Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials

Georg Fuchsbauer[1], Christian Hanser[2], and Daniel Slamanig[2]

[1] Inria, ENS, CNRS and PSL Research University, Paris, France
georg.fuchsbauer@ens.fr

[2] IAIK, Graz University of Technology, Austria
{christian.hanser|daniel.slamanig}@iaik.tugraz.at

Abstract. Structure-preserving signatures (SPS) are a powerful building block for cryptographic protocols. We introduce SPS on equivalence classes (SPS-EQ), which allow joint randomization of messages and signatures. Messages are projective equivalence classes defined on group element vectors, so multiplying a vector by a scalar yields a different representative of the same class. Our scheme lets one adapt a signature for one representative to a signature for another representative without knowledge of any secret; and given a signature, an adapted signature for a different representative is indistinguishable from a fresh signature on a random message. We propose a definitional framework for SPS-EQ and an efficient construction in Type-3 bilinear groups, which we prove secure against generic forgers.

We also introduce a set-commitment scheme that lets one open subsets of the committed set. From this and SPS-EQ we then build an efficient multi-show attribute-based anonymous credential system for an arbitrary number of attributes. Our ABC system avoids costly zero-knowledge proofs and only requires a short interactive proof to thwart replay attacks. It is the first credential system whose bandwidth required for credential showing is independent of the number of its attributes, i.e., constant-size. We propose strengthened game-based security definitions for ABC and prove our scheme anonymous against malicious organizations in the standard model; finally, we give a concurrently secure variant in the CRS model.

Keywords: Public-key cryptography, structure-preserving signatures, attribute-based anonymous credentials, set commitments

1 Introduction

Digital signatures are an important cryptographic primitive that provide a means for integrity protection, non-repudiation and authenticity of messages in a publicly verifiable way. In most signature schemes, the message space consists of integers in $\mathbb{Z}_{\mathrm{ord}(\mathbb{G})}$ for some group $\mathbb{G}$, or of arbitrary strings mapped to either integers in $\mathbb{Z}_{\mathrm{ord}(\mathbb{G})}$ or elements of a group $\mathbb{G}$ via a cryptographic hash function. In the latter case, the hash function is often modeled as a random oracle (thus, one effectively signs random group elements).

In contrast, structure-preserving signature (SPS) schemes [Fuc09, AHO10, AFG+10, AGHO11, ACD+12, AGOT14a, AGOT14b, BFF+15, KPW15, Gha16] sign group elements without requiring any prior encoding. In particular, SPS are defined over two groups $\mathbb{G}_1$ and $\mathbb{G}_2$, equipped with a bilinear map (pairing), and messages are vectors of group elements (from either $\mathbb{G}_1$ or $\mathbb{G}_2$, or both). Moreover, public keys and signatures also consist of group elements only and signatures are verified by deciding group membership of their elements and evaluating the pairing on elements from the public key, the message and the signature. Fully SPS schemes [AKOT15, Gro15] also require the secret key to consist of group elements.

Randomization is a useful feature of signature schemes that lets anyone transform one signature into a new one that looks like a freshly generated signature on the same message. There have been various constructions of randomizable signatures [CL03, CL04, BBS04, Wat05, PS16] and SPS schemes supporting some types of randomization (inner, sequential, etc.) [AFG^{+}10, AGOT14b].

In this paper, we extend this randomization, in particular, we construct SPS schemes that in addition to randomizing signatures also enable randomization of the signed *messages* in particular ways, and adaptation of the corresponding signatures. As we show, such signature schemes are particularly interesting for applications in privacy-enhancing cryptographic protocols.

1.1 Contribution

Our contributions can be broken down as follows: (1) Introduction and instantiation of SPS on equivalence classes (SPS-EQ), which are defined on group element vectors; (2) a randomizable set commitment scheme that enables constant-size opening of subsets of the committed set; and building on these primitives (3) a new construction approach for multi-show attribute-based anonymous credentials, which we efficiently instantiate and analyze in a comprehensive security model we propose.

Structure-Preserving Signature Scheme on Equivalence Classes. Inspired by randomizable signatures, we introduce a variant of SPS. Instead of signing message vectors as in previous SPS schemes, our variant signs classes of a projective equivalence relation $\mathcal{R}$ defined over $\mathbb{G}^{\ell}$ with $\ell > 1$. These classes are lines going through the origin and are determined by the mutual ratios of the discrete logarithms of the vector components. By multiplying each component by the same scalar, a different representative of the same equivalence class is obtained. If the DDH assumption holds in group $\mathbb{G}$ then it is hard to decide whether two vectors belong to the same equivalence class.

In SPS-EQ an equivalence class is signed by signing an arbitrary representative of the class. From this signature one can later derive a signature for any other representative of the same class, without having access to the secret key. Unforgeability for SPS-EQ is defined with respect to classes. Thus, after obtaining signatures on representatives of its choice, no adversary should be able to compute a signature on a representative of a class that is different from the ones signed. We also require that adaptation of signatures leads to freshly distributed ones; in combination with unlinkability of equivalence classes this implies the following: given a representative and a signature on it, a random representative of the same class and an adapted signature on it are indistinguishable from a completely random message and a fresh signature on it.

