\Pi}'_b]_1 := \alpha\mu[\mathbf{\Pi}_{1,b}]_1 + \alpha\psi[\mathbf{\Pi}_{2,b}]_1 + \beta_b[\mathbf{A}_b]_1$
$\pi' := \alpha\pi$
$\Omega' := (\Omega'_1, [\mathbf{z}'_i]_2, \pi')$
$\sigma' := ([\mathbf{u}'_1]_1, \Omega', [\mathbf{t}']_1)$
return $(\mu[\mathbf{m}]_1, \sigma')$

Fig. 3. Our SPS-EQ scheme.

Theorem 2. *If* KerMDH *and* MDDH *assumptions holds, our SPS scheme is unforgeable.*

Proof. We prove the claim by using a sequence of Games and we denote the advantage of the adversary in the j-th game as $\mathbf{Adv}_j$.
Game 0: This game is the original game and we have:

$$\mathbf{Adv}_0 = \mathbf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SPS\text{-}EQ}}(\mathcal{A})$$

Game 1: In this game, in Verify, we replace the verification in line (2:) with the following equation:

$$[\mathbf{u}_1^*]_1 = \mathbf{K_0}^\top[\mathbf{t}^*]_1 + \mathbf{K}^\top[\mathbf{m}^*]_1$$

For any signature $\sigma = ([\mathbf{u}_1^*]_1, \Omega_1^*, [\mathbf{z}_0^*]_2, [\mathbf{z}_1^*]_2, \pi^*, [\mathbf{t}^*]_1)$ that passes the original verification but not verification of Game 1 the value

$$[\mathbf{u}_1^*]_1 - \mathbf{K_0}^\top[\mathbf{t}^*]_1 - \mathbf{K}^\top[\mathbf{m}^*]_1$$

is a non-zero vector in the kernel of $\mathbf{A}$. Thus if $\mathcal{A}$ outputs such a signature, we can construct an adversary $\mathcal{B}$ that breaks the $\mathcal{D}_1$-KerMDH assumption in $\mathbb{G}_2$. To do this we proceed as follows: The adversary $\mathcal{B}$ receives $(\mathsf{BG}, [\mathbf{A}]_2)$, samples all other parameters and simulates Game 1 for $\mathcal{A}$. When $\mathcal{B}$ receives the forgery from $\mathcal{A}$ as tuple $\sigma = ([\mathbf{u}_1^*]_1, \Omega_1^*, [\mathbf{z}_0^*]_2, [\mathbf{z}_1^*]_2, \pi^*, [\mathbf{t}^*]_1)$ for message $[\mathbf{m}^*]_1$, he passes following values to its own challenger:

$$[\mathbf{u}_1^*]_1 - \mathbf{K_0}^\top[\mathbf{t}^*]_1 - \mathbf{K}^\top[\mathbf{m}^*]_1$$

We have:

$$|\mathbf{Adv}_1 - \mathbf{Adv}_0| \leqslant \mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_1,\mathbb{G}_2}(\mathcal{B})$$

Game 2: In this game, we set $\mathbf{K}_0 = \mathbf{K}_0 + \mathbf{k}_0(\mathbf{a}^\perp)^\top$ (in key generation we can pick $\mathbf{k}_0 \in \mathbb{Z}_p^2$ and $\mathbf{K}_0 \in \mathbb{Z}_p^{2\times 2}$ and set $\mathbf{K}_0$; we have $\mathbf{a}^\perp\mathbf{A} = 0$). We compute $[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + \mathbf{K}^\top[\mathbf{m}]_1 + \mathbf{a}^\perp(\mathbf{k}_0)^\top[\mathbf{t}]_1$ and $[\mathbf{u}_2]_1 = \mathbf{K}_0^\top[\mathbf{w}]_1 + \mathbf{a}^\perp(\mathbf{k}_0)^\top[\mathbf{w}]_1$. There is no difference to the previous game since both are distributed identically. So, we have:

$$\mathbf{Adv}_2 = \mathbf{Adv}_1$$

Game 3: In this game, we add the part of $\mathbf{F}(\mathsf{ctr})$ for $\mathsf{ctr} = \mathsf{ctr} + 1$, where $\mathbf{F}$ is a random function, and obtain $[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + \mathbf{K}^\top[\mathbf{m}]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(\mathsf{ctr}))^\top[\mathbf{t}]_1$ and $[\mathbf{u}_2]_1 = \mathbf{K}_0^\top[\mathbf{w}]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{k}')^\top[\mathbf{w}]_1$. In the verification we have:

$$1 \leftarrow \mathsf{PVer}(\mathsf{crs}, [\mathbf{t}]_1, (\Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi)) \quad \text{and}$$
$$\exists \mathsf{ctr}' \leq \mathsf{ctr} :$$
$$[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(\mathsf{ctr}'))^\top + \mathbf{K}^\top[\mathbf{m}]_1$$

Let $\mathcal{A}$ be an adversary that distinguishes between Game 3 and Game 2. We can construct an adversary $\mathcal{B}_1$ that breaks the core lemma. $\mathcal{B}_1$ receives $\mathsf{par} = (\mathsf{BG}, [\mathbf{A}_0]_1, \mathsf{crs})$ from $\mathrm{Exp}^{\mathrm{core}}_{\beta,\mathcal{B}_1}$. $\mathcal{B}_1$ picks $\mathbf{A} \xleftarrow{R} \mathcal{D}_k$, $\boldsymbol{a}^\perp \in \mathrm{orth}(\mathbf{A})$, $\mathbf{K}_0 \xleftarrow{R} \mathbb{Z}_p^{2\times 2}$, $\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{2\times \ell}$, and sends public key $\mathsf{pk} = ([\mathbf{A}_0]_1, [\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$ to $\mathcal{A}$. $\mathcal{B}_1$ uses the oracle $\mathsf{TAGO}()$ to construct the signing algorithm. This oracle takes no input and returns $\mathsf{tag} = ([\mathbf{t}]_1, [\mathbf{w}]_1, \Omega = (\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi), [u']_1, [u'']_1)$. Then $\mathcal{B}_1$ computes $[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + \mathbf{a}^\perp[u']_1 + \mathbf{K}^\top[\mathbf{m}]_1$,