We present a definitional framework for SPS-EQ including game-based security definitions and present an efficient construction whose signatures are short and their length is independent of the message-vector length ℓ. We prove our construction secure in the generic-group model.

Set Commitments. We propose a new type of commitment scheme that lets one commit to sets and open arbitrary subsets. We first propose a model for this primitive and then give an efficient construction, which we prove secure in this model. It lets one commit to subsets of $\mathbb{Z}_p$ and a commitment and a subset-opening both consist of a single bilinear-group element. Our scheme is computationally binding, perfectly hiding, and computationally subset-sound, meaning that given a commitment to a set S it is hard to produce a subset-opening for some $T \not\subseteq S$. We prove security under a generalization of the strong Diffie-Hellman assumption [BB04].

The scheme also enables commitment randomization, which is compatible with the randomization of our SPS-EQ scheme (i.e., multiplication by a scalar). Randomization is perfect and the witness used for subset opening can be consistently adapted. This property has not been achieved by existing constructions (cf. Section 1.2) without relying on costly zero-knowledge proofs of randomization.

A Multi-Show Attribute-Based Anonymous Credential System. *Attribute-based anonymous credentials* provide means for anonymous authentication. A credential system is a multi-party protocol involving a user, an organization (or issuer) and a verifying party. The user can obtain a credential on multiple attributes, such as her nationality or age, from an organization and present the credential to some verifier later on, revealing only certain attributes. While not learning any information about the user *(anonymity)*, the verifier can still be sure that presented information (the shown attributes) is authentic *(unforgeability)*. In a *multi-show* credential system, a user obtains a credential from an organization, typically in a non-anonymous way, and can later perform an arbitrary number of unlinkable showings.

We propose a new way of building multi-show attribute-based anonymous credentials (often called Privacy-ABCs; we simply write ABCs) from SPS-EQ and set commitments. Using our instantiations, we construct the first standard-model multi-show ABC with anonymity holding against malicious organization keys.

An SPS-EQ scheme allows to randomize a vector of group elements together with a signature on it, a property we use to achieve unlinkability of credential showings. We use set commitments to commit to a user's attributes. To issue a credential, the issuer signs a message vector containing this set commitment; the credential is essentially this signature together with its message. During a showing, a subset of the issued attributes can then be opened. Unlinkability of showings is achieved via the rerandomization properties of both the signature scheme and the set-commitment scheme, whose rerandomizations are compatible with each other. Furthermore, to thwart replay attacks of showings, we add a short constant-size proof of knowledge, which guarantees freshness.

We emphasize that our approach to constructing ABCs differs considerably from existing ones, as we do not use zero-knowledge proofs to selectively disclose attributes during showings. This makes *constant-size* showings possible, as achieved by our construction. In particular, the size of credentials as well as the bandwidth required when showing a credential are independent of the number of possible attributes as well as those contained in the credential; it is a small constant number of group elements. This is the first ABC system with this feature. We note that Camenisch et al. [CDHK15] recently proposed an approach with identical asymptotic complexity (see Section 5.7 for details).

We introduce a game-based security model for ABCs in the vein of the Bellare, Shi and Zhang's [BSZ05] model for group signatures and prove our ABC system secure in it. We note that there are no other comprehensive models for attribute-based credential systems (apart from independently developed very strong simulation-based notions in [CKL+14, CDHK15]). Our model considers replays and provides a strong form of anonymity against organizations that may generate malicious keys—both of which are not considered by earlier models. Replay attacks have often been considered an implementation issue, but we believe that such attacks should already be considered in the formal analysis, avoiding from the beginning problems that might later appear within an implementation.

We note that the independently proposed formal model by Camenisch et al. [CKL+14] and the ABC construction in [CDHK15]—using a different model—do consider replays and malicious keys too, although the former in a seemingly weaker sense and the latter only assuming a CRS.

Finally, we discuss a variant of our scheme with smaller organization key sizes that is concurrently secure in the CRS model. We provide a comparison of our ABC system to other existing multi- and one-show ABC approaches.

1.2 Related Work

Signatures. Blazy et al. [BFPV11] introduce a new primitive, termed *signatures on randomizable ciphertexts* for which they modify Waters' signature scheme [Wat05]. Given a signature on a ciphertext, anyone can randomize the ciphertext and adapt the signature accordingly, knowing neither signing key nor encrypted message. Their construction is only practical for very small message spaces, which makes it unsuitable for our purposes.

Another related approach is the proofless variant of the Chaum-Pedersen signature [CP93], used for self-blindable certificates by Verheul [Ver01]. The certificate as well as the initial message can be randomized using the same scalar, preserving the validity of the certificate. This approach works for the construction in [Ver01], but (as also observed in [Ver01]) it is not a secure signature scheme due to its homomorphic property and the possibility of efficient existential forgeries.

Linearly homomorphic signatures [BFKW09, CFW12, Fre12] allow to sign any subspace of a vector space by publishing a signature for every basis vector with respect to the same (file) identifier; this identifier "glues" together the single vectors (of a file). Given a sequence of scalar/signature pairs $(\beta_i, \sigma_i)_{i\in[\ell]}$ for vectors $\boldsymbol{v}_i$ (with the same identifier), one can publicly compute a signature for the vector $\boldsymbol{v} = \sum_{i\in[\ell]} \beta_i \boldsymbol{v}_i$.

If one uses a different identifier for every signed vector $\boldsymbol{v}$ then such signatures would support a functionality similar to signature adaptation in SPS-EQ, that is, publicly compute signatures for vectors $\boldsymbol{v}' = \beta\boldsymbol{v}$ (although they are not structure-preserving). Various constructions also provide a privacy feature called strongly/completely context-hiding [ALP12, ALP13], requiring that a signature resulting from homomorphic operations is indistinguishable from a fresh one. Nevertheless, homomorphic signatures do not help in our context: for SPS-EQ unforgeability, we must prevent combination of signatures on several (independent) vectors; so every vector must be assigned a unique identifier. Then however, our unlinkability notion cannot be satisfied as every signature can be linked to its initial signature via the unique identifier. The same arguments also apply to structure-preserving linearly homomorphic signatures [LPJY13]. Homomorphic signatures supporting richer classes of admissible functions (beside linear ones) have also been considered, but are not applicable in our context either (cf. [ABC$^+$12, ALP12] for an overview). We note that the general framework of *P-homomorphic signatures* [ABC$^+$12, ALP12] is related to our approach in terms of unforgeability and privacy guarantees, but there are no existing instantiations for the functionality that we require (and we find our formalization more natural).

Chase et al. [CKLM14] introduce *malleable signatures* that let one derive, from a signature on a message m, a signature σ' on $m' = T(m)$ for an "allowable" transformation T. This generalizes signature schemes, including quotable [ABC$^+$12, ALP13] or redactable signatures [SBZ02, JMSW02] with an additional context-hiding property. Letting messages be pseudonyms and allowable transformations map one pseudonym to another one, the authors use malleable signatures to construct anonymous credential systems and *delegatable* anonymous credential systems [BCC$^+$09]. The general construction in [CKLM14] however relies on malleable zero-knowledge proofs [CKLM12] and is not practically efficient—even when instantiated with the Groth-Sahai proof system [GS08]. Although the above framework is conceptually totally different from our approach, we note that SPS-EQ can be cast into the definition of malleable signatures: the evaluation algorithm takes only a single message vector with corresponding signature and there is a single type of allowable transformation. However, our construction is practical and moreover Chase et al. [CKLM14] only focus on transformations of single messages (pseudonyms) and do not consider multi-show ABCs, which is the main focus of our construction.

Set Commitments. The best-known approach for commitments to (ordered) sets are *Merkle hash trees* (MHTs) [Mer88], where for a set S the commitment size is $O(1)$ and the opening of a committed set element is of size $O(\log |S|)$. Boneh and Corrigan-Gibbs [BC14] propose an alternative MHT construction using a novel commitment scheme based on a bivariate polynomial modulo RSA composites. In contrast to MHTs, their construction supports succinct proofs of knowledge (PoK) of committed values.

Kate, Zaverucha and Goldberg [KZG10] introduce *polynomial-commitment* schemes that allow to commit to polynomials and support (batch) openings of polynomial evaluations. They can be used to commit to ordered sets (by fixing an index set) or to sets by identifying committed values with roots. Their two constructions are analogues to DL and Pedersen commitments and have $O(1)$-size commitments and openings. Recently, Camenisch et al. [CDHK15] proposed a variant of the Pedersen version from [KZG10]. A related commitment scheme, called *knowledge commitment*, was proposed by Groth [Gro10] and later generalized by Lipmaa [Lip12].

Other commitments to ordered sets are generalized Pedersen [Ped92] or Fujisaki-Okamoto [FO98] commitments. Both have commitment size $O(1)$, but opening proofs are of size $O(|S|)$. For completeness, let us also mention *vector commitments* [CF13], which allow to open specific positions as well as subsequent updates at specific positions (but do not necessarily require hiding). *Zero-knowledge sets* [MRK03] are another primitive in this context. They allow to commit to a set and to perform membership and non-membership queries on values without revealing any further information on the set. In [DHS15b], it was shown that zero-knowledge sets imply commitments in a black-box way.

ABCs. Signatures providing randomization features together with efficient zero-knowledge PoKs of committed values can be used to generically construct ABC systems. The most prominent example are CL credentials [CL03, CL04], based on Σ-protocols. With the advent of Groth-Sahai proofs [GS08], which provide efficient non-interactive proofs in the CRS model without random oracles, various constructions of non-interactive anonymous credentials [BCKL08, ILV11] and delegatable (hierarchical) anonymous credentials [BCC^{+}09, Fuc11] have been proposed. These have a non-interactive showing protocol, that is, the show and verify algorithms do not interact when demonstrating credential possession (also the recent model for conventional ABCs in [CKL^{+}14] demands showings to be non-interactive). We note that although such credential systems with non-interactive protocols extend the scope of applications of anonymous credentials, the most common use case (i.e., authentication and authorization), essentially relies on interaction (to provide freshness/liveness). We emphasize that our goal is not to construct non-interactive anonymous credentials.