$[\mathbf{u}_2]_1 = \mathbf{K}_0^\top[\mathbf{w}]_1 + \mathbf{a}^\perp[u'']_1$, and sends the signature $\sigma = ([\mathbf{u}_1]_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$ and tag $\tau = ([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1,)$ to $\mathcal{A}$. When the adversary $\mathcal{A}$ sends his forgery $([\mathbf{m}^*]_1, \sigma^*) = (\mathbf{u}_1^*, [\mathbf{t}^*]_1, \Omega_1^*, [\mathbf{z}_0^*]_2, [\mathbf{z}_1^*]_2, \pi^*)$, $\mathcal{B}_1$ returns 0 if $[\mathbf{u}_1]_1 = 0$; otherwise he checks whether there exists $[u'^*]_1$ such that $[\mathbf{u}_1^*]_1 - \mathbf{K}_0^\top[\mathbf{t}^*]_1 - \mathbf{K}^\top[\mathbf{m}^*]_1 = \mathbf{a}^\perp[u'^*]_1$. If it does not hold, then it returns 0 to $\mathcal{A}$, otherwise $\mathcal{B}_1$ computes $[u'^*]_1$, and calls the verification oracle $\mathsf{VERO}()$ on the tag $\mathsf{tag}^* = ([\mathbf{t}^*]_1, \Omega_1^*, [\mathbf{z}_0^*]_2, [\mathbf{z}_1^*]_2, \pi^*, [u'^*]_1)$ and returns the answer to $\mathcal{A}$. Using the core lemma, we have:

$$\mathbf{Adv}_2 - \mathbf{Adv}_3 \leqslant \mathbf{Adv}_{\mathsf{BG}}^{\mathrm{core}}(\mathcal{B}_1)$$

Game 4: In this game, we pick r_1, r_2 from $\mathbb{Z}_p^*$ instead of $\mathbb{Z}_p$. The difference of advantage between Game 3 and Game 4 is bounded by the statistical distance between the two distributions of r_1, r_2. So, under Q adversarial queries, we have:

$$|\mathbf{Adv}_4 - \mathbf{Adv}_3| \leqslant \frac{Q}{p}$$

Game 5: In this game, we pick $\tilde{\mathsf{ctr}} \xleftarrow{R} [1, Q]$, and we add a condition $\mathsf{ctr}' = \tilde{\mathsf{ctr}}$ to verification. Actually, now we have this conditions:

$$1 \leftarrow \mathsf{PVer}(\mathsf{pk}, [\mathbf{t}]_1, (\Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi)) \quad \text{and}$$

$$\exists \mathsf{ctr}' \leq \mathsf{ctr} : \mathsf{ctr}' = \tilde{\mathsf{ctr}} \quad \text{and}$$

$$[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(\mathsf{ctr}'))^\top + \mathbf{K}^\top[\mathbf{m}]_1$$

Since the view of the adversary is independent of $\tilde{\mathsf{ctr}}$, we have

$$\mathbf{Adv}_5 = \frac{\mathbf{Adv}_4}{Q}$$

Game 6: In this game, we can replace $\mathbf{K}$ by $\mathbf{K} + \mathbf{v}(\mathbf{a}^\perp)^\top$ for $\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^\ell$. Also, we replace $\{\mathbf{F}(i) : i \in [1, Q], i \neq \tilde{\mathsf{ctr}}\}$ by $\{\mathbf{F}(i) + \mathbf{w}_i : i \in [1, Q], i \neq \tilde{\mathsf{ctr}}\}$, for $\mathbf{w}_i \xleftarrow{R} \mathbb{Z}_p^{2k}$ and $i \neq \hat{\mathsf{ctr}}$. So, in each i-th query, where $i \neq \hat{\mathsf{ctr}}$, we compute

$$[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + (\mathbf{K}^\top + \mathbf{a}^\perp\mathbf{v}^\top)[\mathbf{m}_i]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(i) + \mathbf{w}_i)^\top[\mathbf{t}]_1$$

Also, for $\tilde{\mathsf{ctr}}$-th query for the message $[\mathbf{m}_{\tilde{\mathsf{ctr}}}]_1$, we compute

$$[\mathbf{u}_1]_1 = \mathbf{K}_0^\top[\mathbf{t}]_1 + (\mathbf{K}^\top + \mathbf{a}^\perp\mathbf{v}^\top)[\mathbf{m}_{\tilde{\mathsf{ctr}}}]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(\tilde{\mathsf{ctr}}) + \mathbf{w}_i)^\top[\mathbf{t}]_1$$

So, $\mathcal{A}$ must compute the following:

$$[\mathbf{u}_1^*]_1 = \mathbf{K}_0^\top[\mathbf{t}^*]_1 + (\mathbf{K}^\top + \mathbf{a}^\perp\mathbf{v}^\top)[\mathbf{m}^*]_1 + \mathbf{a}^\perp(\mathbf{k}_0 + \mathbf{F}(\tilde{\mathsf{ctr}}) + \mathbf{w}_i)^\top[\mathbf{t}^*]_1$$

Since $\mathbf{m}^* \neq [\mathbf{m}_{\tilde{\mathsf{ctr}}}]_{\mathcal{R}}$ (in different classes) by definition of the security game, we can argue $\mathbf{v}^\top\mathbf{m}^*$ and $\mathbf{v}^\top\mathbf{m}_{\tilde{\mathsf{ctr}}}$ are two independent values, uniformly random over $\mathbb{G}_1$. So, $\mathcal{A}$ only can guess it with probability of $\frac{1}{p}$. So, we have

$$\mathbf{Adv}_{\mathsf{SPS\text{-}EQ}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{A}) \leqslant \mathbf{Adv}_{\mathsf{BG}}^{\mathsf{KerMDH}}(\mathcal{B}) + \mathbf{Adv}_{\mathsf{BG}}^{core}(\mathcal{B}_1) + \frac{2Q}{p}.$$

Theorem 3. *Our scheme satisfies perfect adaption under malicious keys in the honest parameters model, i.e., Definition 10.*