1.3 Differences to the Original Work

The original version of this paper by Hanser and Slamanig [HS14] contained an SPS-EQ instantiation that was shown not to be EUF-CMA by Fuchsbauer [Fuc14]. We propose a new instantiation, which we prove EUF-CMA-secure and which is more efficient than the one in [HS14] in terms of key size, signature size and number of verification equations. We also show that our scheme satisfies strengthened security properties, whose relation to the original properties we also analyze.

While [HS14] use the notion of polynomial commitments with factor opening, we found set commitments with subset openings a more natural notion. We also strengthen the ABC security model from [HS14]: we define anonymity against adversaries that create malicious organization keys and provide a stronger notion of unforgeability.

1.4 Subsequent Work

Since its introduction, SPS-EQ has been used in various contexts. The attribute-based multi-show anonymous credential system presented in [HS14] was extended in [DHS15a] by an efficient revocation mechanism, which nicely fits the randomization of SPS-EQ.

Besides ABCs, SPS-EQs have also been used to efficiently instantiate other cryptographic concepts. They yielded an intuitive construction of practical *round-optimal blind signatures* in the standard model [FHS15], which led to an attribute-based one-show anonymous credential system. They were also used to construct conceptually simple *verifiably encrypted signatures* in the standard model by Hanser et al. [HRS15]. As they show that certain SPS-EQ imply public-key encryption, this separates them from one-way functions.

Apart from results concerning SPS-EQ, let us also mention a recent alternative construction of ABCs by Camenisch et al. [CDHK15] from what they call unlinkable redactable signatures. In their approach (whose underlying ideas are related to ours) the size of the credentials and showings is asymptotically identical to that of our construction. However, the concrete efficiency of our construction is much better, partly due to the fact that [CDHK15] target UC security (cf. Section 5.7 for more details).

1.5 Organization

Section 2 discusses preliminaries and Section 3 presents SPS-EQ. In Section 4 we propose set-commitment schemes together with an efficient construction. Section 5 shows how to build an efficient ABC system from the previously presented signature and commitment schemes and compares the efficiency of the resulting ABC scheme to existing approaches. Finally, we discuss open issues and future work in Section 6.

2 Preliminaries

A function $\epsilon\colon \mathbb{N} \to \mathbb{R}^+$ is called *negligible* if for all $c > 0$ there is a k_0 such that $\epsilon(k) < 1/k^c$ for all $k > k_0$. By $a \xleftarrow{R} S$, we denote that a is chosen uniformly at random from a set S. Furthermore, we write $\mathsf{A}(a_1, \ldots, a_n; r)$ if we want to make the randomness r used by a probabilistic algorithm $\mathsf{A}(a_1, \ldots, a_n)$ explicit and denote by $[\mathsf{A}(a_1, \ldots, a_n)]$ the set of points with positive probability of being output by A. For an (additive) group $\mathbb{G}$ we use $\mathbb{G}^*$ to denote $\mathbb{G} \setminus \{0_\mathbb{G}\}$.

Definition 1 (Bilinear Map). Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic groups of prime order p, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive and $\mathbb{G}_T$ is multiplicative. Let P and $\hat{P}$ be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, resp. We call $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ a *bilinear map* or *pairing* if it is efficiently computable and the following holds:

Bilinearity: $e(aP, b\hat{P}) = e(P, \hat{P})^{ab} = e(bP, a\hat{P}) \quad \forall\, a, b \in \mathbb{Z}_p$.
Non-degeneracy: $e(P, \hat{P}) \neq 1_{\mathbb{G}_T}$, i.e., $e(P, \hat{P})$ generates $\mathbb{G}_T$.

If $\mathbb{G}_1 = \mathbb{G}_2$ then e is *symmetric* (Type-1) and *asymmetric* (Type-2 or 3) otherwise. For Type-2 pairings there is an efficiently computable isomorphism $\Psi\colon \mathbb{G}_2 \to \mathbb{G}_1$; for Type-3 pairings no such isomorphism is known. Type-3 pairings are currently the optimal choice in terms of efficiency for a given security level [CM11].

Definition 2 (Bilinear-Group Generator). A *bilinear-group generator* BGGen is a (possibly probabilistic) polynomial-time algorithm that takes a security parameter 1^κ and outputs a description of a bilinear group $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$ consisting of groups $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle \hat{P} \rangle$ and $\mathbb{G}_T$ of prime order p with $\log_2 p = \lceil \kappa \rceil$ and an asymmetric pairing $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.

Definition 3 (DL). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. The *discrete logarithm assumption* holds in $\mathbb{G}_i$ for BGGen if for all probabilistic polynomial-time (PPT) adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ a \xleftarrow{R} \mathbb{Z}_p,\ a' \xleftarrow{R} \mathcal{A}(\mathsf{BG}, aP_i)\ :\ a'P_i = aP_i\right] \leq \epsilon(\kappa)\ .$$

The next assumption states that DL remains hard when given additional elements $a^j P_i$. It is implied e.g. by the Type-3 bilinear-group counterpart of the q-SDH assumption [BB04, CM11].