Proof. For any message $[\mathbf{m}]_1$, and pk which is generated according to the CRS $([\mathbf{A}]_2, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1, [\mathbf{z}]_2, [\mathbf{D}]_2, [\mathbf{P}]_2)$, a signature $\sigma = ([\mathbf{u}_1]_1, \Omega, [\mathbf{t}]_1,)$ satisfying the verification algorithm must be of the form $\sigma = (\mathbf{K}_0^\top[\mathbf{A}_0]_1 r + \mathbf{K}^\top[\mathbf{m}]_1, v[\mathbf{z}]_2, v[\mathbf{D}]_2, v[\mathbf{P}]_2, s_0[\mathbf{D}^\top] + rv[\mathbf{z}]_2, s_1[\mathbf{D}^\top]_2, [\mathbf{A}_0]_1 s_0, [\mathbf{A}_1]_1 s_1 - [\mathbf{A}_0]_1 rv, [\mathbf{A}_0]_1 r)$. A signature output by ChgRep has the form $\sigma' = (\mathbf{K}_0^\top[\mathbf{A}_0]_1 r' + \mathbf{K}^\top[\mathbf{m}]_1, v'[\mathbf{z}]_2, v'[\mathbf{D}]_2, v'[\mathbf{P}]_2, s_0'[\mathbf{D}^\top] + r'v'[\mathbf{z}]_2, s_1'[\mathbf{D}^\top]_2, [\mathbf{A}_0]_1 s_0', [\mathbf{A}_1]_1 s_1 - [\mathbf{A}_0]_1 r'v', [\mathbf{A}_0]_1 r')$ for new independent randomness r', v', s_0', s_1' and so is a random element in the space of all signatures. Actually, the signature output by ChgRep is distributed identically to a fresh signature on message $[\mathbf{m}]_1$ output by Sign. □

6 Applications

As already discussed in [FG18], there are no known applications of SPS-EQ where signatures that have been randomized need to be randomized again by an entity that does not know the original signature. Consequently, and as shown in [FG18], tag-based schemes as the one introduced in this paper can be used within all the known applications without restrictions. Now let us summarize and clarify how our SPS-EQ scheme can be used in existing applications of SPS-EQ.

Using our scheme we can instantiate the group signatures in [DS18] and [BHKS18] as well as access control encryption (ACE) in [FGKO17]. As already mentioned earlier, both models assume honest key generation and so we can merge ParGen and KeyGen of the SPS-EQ scheme and do not need a trusted party to generate the CRS, i.e., it can be done by the signer during key generation.

Also we can instantiate attribute-based credentials [HS14, FHS14, FHS19] in the honest key model or under malicious keys (for latter requiring a CRS), but not in the malicious key model without a CRS. Due to an argumentation following a reasoning related to the one in Section 3.3, our scheme cannot be used to instantiate the verifiable encrypted signatures from [HRS15].

Round-optimal blind signatures in the CRS model. What remains to be discussed is the application to round-optimal blind signatures as introduced in [FHS15, FHKS16]. As already mentioned, as our SPS-EQ scheme does not provide the strongest notion of perfect adaption under malicious keys, we are only able to construct round-optimal blind signatures in the CRS model. In contrast to existing schemes in the CRS model relying on non-standard and non-static q-type assumptions such as [Fuc09, AO09] which require around 30 group elements in the signature, the most recent scheme under standard assumptions, i.e., SXDH, by Abe et al. [AJOR18] requires $(42, 40)$ elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. In contrast to other existing schemes which follow the framework of Fischlin [Fis06], we can take our SPS-EQ scheme to instantiate the framework in [FHS15]. We note that when we are in the CRS model, we can move the commitment parameters Q and $\hat{Q}$ from [FHS15] in the CRS, and thus obtain a round optimal blind signature scheme under SXDH. This is the same assumption as used by Abe et al. in [AJOR18], but our signature sizes are only $(10, 9)$ elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, improving over [AJOR18] by about a factor of 4 and even beating constructions proven secure under q-type assumptions.

Acknowledgments. We are grateful to the anonymous reviewers from ASIACRYPT 2019 and Romain Gay for their careful reading of the paper, their valuable feedback and suggestions to improve the presentation. We also thanks Carla Ràfols and Alonso González for their comments on earlier versions of this work. This work was supported by the EUs Horizon 2020 ECSEL Joint Undertaking project SECREDAS under grant agreement n°783119 and by the Austrian Science Fund (FWF) and netidee SCIENCE project PROFET (grant agreement P31621-N38).

References

ACD+12. Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24. Springer, Heidelberg, December 2012.

ACHO11. Masayuki Abe, Sherman SM Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-trapdoor anonymous tags for traceable signatures. In *International Conference on Applied Cryptography and Network Security*, pages 183–200. Springer, 2011.

AFG+10. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In *Annual Cryptology Conference*, 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, Heidelberg, August 2011.

AGOT14. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 688–712. Springer, Heidelberg, February 2014.

AHN+17. Masayuki Abe, Dennis Hofheinz, Ryo Nishimaki, Miyako Ohkubo, and Jiaxin Pan. Compact structure-preserving signatures with almost tight security. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 548–580. Springer, Heidelberg, August 2017.

AJOR18. Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 627–656. Springer, Heidelberg, December 2018.

ALP12. Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Computing on authenticated data: New privacy definitions and constructions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 367–385. Springer, 2012.

ALSZ18. Behzad Abdolmaleki, Helger Lipmaa, Janno Siim, and Micha Zajc. On qa-nizk in the bpk model. Cryptology ePrint Archive, Report 2018/877, 2018.

AO09. Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 435–450. Springer, Heidelberg, December 2009.

BCF+11. Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In *International Conference on Cryptology in Africa*, pages 206–223. Springer, 2011.

BCG+15. Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer, and Madars Virza. Secure sampling of public parameters for succinct zero knowledge proofs. In *2015 IEEE Symposium on Security and Privacy*, pages 287–304. IEEE Computer Society Press, May 2015.

BFM88. Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th ACM STOC*, pages 103–112. ACM Press, May 1988.

BFS16. Mihir Bellare, Georg Fuchsbauer, and Alessandra Scafuro. NIZKs with an untrusted CRS: Security in the face of parameter subversion. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 777–804. Springer, Heidelberg, December 2016.

BGG19. Sean Bowe, Ariel Gabizon, and Matthew D. Green. A multi-party protocol for constructing the public parameters of the pinocchio zk-SNARK. In Aviv Zohar, Ittay Eyal, Vanessa Teague, Jeremy Clark, Andrea Bracciali, Federico Pintore, and Massimiliano Sala, editors, *FC 2018 Workshops*, volume 10958 of *LNCS*, pages 64–77. Springer, Heidelberg, March 2019.

BGM17. Sean Bowe, Ariel Gabizon, and Ian Miers. Scalable multi-party computation for zk-snark parameters in the random beacon model. *IACR Cryptology ePrint Archive*, 2017:1050, 2017.

BHJ+15. Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, and Yong Li. Tightly-secure authenticated key exchange. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 629–658. Springer, Heidelberg, March 2015.

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, Heidelberg, December 2018.