Definition 4 (q-co-DL). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$. The *$q$-co-discrete logarithm assumption* assumption holds for BGGen, if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}\mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ a \xleftarrow{R} \mathbb{Z}_p \\ a' \xleftarrow{R} \mathcal{A}(\mathsf{BG}, (a^j P, a^j \hat{P})_{j\in[q]})\end{array} \ :\ a'P = aP\right] \le \epsilon(\kappa)\ .$$

Note that we will use the q-co-DL assumption statically throughout this paper, that is, q is a fixed system parameter and does not depend on the adversary's behavior, as e.g. in [BB04].

Definition 5 (DDH). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. The *decisional Diffie-Hellman assumption* holds in $\mathbb{G}_i$ for BGGen, if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}b \xleftarrow{R} \{0,1\},\ \mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ r, s, t \xleftarrow{R} \mathbb{Z}_p \\ b^* \xleftarrow{R} \mathcal{A}(\mathsf{BG}, rP_i, sP_i, ((1-b)\cdot t + b \cdot rs)P_i)\end{array} \ :\ b^* = b\right] - \frac{1}{2} \le \epsilon(\kappa)\ .$$

The XDH assumption formalizes the absence of efficiently computable isomorphisms from $\mathbb{G}_1$ to $\mathbb{G}_2$; the SXDH assumption implies that there is none from $\mathbb{G}_2$ to $\mathbb{G}_1$ either.

Definition 6 ((S)XDH). Let BGGen be a bilinear group generator outputting $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$. The *(symmetric) external Diffie-Hellman assumption* holds for BGGen if DDH holds in $\mathbb{G}_1$ (and in $\mathbb{G}_2$).

The last assumption we use (Definition 8) falls in the uber-assumption family [Boy08, Corollary 1] for the Type-3 bilinear group setting, which we state for completeness:

Definition 7 ($(\mathsf{R}, \mathsf{S}, \mathsf{T}, f)$-DH). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$; let $\mathsf{R} = (\mathsf{r}_i)_{i\in[r]}$, $\mathsf{S} = (\mathsf{s}_j)_{j\in[s]}$ and $\mathsf{T} = (\mathsf{t}_k)_{k\in[t]}$ be three tuples of n-variate polynomials in $\mathbb{Z}_p[X_1, \dots, X_n]$ and also let $f \in \mathbb{Z}_p[X_1, \dots, X_n]$. Define $\mathsf{R}(\boldsymbol{x}) := (\mathsf{r}_i(\boldsymbol{x})P)_{i\in[r]}$, $\mathsf{S}(\boldsymbol{x}) := (\mathsf{s}_i(\boldsymbol{x})\hat{P})_{i\in[s]}$ and $\mathsf{T}(\boldsymbol{x}) := (e(P, \hat{P})^{\mathsf{t}_i(\boldsymbol{x})})_{i\in[t]}$. The $(\mathsf{R}, \mathsf{S}, \mathsf{T}, f)$*-Diffie-Hellman assumption* holds for BGGen, if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}\mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ \boldsymbol{x} \xleftarrow{R} \mathbb{Z}_p^n, \\ e(P, \hat{P})^{f(\boldsymbol{x})} \xleftarrow{R} \mathcal{A}(\mathsf{BG}, \mathsf{R}(\boldsymbol{x}), \mathsf{S}(\boldsymbol{x}), \mathsf{T}(\boldsymbol{x}))\end{array} \ :\ \begin{array}{r}0 \ne f \ne \sum_{(i,j)\in[r]\times[s]} A_{ij}\mathsf{r}_i\mathsf{s}_j + \sum_{k\in[t]} b_k \mathsf{t}_k \\ \forall\, A \in \mathbb{Z}_p^{r\times s}\ \forall\, \boldsymbol{b} \in \mathbb{Z}_p^t\end{array}\right] \le \epsilon(\kappa)\ .$$

Essentially, this assumption says that it is hard to evaluate a polynomial $f \in \mathbb{Z}_p[X_1, ..., X_n]$ at vector $\boldsymbol{x} \in \mathbb{Z}_p^n$ such that f is independent of the polynomials in R, S and T, whose evaluations at $\boldsymbol{x}$ are given to $\mathcal{A}$.

We introduce the following assumption, which is implied by the above assumption and generalizes the q-co-SDH assumption [BB04, CM11]. The latter states that given $(a^i P, a^i \hat{P})_{i\in[q]}$, it is hard to output $(s, \frac{1}{a+s}P)$ for any s. This can be interpreted as outputting the polynomial $h(X) := X + s$ and $\frac{1}{h(a)}P$. The next assumption states that it is not only hard to compute $\frac{1}{h(a)}P$ for h of this specific form, but it is also hard to compute $\frac{g(a)}{h(a)}P$ for any polynomials g, h for which $\deg g < \deg h$.

Definition 8 (Generalized q-co-SDH). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$. Then, the *generalized q-co-strong-Diffie-Hellman assumption* holds for BGGen in $\mathbb{G}_1$, if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}\mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ a \xleftarrow{R} \mathbb{Z}_p, \\ (g, h, T) \xleftarrow{R} \mathcal{A}(\mathsf{BG}, (a^i P, a^i \hat{P})_{i\in[q]})\end{array} \ :\ \begin{array}{r}T \in \mathbb{G}_1\ \wedge\ g, h \in \mathbb{Z}_p[X]\ \wedge \\ 0 \le \deg g < \deg h \le q\ \wedge \\ e(T, h(a)\hat{P}) = e(g(a)P, \hat{P})\end{array}\right] \le \epsilon(\kappa)\ .$$

Analogously, the above assumption can be defined to require $T \in \mathbb{G}_2$. As with the q-co-DL assumption, we will use the generalized q-co-SDH assumption statically.