BHS18. Michael Backes, Lucjan Hanzlik, and Jonas Schneider. Membership privacy for fully dynamic group signatures. Cryptology ePrint Archive, Report 2018/641, 2018. https://eprint.iacr.org/2018/641.

BKP14. Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (hierarchical) identity-based encryption from affine message authentication. In *International Cryptology Conference*, pages 408–425. Springer, 2014.

BLL+19. X. Bultel, P. Lafourcade, R. W. F. Lai, G. Malavolta, D. Schröder, and S. A. Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. to appear at PKC 2019, 2019.

BSZ05. Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, Heidelberg, February 2005.

CKLM12. Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable proof systems and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–300. Springer, 2012.

CL19. Elizabeth C. Crites and Anna Lysyanskaya. Delegatable anonymous credentials from mercurial signatures. In *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, pages 535–555, 2019.

CLY09. Julien Cathalo, Benoît Libert, and Moti Yung. Group encryption: Non-interactive realization in the standard model. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 179–196. Springer, 2009.

CS18. Remi Clarisse and Olivier Sanders. Short group signature in the standard model. *IACR Cryptology ePrint Archive*, 2018:1115, 2018.

CW13. Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Heidelberg, August 2013.

DGP+19. Vanesa Daza, Alonso González, Zaira Pindado, Carla Ráfols, and Javier Silva. Shorter quadratic qa-nizk proofs. In *IACR International Workshop on Public Key Cryptography*. Springer, 2019.

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, Heidelberg, December 2015.

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, April 2018.

EHK+17. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Rafols, and Jorge 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 *IACR International Workshop on Public Key Cryptography*, 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, Heidelberg, March 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, Heidelberg, August / September 2016.

FHS14. Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. Cryptology ePrint Archive, Report 2014/944, 2014.

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, Heidelberg, August 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, April 2019.

Fis06. Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 60–77. Springer, Heidelberg, August 2006.

Fuc09. Georg Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009. http://eprint.iacr.org/2009/320.

Fuc11. Georg Fuchsbauer. Commuting signatures and verifiable encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 224–245. Springer, 2011.

GH08. Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 179–197. Springer, 2008.

Gha16. Essam Ghadafi. Short structure-preserving signatures. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of *LNCS*, pages 305–321. Springer, Heidelberg, February / March 2016.

Gha17. Essam Ghadafi. More efficient structure-preserving signatures - or: Bypassing the type-III lower bounds. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *ESORICS 2017, Part II*, volume 10493 of *LNCS*, pages 43–61. Springer, Heidelberg, September 2017.

GHK17. Romain Gay, Dennis Hofheinz, and Lisa Kohl. Kurosawa-desmedt meets tight security. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 133–160. Springer, Heidelberg, August 2017.

GHKP18. Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan. More efficient (almost) tightly secure structure-preserving signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 230–258. Springer, 2018.

GHKW16. Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly CCA-secure encryption without pairings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 1–27. Springer, Heidelberg, May 2016.

GHR15. Alonso González, Alejandro Hevia, and Carla Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 605–629. Springer, Heidelberg, November / December 2015.

GJ18. Kristian Gjøsteen and Tibor Jager. Practical and tightly-secure digital signatures and authenticated key exchange. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 95–125. Springer, Heidelberg, August 2018.

GKM+18. Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers. Updatable and universal common reference strings with applications to zk-SNARKs. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 698–728. Springer, Heidelberg, August 2018.

GS08. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.

HHK18. Julia Hesse, Dennis Hofheinz, and Lisa Kohl. On tightly secure non-interactive key exchange. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 65–94. Springer, Heidelberg, August 2018.

HJ12. Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Heidelberg, August 2012.

HJ16. Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. *Designs, Codes and Cryptography*, 80(1):29–61, 2016.

HJP18. Dennis Hofheinz, Dingding Jia, and Jiaxin Pan. Identity-based encryption tightly secure under chosen-ciphertext attacks. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 190–220. Springer, Heidelberg, December 2018.

HKS15. Dennis Hofheinz, Jessica Koch, and Christoph Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 799–822. Springer, Heidelberg, March / April 2015.

Hof17. Dennis Hofheinz. Adaptive partitioning. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 489–518. Springer, Heidelberg, April / May 2017.

HPP19. Chlo Hbant, Duong Hieu Phan, and David Pointcheval. Linearly-homomorphic signatures and scalable mix-nets. Cryptology ePrint Archive, Report 2019/547, 2019.

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, Heidelberg, September 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, Heidelberg, December 2014.

JOR18. Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure structure-preserving signatures. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 123–152. Springer, Heidelberg, March 2018.

JR13. Charanjit S Jutla and Arnab Roy. Shorter quasi-adaptive nizk proofs for linear subspaces. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 1–20. Springer, 2013.

JR14. Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Heidelberg, August 2014.

JR17. Charanjit S. Jutla and Arnab Roy. Improved structure preserving signatures under standard bilinear assumptions. In Serge Fehr, editor, *PKC 2017, Part II*, volume 10175 of *LNCS*, pages 183–209. Springer, Heidelberg, March 2017.

KPW15. Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 275–295. Springer, Heidelberg, August 2015.

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015.

Lip19. Helger Lipmaa. Key-and-argument-updatable qa-nizks. Cryptology ePrint Archive, Report 2019/333, 2019.

LPJY13. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Linearly homomorphic structure-preserving signatures and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 289–307. Springer, Heidelberg, August 2013.

LPJY14. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, Heidelberg, May 2014.

LPY15. Benoît Libert, Thomas Peters, and Moti Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 296–316. Springer, Heidelberg, August 2015.

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, Heidelberg, December 2016.

Ràf15. Carla Ràfols. Stretching groth-sahai: Nizk proofs of partial satisfiability. In *Theory of Cryptography Conference*, pages 247–276. Springer, 2015.

A OR-NIZK and QA-NIZK Proofs

A.1 A Concrete OR-Proof

We recall a NIZK for an OR-language presented in [Ràf15, GHKP18] in Figure 4. The language is

$$\mathcal{L}^{\vee}_{\mathbf{A_0},\mathbf{A_1}} = \{[\mathbf{x}]_1 \in \mathbb{G}_1^{2k} | \exists \mathbf{r} \in \mathbb{Z}_p^k : [\mathbf{x}]_1 = [\mathbf{A_0}]_1 \cdot \mathbf{r} \vee [\mathbf{x}]_1 = [\mathbf{A_1}]_1 \cdot \mathbf{r}\}$$

and the instantiation is as follows, where $\mathsf{par} := (\mathsf{BG}, [\mathbf{A_0}]_1, [\mathbf{A_1}]_1)$ with $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$ and $\mathbf{A_0}, \mathbf{A_1} \xleftarrow{R} \mathcal{D}_{2k,k}$ for $k \in \mathbb{N}$.

$\mathsf{PGen}(1^\lambda, \mathsf{par})$:

$\mathbf{D} \xleftarrow{R} \mathcal{D}_k$
$\mathbf{z} \xleftarrow{R} \mathbb{Z}_p^{k+1}$
$\mathsf{crs} = (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2)$
return crs

$\mathsf{PPro}(\mathsf{crs}, [\mathbf{x}]_1, \mathbf{r})$:

Let $b \in \{0,1\}$ **s.t.** $[\mathbf{x}]_1 = [\mathbf{A}_b]_1\mathbf{r}$
$\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^k$
$[\mathbf{z}_{1-b}]_2 := [\mathbf{D}]_2 \cdot \mathbf{v}$
$[\mathbf{z}_b]_2 := [\mathbf{z}]_2 - [\mathbf{z}_{1-b}]_2$
$\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{R} \mathbb{Z}_p^{k\times k}$
$[\mathbf{C}_b]_2 := \mathbf{S}_b[\mathbf{D}]_2^\top + \mathbf{r} \cdot [\mathbf{z}_b]_2$
$[\mathbf{\Pi}_b]_1 := [\mathbf{A}_b]_1^\top \cdot \mathbf{S}_b$
$[\mathbf{C}_{1-b}]_2 := \mathbf{S}_{1-b}[\mathbf{D}]_2^\top$
$[\mathbf{\Pi}_{1-b}]_1 := [\mathbf{A}_{1-b}]_1 \cdot \mathbf{S}_{1-b} - [\mathbf{x}]_1 \cdot \mathbf{v}^\top$
$\pi = ([\mathbf{z}_0]_2, ([\mathbf{C}_i]_2, [\mathbf{\Pi}_i]_1))_{i\in\{0,1\}}$
return π

$\mathsf{PVer}(\mathsf{crs}, [\mathbf{x}]_1, \pi)$:

$[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$
if for all $i \in \{0,1\}$ **it holds**
$e([\mathbf{A}_i]_1, [\mathbf{C}_i]_2) = e([\mathit{\Pi}_i]_1, [\mathbf{D}]_2^\top) + e([\mathbf{x}]_1, [\mathbf{z}_i]_2^\top)$
return 1
else return 0

$\mathsf{PTGen}(1^\lambda, \mathsf{par})$:

$\mathbf{D} \xleftarrow{R} \mathcal{D}_k$
$\mathbf{u} \xleftarrow{R} \mathbb{Z}_p^k$
$\mathbf{z} = \mathbf{D} \cdot \mathbf{u}$
$\mathsf{crs} = (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2)$
$\mathsf{trap} = \mathbf{u}$
return $(\mathsf{crs}, \mathsf{trap})$

$\mathsf{PSim}(\mathsf{crs}, \mathsf{trap}, [\mathbf{x}]_1)$:

$\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^k$
$[\mathbf{z}_0]_2 := [\mathbf{D}]_2 \cdot \mathbf{v}$
$[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$
$\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{R} \mathbb{Z}_p^{k\times k}$
$[\mathbf{C}_0]_2 := \mathbf{S}_0[\mathbf{D}]_2^\top$
$[\mathbf{\Pi}_0]_1 := [\mathbf{A}_0]_1\mathbf{S}_0 - [\mathbf{x}]_1 \cdot \mathbf{v}^\top$
$[\mathbf{C}_1]_2 := \mathbf{S}_1[\mathbf{D}]_2^\top$
$[\mathbf{\Pi}_1]_1 := [\mathbf{A}_1]_1 \cdot \mathbf{S}_1 - [\mathbf{x}]_1 \cdot (\mathbf{u} - \mathbf{v})^\top$
$\pi = ([\mathbf{z}_0]_2, ([\mathbf{C}_i]_2, [\mathbf{\Pi}_i]_1))_{i\in\{0,1\}}$
return π

Fig. 4. NIZK for language $\mathcal{L}^{\vee}_{\mathbf{A_0},\mathbf{A_1}}$

A.2 Efficient QA-NIZK for WS Distributions

In [JR13], Jutla and Roy introduced very efficient QA-NIZK proofs for languages $\{\mathcal{L}_{[\mathbf{M}]_1}\}$ that are linear subspaces of a vector space. In this setting, language members have the form

$[\mathbf{M}\boldsymbol{x}]_1$, with parameters sampled from a probability distribution $\mathcal{D}_{\mathsf{par}}$, parametrized by a string ρ with an associated language $\mathcal{L}_\rho$ and with soundness under a MDH assumption. Later, Kiltz and Wee improved on this work, generalized the work of [LPJY14, JR14] and proved soundness under the weaker KerMDH assumption. Here, we recall the construction of a QA-NIZK, as proposed in [KW15].

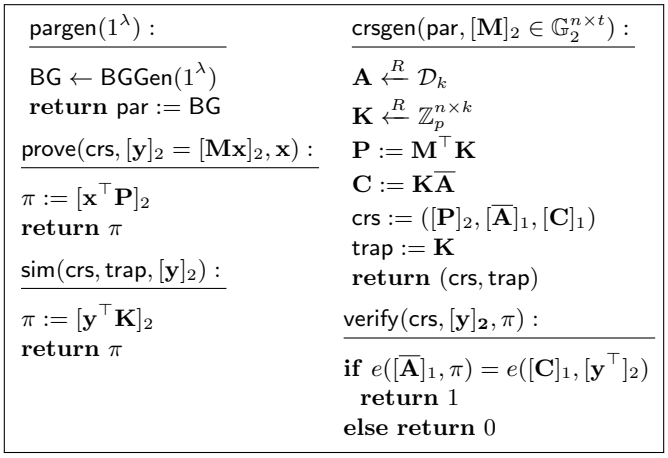

Fig. 5. QA-NIZK from [KW15]

Theorem 4 ([KW15]). *The protocol in Figure 5 is a Quasi-adaptive Non-Interactive Zero-Knowledge Argument. Suppose in addition that $\mathcal{D}_{par}$ is a witness sampleable distribution. Then, under the $\mathcal{D}_k$-KerMDH assumption in $\mathbb{G}_1$, the protocol has adaptive soundness.*