It allows exponentially many solutions and involves rational polynomials. Thus, to cover it with the uber-assumption framework[3], we introduce the following family of rational target polynomials $\mathcal{F}_q = \{\frac{g(X)}{h(X)} : g, h \in \mathbb{Z}_p[X], 0 \leq \deg g < \deg h \leq q\}$. Then, we require the adversary to additionally specify the target polynomial $f \in \mathcal{F}_q$. It can easily be seen that for $(\mathsf{R}, \mathsf{S}, \mathsf{T}) = ((X^i)_{i\in[0,q]}, (X^i)_{i\in[0,q]}, 1)$ and any $f \in \mathcal{F}_q$ the generalized q-co-SDH assumption is implied by the $(\mathsf{R}, \mathsf{S}, \mathsf{T}, f)$-Diffie Hellman assumption: Observe that the generalized q-co-SDH assumption demands the solution to be in $\mathbb{G}_1$ and that any $f = \frac{g}{h} \in \mathcal{F}_q$ is—due to being rational—independent from all polynomials in $\mathsf{R}, \mathsf{S}, \mathsf{T}$. The asymptotic simulation error in the generic-group model proof of the generalized q-co-SDH assumption attains a cubic error bound.

2.1 Digital Signatures

Definition 9 (Signature Scheme). A *digital signature scheme* is a tuple $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ of PPT algorithms:

$\mathsf{KeyGen}(1^\kappa)$: This probabilistic algorithm takes input a security parameter 1^κ. It outputs a private key sk and a public key pk (we assume that pk includes a description of the message space $\mathcal{M}$).

$\mathsf{Sign}(M, \mathsf{sk})$: This (probabilistic) algorithm takes input a message $M \in \mathcal{M}$ and a secret key sk. It outputs a signature σ.

$\mathsf{Verify}(M, \sigma, \mathsf{pk})$: This deterministic algorithm takes input a message $M \in \mathcal{M}$, a signature σ and a public key pk. It outputs 1 if σ is a valid signature for M under pk and 0 otherwise.

A digital signature scheme is secure if it is *correct* and existentially unforgeable under adaptive chosen-message attacks (EUF-CMA) [GMR88]. We define the properties below:

Definition 10 (Correctness). A digital signature scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is *correct* if for all $\kappa \in \mathbb{N}$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KeyGen}(1^\kappa)]$ and all $M \in \mathcal{M}$ we have:

$$\Pr\left[\mathsf{Verify}(M, \mathsf{Sign}(M, \mathsf{sk}), \mathsf{pk}) = 1\right] = 1 \ .$$

Definition 11 (EUF-CMA). A digital signature scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is *existentially unforgeable under adaptive chosen-message attacks* if for all PPT algorithms $\mathcal{A}$ with access to a signing oracle $\mathsf{Sign}(\cdot, \mathsf{sk})$ there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}(1^\kappa), \\ (M^*, \sigma^*) \xleftarrow{R} \mathcal{A}^{\mathsf{Sign}(\cdot,\mathsf{sk})}(\mathsf{pk})\end{array} : \ M^* \notin Q \quad \wedge \quad \mathsf{Verify}(M^*, \sigma^*, \mathsf{pk}) = 1\right] \leq \epsilon(\kappa) \ ,$$

where Q is the set of queries which $\mathcal{A}$ has issued to the signing oracle.

3 Structure-Preserving Signatures on Equivalence Classes

We are looking for an efficient, randomizable structure-preserving signature scheme for group-element vectors that allows to jointly randomize messages and signatures in the public. We associate messages with representatives of projective equivalence classes defined on the projective space underlying $\mathbb{G}^\ell$

[3] As generally discussed and, in particular, demonstrated for, e.g., the similar but weaker SDH assumption in [Boy08, Sections 6.1 and 6.2]: There, the target polynomial f is allowed to be rational and a family $\mathcal{F} = \{\frac{1}{h(X)} : h \in \mathbb{Z}_p[X], \deg h = 1\}$ is used to describe all possible target polynomials (as there are exponentially many). It must be particularly taken care of that its denominator does not vanish.

(for $\ell > 1$ and some prime order group $\mathbb{G}$). Based on such classes, we will construct a signature scheme that allows the randomization of both messages and signatures via a change of representatives and a consistent signature update.