B Proof of the Core Lemma

Proof. We proceed with a sequence of games, where our proof follows (in parts verbatim) the approach in [GHKP18]:

Game 0: We have Game 0 = $\mathrm{Exp}_0^{\mathrm{core}}$ and thus by definition:

$$\mathbf{Adv}_0 = \mathbf{Adv}_0^{\mathrm{core}}(\mathcal{A})$$

Game 1: In this game, we use PSim instead of PPro to compute the proof. Game 1 is as Game 0, except that crs is generated by PTGen instead of PGen. Because the output of PSim and PPro are identically distributed on a crs generated by PTGen, we can argue that the crs distribution is the only difference in these two games. This difference is justified by the zero-knowledge of PS. Namely, we build an adversary $\mathcal{B}$ on the composable zero-knowledge property of PS as follows. The adversary $\mathcal{B}$ obtains crs from its own experiment instead of calling PGen, samples $\mathbf{A}_0 \xleftarrow{R} \mathcal{D}_1$, and forwards par := (BG, $[\mathbf{A}_0]_1$, crs) to $\mathcal{A}$. Then $\mathcal{B}$ samples $\mathbf{k}_0, \mathbf{k}_1 \xleftarrow{R} \mathbb{Z}_p^2$, thanks to which it can answer TAGO and VERO queries. Note that $\mathcal{B}$ simulates

Game 0 in case it was given crs generated by PGen, whereas it simulates Game 1 in case it was given crs generated by PTGen. Thus, $\mathcal{B}$ is such that $T(\mathcal{B}) \approx T(\mathcal{A}) + Q \cdot \mathrm{poly}(\lambda)$ and

$$|\mathbf{Adv}_0 - \mathbf{Adv}_1| \leq \mathbf{Adv}^{\mathsf{zk}}_{\mathsf{PS}}(\mathcal{B})$$

Game 2: In this game we pick $[\mathbf{t}]_1, [\mathbf{w}]_1 \xleftarrow{R} \mathbb{G}_1^2$ instead of computing it as in the previous game. We can switch $[\mathbf{t}]_1$ and $[\mathbf{w}]_1$ to random over $\mathbb{G}_1^2$ by applying the $\mathcal{D}_1$-MDDH assumption. More precisely, let $\mathcal{A}$ be an adversary distinguishing between Game 1 and Game 2 and let $\mathcal{B}_1$ be an adversary given two Q-fold $\mathcal{D}_1$-MDDH challenge $(\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{z}_1]_1, \ldots, [\mathbf{z}_q]_1)$ and $(\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{z}'_1]_1, \ldots, [\mathbf{z}'_q]_1)$ as input. Now $\mathcal{B}_1$ sets up the game for $\mathcal{A}$ similar to Game 1, but instead choosing $\mathbf{A}_0 \xleftarrow{R} \mathcal{D}_1$, it uses its challenge matrix $[\mathbf{A}_0]_1$ as part of the public parameters par. Further, to answer tag queries $\mathcal{B}_1$ sets $[\mathbf{t}_i]_1 := [\mathbf{z}_i]_1$, and $[\mathbf{w}_i]_1 := [\mathbf{z}'_i]_1$ and computes the rest accordingly. This is possible as the proof Ω is simulated from Game 1 on. In case $\mathcal{B}_1$ was given a real $\mathcal{D}_1$-MDDH challenge, it simulates Game 1 and otherwise Game 2. There is an adversary $\mathcal{B}_1$ with $T(\mathcal{B}_1) \approx T(\mathcal{A}) + Q \cdot \mathrm{poly}(\lambda)$ and

$$|\mathbf{Adv}_1 - \mathbf{Adv}_2| \leq 2\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_1, \mathbb{G}_s}(\mathcal{B}_1) + \frac{2}{p-1}$$

Game 3.0: In this game, we compute $[u']_1 = (\mathbf{k}_0 + \mathbf{F}_i(\mathsf{ctr}_{|i})[\mathbf{t}]_1$ (in this game for $i = 0$, and we have a random function $\mathbf{F}_i$ on i-bit prefixes, and the i-bit prefix $\mathsf{ctr}_{|i}$ of ctr), and $[u'']_1 = (\mathbf{k}_0 + \mathbf{k}'_0)[\mathbf{w}]_1$ (where $\mathbf{k}'_0 = \mathbf{F}_0(\mathsf{ctr}_{|0}))$. In the verification algorithm also, we verify $[u']_1 = (\mathbf{k}_0 + \mathbf{F}_i(\mathsf{ctr}'_{|i})[\mathbf{t}]_1$ for $\mathsf{ctr}' \leq \mathsf{ctr}$, and $[u'']_1 = (\mathbf{k}_0 + \mathbf{k}'_0)[\mathbf{w}]_1$. As for all $\mathsf{ctr} \in \mathbb{N}$ we have $\mathbf{F}_0(\mathsf{ctr}_{|0}) = \mathbf{F}_0(\epsilon)$ and $\mathbf{k}_0$ is distributed identically to $\mathbf{k}_0 + \mathbf{F}_0(\epsilon)$ for $\mathbf{k}_0 \xleftarrow{R} \mathbb{Z}_p^2$ we have

$$\mathbf{Adv}_{3.0} = \mathbf{Adv}_2$$

Game 3.i $\rightarrow$ Game 3.(i+1): We proceed via a series of hybrid games $H_{i.j}$ for $i \in [0, \log(Q) - 1], j \in [1, 8]$, in the following. We mark the advantage of the hybrid game by a prime.

Game 3.i $\rightarrow$ $H_{i.1}$: In this game, we compute $[\mathbf{t}]_1 = [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_{1.i}$ and $[\mathbf{w}]_1 = [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_{2.i}$, instead of picking them randomly. Here, ctr_{i+1} is the $i+1$'st bit of the binary representation of ctr. More precisely, we introduce an intermediary game $H_{i.0}$, where we choose $[\mathbf{t}_i]_1$ and $[\mathbf{w}_i]_1$ as

$$[\mathbf{t}_i]_1 = \begin{cases} [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_{1.i} \text{ for } r_{1.i} \xleftarrow{R} \mathbb{Z}_p, & \text{if } \mathsf{ctr}_{i+1} = 0 \\ [\mathbf{u}_i]_1 \text{ for } \mathbf{u}_i \xleftarrow{R} \mathbb{Z}_p^2, & \text{otherwise} \end{cases}$$

$$[\mathbf{w}_i]_1 = \begin{cases} [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_{2.i} \text{ for } r_{2.i} \xleftarrow{R} \mathbb{Z}_p, & \text{if } \mathsf{ctr}_{i+1} = 0 \\ [\mathbf{u}'_i]_1 \text{ for } \mathbf{u}'_i \xleftarrow{R} \mathbb{Z}_p^2, & \text{otherwise} \end{cases}$$

Let $\mathcal{A}$ be an adversary distinguishing between Game 3.i and $H_{i.0}$ and let $\mathcal{B}_1$ be an adversary receiving two Q-fold $\mathcal{D}_1$-MDDH challenges $(\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{z}_1]_1, \ldots, [\mathbf{z}_Q]_1)$ and $(\mathsf{BG}, [\mathbf{A}_0]_1, [\mathbf{z}'_1]_1, \ldots, [\mathbf{z}'_Q]_1)$. Then $\mathcal{B}_1$ sets up the game for $\mathcal{A}$ similar to Game 3.i, where he embeds $[\mathbf{A_0}]_1$ into the public parameters pars. Further, whenever obtaining a simulation query ctr with $\mathsf{ctr}_{i+1} = 0$, $\mathcal{B}_1$ sets $[\mathbf{t}_i]_1 := [\mathbf{z}_i]_1$ and $[\mathbf{w}_i]_1 := [\mathbf{z}'_i]_1$ and otherwise follows Game 3.i. Similar, we can reduce the transition from game $H_{i.0}$ to $H_{i.1}$ to the MDDH assumption. We have

$$|\mathbf{Adv}_{3.i} - \mathbf{Adv}'_{i.1}| \leq 4\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_1,\mathbb{G}_s}(\mathcal{B}_1) + \frac{4}{p-1}$$

$H_{i.1} \to H_{i.2}$: In this step we reverse the transition from Game 0 to Game 1. Namely, we generate crs again using PGen instead of PTGen, and we use the fact that proofs generated by PPro or PSim are identically distributed when $\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, \mathsf{par})$. Note that it is possible to use the algorithm PPro, as from game $H_{i.1}$ on, we choose all $[\mathbf{t}]_1, [\mathbf{w}]_1$ in tag queries from $\mathcal{L}^\vee_{\mathbf{A_0},\mathbf{A_1}}$ with corresponding witness and can thus honestly generate proofs. Therefore,

$$|\mathbf{Adv}'_{i.2} - \mathbf{Adv}'_{i.1}| \leq \mathbf{Adv}^{\mathsf{zk}}_{\mathsf{PS}}(\mathcal{B}_2)$$

$H_{i.2} \to H_{i.3}$: From game $H_{i.3}$ on we introduce an additionally check in the verification oracle. Namely, VERO checks that $[\mathbf{t}]_1, [\mathbf{w}]_1 \in \mathrm{span}([\mathbf{A}_0]_1) \vee \mathrm{span}([\mathbf{A}_1]_1)$. As the crs is generated by PGen, we can employ the soundness of PS to obtain

$$|\mathbf{Adv}'_{i.3} - \mathbf{Adv}'_{i.2}| \leq \mathbf{Adv}^{\mathsf{snd}}_{\mathsf{PS}}(\mathcal{B}_2)$$

$H_{i.3} \to H_{i.4}$: Let $\mathbf{A}_0^\perp \in \mathrm{orth}(\mathbf{A}_0)$ and $\mathbf{A}_1^\perp \in \mathrm{orth}(\mathbf{A}_1)$. We introduce an intermediary game $H_{i.3.1}$, where we replace the random function $\mathbf{F}_i : \{0,1\}^i \to \mathbb{Z}_p^2$ by

$$\mathbf{F}'_i : \{0,1\}^i \to \mathbb{Z}_p^2, \;\; \mathbf{F}'_i(\nu) := (\mathbf{A}_0^\perp | \mathbf{A}_1^\perp)(\Gamma_i(\nu) \;\; \Upsilon_i(\nu))^\top$$

where $\nu \leftarrow \{0,1\}^i$ is an i-bit string and $\Gamma_i, \Upsilon_i : \{0,1\}^i \to \mathbb{Z}_p$ are two independent random functions. With probability $1 - \Delta_{\mathcal{D}_1}$ the matrix $(\mathbf{A}_0^\perp | \mathbf{A}_1^\perp)$ has full rank. In this case, going from game $H_{i.3}$ to game $H_{i.3.1}$ consists merely in a change of basis, thus, these two games are perfectly indistinguishable. We obtain

$$|\mathbf{Adv}'_{i.3.1} - \mathbf{Adv}'_{i.3}| \leq \Delta_{\mathcal{D}_1}$$

We now define

$$\mathbf{F}_{i+1} : \{0,1\}^{i+1} \to \mathbb{Z}_p^2,$$
$$\mathbf{F}_{i+1}(\nu) := \begin{cases} (\mathbf{A}_0^\perp | \mathbf{A}_1^\perp)(\Gamma'_i(\nu_{|i}) \;\; \Upsilon_i(\nu_{|i}))^\top, & \text{if } \nu_{i+1} = 0 \\ (\mathbf{A}_0^\perp | \mathbf{A}_1^\perp)(\Gamma_i(\nu_{|i}) \;\; \Upsilon'_i(\nu_{|i}))^\top, & \text{otherwise} \end{cases}$$

where $\Gamma'_i, \Upsilon'_i : \{0,1\}^i \to \mathbb{Z}_p$ are fresh independent random functions. Now $\mathbf{F}_{i+1}$ constitutes a random function $\{0,1\}^{i+1} \to \mathbb{Z}_p^2$. Replacing $\mathbf{F}'_i(\mathsf{ctr}_{|i})$ by $\mathbf{F}_{i+1}(\mathsf{ctr}_{|i+1})$ does not show up in any of the tag queries, as we have

$$\mathbf{F}_{i+1}(\mathsf{ctr}_{|i+1})^\top [\mathbf{t}]_1 = \mathbf{F}_{i+1}(\mathsf{ctr}_{|i+1})^\top [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_1 = ... = \mathbf{F}'_i(\mathsf{ctr}_{|i})^\top [\mathbf{A}_{\mathsf{ctr}_{i+1}}]_1 r_1$$