Let us detail these equivalence classes. All elements of a vector $(M_i)_{i\in[\ell]} \in (\mathbb{G}^*)^\ell$ share different mutual ratios. These ratios depend on their discrete logarithms and are invariant under the operation $\gamma\colon \mathbb{Z}_p^* \times (\mathbb{G}^*)^\ell \to (\mathbb{G}^*)^\ell$ with $(s, (M_i)_{i\in[\ell]}) \mapsto s \cdot (M_i)_{i\in[\ell]}$. This invariance allows for re-randomization of messages and coincides with the operation performing a switch of representatives inside projective equivalence classes defined on $\mathbb{G}^\ell$. More precisely, we use the following projective equivalence relation to partition $(\mathbb{G}^*)^\ell$ into classes:

$$\mathcal{R} = \{(M, N) \in (\mathbb{G}^*)^\ell \times (\mathbb{G}^*)^\ell : \exists\, s \in \mathbb{Z}_p^* \text{ such that } N = s \cdot M\} \subseteq (\mathbb{G}^*)^{2\ell} \ .$$

Note that $\mathcal{R}$ is an equivalence relation if and only if $\mathbb{G}$ has prime order. (We exclude the 0 element from $\mathbb{G}$, since for any $(M_i)_{i\in[\ell]}$, a randomization $s \cdot (M_i)_{i\in[\ell]}$ should look random in $(\mathbb{G}^*)^\ell$, which is clearly not the case if $M_i = 0$ for some i.)

In our scheme an equivalence class $[M]_\mathcal{R}$ is signed by actually signing an arbitrary representative M of $[M]_\mathcal{R}$. The scheme then allows to choose a different representative $s \cdot M$ and to update a signature for M in the public, i.e., without any secret key. One of our goals is to guarantee that two message-signature pairs from the same equivalence class cannot be linked. (Note that such an approach is only feasible for structure-preserving signature schemes where we have no direct access to scalars; if the messages were vectors of elements of $\mathbb{Z}_p^*$, class membership could be decided efficiently.)

3.1 Defining the Signature Scheme

Definition 12 (SPS-EQ). A *structure-preserving signature scheme for equivalence relation* $\mathcal{R}$ over $\mathbb{G}_i$ is a tuple $\mathsf{SPS\text{-}EQ}$ of the following polynomial-time algorithms:

$\mathsf{BGGen}_\mathcal{R}(1^\kappa)$ is a (probabilistic) bilinear-group generation algorithm which on input a security parameter 1^κ outputs a prime-order bilinear group BG.

$\mathsf{KeyGen}_\mathcal{R}(\mathsf{BG}, 1^\ell)$ is a probabilistic algorithm which on input a bilinear group BG and a vector length $\ell > 1$ (in unary) outputs a key pair $(\mathsf{sk}, \mathsf{pk})$.

$\mathsf{Sign}_\mathcal{R}(M, \mathsf{sk})$ is a probabilistic algorithm which on input a representative $M \in (\mathbb{G}_i^*)^\ell$ of an equivalence class $[M]_\mathcal{R}$ and a secret key sk outputs a signature σ for the equivalence class $[M]_\mathcal{R}$.

$\mathsf{ChgRep}_\mathcal{R}(M, \sigma, \mu, \mathsf{pk})$ is a probabilistic algorithm, which on input a representative $M \in (\mathbb{G}_i^*)^\ell$ of an equivalence class $[M]_\mathcal{R}$, a signature σ for M, a scalar μ and a public key pk returns an updated message-signature pair (M', σ'), where $M' = \mu \cdot M$ is the new representative and σ' its updated signature.

$\mathsf{Verify}_\mathcal{R}(M, \sigma, \mathsf{pk})$ is a deterministic algorithm which given a representative $M \in (\mathbb{G}_i^*)^\ell$, a signature σ and a public key pk outputs 1 if σ is valid for M under pk and 0 otherwise.

$\mathsf{VKey}_\mathcal{R}(\mathsf{sk}, \mathsf{pk})$ is a deterministic algorithm which given a secret key sk and a public key pk checks both keys for consistency and returns 1 on success and 0 otherwise.

When one does not care about which new representative is chosen, $\mathsf{ChgRep}_\mathcal{R}$ can be seen as consistent randomization of a signature and its message using randomizer μ without invalidating the signature on the equivalence class. Our goal is that the signature resulting from $\mathsf{ChgRep}_\mathcal{R}$ is indistinguishable from a freshly issued signature for the new representative of the same class.

The scheme is correct if honestly generated key pairs and signatures verify, and if $\mathsf{ChgRep}_\mathcal{R}$ outputs a valid signature.

Definition 13 (Correctness). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ over $\mathbb{G}_i$ is *correct* if for all security parameters $\kappa \in \mathbb{N}$, for all $\ell > 1$, all bilinear groups $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P}) \in [\mathsf{BGGen}_{\mathcal{R}}(1^\kappa)]$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)]$, all messages $M \in (\mathbb{G}_i^*)^\ell$ and all scalars $\mu \in \mathbb{Z}_p^*$ we have:

$$\begin{aligned}&\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1 \quad \text{and}\\ &\Pr\left[\mathsf{Verify}_{\mathcal{R}}(M, \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk}), \mathsf{pk}) = 1\right] = 1 \quad \text{and}\\ &\Pr\left[\mathsf{Verify}_{\mathcal{R}}(\mathsf{ChgRep}_{\mathcal{R}}(M, \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk}), \mu, \mathsf{pk}), \mathsf{pk}) = 1\right] = 1 \ .\end{aligned}$$

Furthermore, we define EUF-CMA security w.r.t. equivalence classes. In contrast to the standard notion of EUF-CMA, we consider a forgery a valid signature on a message from any equivalence class for which the forger has not seen signatures.