In the verification oracle we check $[\mathbf{t}]_1, [\mathbf{w}]_1 \in \mathrm{span}([\mathbf{A}_0]_1) \vee \mathrm{span}([\mathbf{A}_1]_1)$, define $d_{[\mathbf{t}]} = 0$ if $\mathbf{t} \in \mathrm{span}(\mathbf{A}_0)$ and $d_{[\mathbf{t}]} = 1$ if $\mathbf{t} \in \mathrm{span}(\mathbf{A}_1)$ and replace $\mathbf{F}_i(\mathsf{ctr}_{|i})$ by $\mathbf{F}_{i+1}(\mathsf{ctr}_{|i} | d_{[\mathbf{t}]})$. Thus, by similar reasoning as for tag queries, the change does not show up in the final verification query either. Altogether, we obtain

$$|\mathbf{Adv}'_{i.4} - \mathbf{Adv}'_{i.3}| \leq \Delta_{\mathcal{D}_1}$$

$H_{i.4} \to H_{i.5}$: From game $H_{i.5}$ on, we extend the set $\mathcal{S}$ in the verification oracle from $\mathcal{S}_{i.4} := \mathbf{F}_{i+1}(\mathsf{ctr}'_{|i} | d_{[\mathbf{t}]}) : \mathsf{ctr}' \leq \mathsf{ctr}$ to $\mathcal{S}_{i.5} := \mathbf{F}_{i+1}(\mathsf{ctr}'_{|i} | b) : \mathsf{ctr}' \leq \mathsf{ctr}, b \in \{0,1\}$. That is, we

regard a verification query $([\mathbf{t}]_1, [\mathbf{w}]_1, \Omega, [u']_1, [u'']_1)$ as valid, if there exists a $\mathsf{ctr}' \leq \mathsf{ctr}$ such that $[u']_1 = (\mathbf{k}_0 + \mathbf{F}_{i+1}(\mathsf{ctr}'_{|i}|b)^\top [\mathbf{t}]_1$ for $b \in \{0,1\}$ arbitrary, instead of requiring $b = d_{[\mathbf{t}]}$. As changing the verification oracle does not change the view of the adversary before providing its output and as we have $\mathcal{S}_{i.4} \subseteq \mathcal{S}_{i.5}$, the transition from game $H_{i.4}$ to game $H_{i.5}$ can only increase the chance of the adversary. We thus have

$$\mathbf{Adv}'_{i.4} \leq \mathbf{Adv}'_{i.5}$$

$H_{i.5} \to H_{i.6}$: The difference between game $H_{i.5}$ and game $H_{i.6}$ is that in the latter we only regard a verification query $([\mathbf{t}]_1, [\mathbf{w}]_1, \Omega, [u']_1, [u'']_1)$ valid, if there exists a $\mathsf{ctr}' \leq \mathsf{ctr}$ such that $[u']_1 = (\mathbf{k}_0 + \mathbf{F}_{i+1}(\mathsf{ctr}'_{|i}|\mathsf{ctr}'_{i+1})^\top [\mathbf{t}]_1$ (instead of allowing the last bit to be arbitrary). As the only way an adversary can learn the image of $\mathbf{F}_{i+1}$ on a value is via tag queries and $\mathbf{F}_{i+1}$ is a random function, a union bound over the elements in $\mathcal{Q}_{\mathsf{tag}}$ yields

$$|\mathbf{Adv}'_{i.5} - \mathbf{Adv}'_{i.6}| \leq \frac{Q}{p}$$

$H_{i.6} \to H_{i.7}$: The oracle VERO does not perform the additional check $[\mathbf{t}]_1, [\mathbf{w}]_1 \in \mathrm{span}([\mathbf{A}_0]_1) \vee \mathrm{span}([\mathbf{A}_1]_1)$ anymore from game $H_{i.7}$ on. This is justified by the soundness of PS. As in transition $H_{i.2} \to H_{i.3}$ we obtain

$$|\mathbf{Adv}'_{i.6} - \mathbf{Adv}'_{i.7}| \leq \mathbf{Adv}^{\mathsf{snd}}_{\mathsf{PS}}(\mathcal{B}_2)$$

$H_{i.7} \to H_{i.8}$: This transition is similar to transition Game 0 to Game 1. We use PTGen to generate crs. Namely, for an adversary $\mathcal{A}$ distinguishing the two games, we can employ the composable zero-knowledge property of PS to obtain an adversary $\mathcal{B}_2$ such that

$$|\mathbf{Adv}'_{i.7} - \mathbf{Adv}'_{i.8}| \leq \mathbf{Adv}^{\mathsf{zk}}_{\mathsf{PS}}(\mathcal{B}_2)$$

$H_{i.8} \to$ **Game 3.(i+1)**: We switch $[\mathbf{t}]_1, [\mathbf{w}]_1$ generated by TAGO to uniformly random over $\mathbb{G}_1^2$, using the MDDH assumption first on $[\mathbf{A}_0]_1$, then on $[\mathbf{A}_1]_1$. Similarly than for the transition **Game 3.i** $\to H_{i.1}$, we obtain

$$|\mathbf{Adv}_{3.(i+1)} - \mathbf{Adv}'_{i.8}| \leq 4\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_1,\mathbb{G}_s}(\mathcal{B}_1) + \frac{4}{p-1}$$

Game 3.($\log(Q)$**)** $\to \mathbf{Exp}^{\mathbf{core}}_{1,\mathcal{A}}$: It is left to reverse the changes introduced in the transitions from game Game 0 to Game 2 to end up at the experiment $\mathrm{Exp}^{\mathrm{core}}_{1,\mathcal{A}}$. In order to do so we introduce an intermediary Game 4, where we set $[\mathbf{t}]_1 := [\mathbf{A}_0]_1 r_1$ and $[\mathbf{w}]_1 := [\mathbf{A}_0]_1 r_2$ for $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$. This corresponds to reversing transition Game 1 to Game 2. By the same reasoning for every adversary $\mathcal{A}$ we thus obtain

$$|\mathbf{Adv}_{3.(\log(Q))} - \mathbf{Adv}_4| \leq 2\mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_1,\mathbb{G}_s}(\mathcal{B}_1) + \frac{2}{p-1}$$

As $[\mathbf{t}]_1, [\mathbf{w}]_1$ are now chosen from $\mathrm{span}([\mathbf{A}_0]_1)$ again, we can switch back to honest generation of the common reference string crs. As in transition of Game 0 to Game 1 for an adversary $\mathcal{A}$ we obtain

$$|\mathbf{Adv}_4 - \mathbf{Adv}^{\mathrm{core}}_1| \leq \mathbf{Adv}^{\mathsf{zk}}_{\mathsf{PS}}(\mathcal{B}_2)$$

□