Definition 14 (EUF-CMA). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ over $\mathbb{G}_i$ is *existentially unforgeable under adaptive chosen-message attacks* if for all $\ell > 1$ and all PPT algorithms $\mathcal{A}$ having access to a signing oracle $\mathsf{Sign}_{\mathcal{R}}(\cdot, \mathsf{sk})$, there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{l}\mathsf{BG} \xleftarrow{R} \mathsf{BGGen}_{\mathcal{R}}(1^\kappa),\ (\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell),\\ (M^*, \sigma^*) \xleftarrow{R} \mathcal{A}^{\mathsf{Sign}_{\mathcal{R}}(\cdot, \mathsf{sk})}(\mathsf{pk})\end{array} : \begin{array}{r}[M^*]_{\mathcal{R}} \neq [M]_{\mathcal{R}} \quad \forall\, M \in Q\ \wedge\\ \mathsf{Verify}_{\mathcal{R}}(M^*, \sigma^*, \mathsf{pk}) = 1\end{array}\right] \leq \epsilon(\kappa) \ ,$$

where Q is the set of queries that $\mathcal{A}$ has issued to the signing oracle.

We now define new properties, which are better suited to work with than the class-hiding game originally introduced in [HS14]. We start with a class-hiding property on the message space:

Definition 15 (Class-Hiding). Let $\ell > 1$, and $\mathsf{SPS\text{-}EQ}$ be an SPS-EQ scheme on $(\mathbb{G}_i^*)^\ell$. The message space $(\mathbb{G}_i^*)^\ell$ is *class-hiding* if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}b \xleftarrow{R} \{0,1\},\ \mathsf{BG} \xleftarrow{R} \mathsf{BGGen}_{\mathcal{R}}(1^\kappa),\ M \xleftarrow{R} (\mathbb{G}_i^*)^\ell,\\ M_0 \xleftarrow{R} (\mathbb{G}_i^*)^\ell, M_1 \xleftarrow{R} [M]_{\mathcal{R}},\ b^* \xleftarrow{R} \mathcal{A}(\mathsf{BG}, M, M_b)\end{array} : \ b^* = b\right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

The following result shows that the class-hiding property is linked to the DDH assumption.

Proposition 1. *Let $\ell > 1$ and $\mathsf{SPS\text{-}EQ}$ be an SPS-EQ scheme on $(\mathbb{G}_i^*)^\ell$. Then $(\mathbb{G}_i^*)^\ell$ is a class-hiding message space if and only if the DDH assumption holds in $\mathbb{G}_i$.*

Proof. W.l.o.g. we consider message space $(\mathbb{G}_1^*)^\ell$. We first note that DDH (as defined in Definition 5) is equivalent to a variant DDH* where r, s, t are drawn from $\mathbb{Z}_p^*$ instead of $\mathbb{Z}_p$ (as the respective distributions are statistically indistinguishable). It suffices thus to show that class-hiding is equivalent to DDH*.

"⇒" Assume an adversary $\mathcal{A}$ that breaks DDH*. We define an adversary $\mathcal{B}$ against the class-hiding property of $(\mathbb{G}_i^*)^\ell$: $\mathcal{B}$ is given an instance (BG, M, M'); it randomly selects two distinct indexes $i, j \in [\ell]$ and runs $\mathcal{A}$ on (M_i, M_j, M'_i, M'_j) and outputs whatever $\mathcal{A}$ outputs.

If $M' \in [M]_{\mathcal{R}}$ then $M' = \lambda M$ for some $\lambda \in \mathbb{Z}_p^*$ and $(M_i, M_j, M'_i, M'_j) = (m_i P, m_j P, \lambda m_i P, \lambda m_j P)$ is a valid DDH* tuple in $\mathbb{G}_1$. Finally, there is the case of false positives, i.e., the case that $M' \notin [M]_{\mathcal{R}}$ but the input given to $\mathcal{A}$ constitutes a valid DDH* tuple in $\mathbb{G}_1$. This occurs however only with negligible probability.

"⇐" Let us parametrize the game from Definition 15 by bit b and denote it as Game_b, that is, $\mathcal{A}$ is given $(\mathsf{BG}, M, M' \xleftarrow{R} (\mathbb{G}_1^*)^\ell)$ in Game_0 and $(\mathsf{BG}, M, M' \xleftarrow{R} [M]_{\mathcal{R}})$ in Game_1. We next define a hybrid game Game'_j for every $j \in [\ell]$: it chooses $\mu \xleftarrow{R} \mathbb{Z}_p^*$ and $R_{j+1}, \ldots, R_\ell \xleftarrow{R} \mathbb{G}_1^*$ and runs $\mathcal{A}$ on BG, M and

$$M' := (\mu M_1, \ldots, \mu M_j, R_{j+1}, \ldots, R_\ell) \ .$$

Note that by definition $\mathsf{Game}'_1 = \mathsf{Game}_0$ and $\mathsf{Game}'_\ell = \mathsf{Game}_1$, respectively.

If there exists an adversary that distinguishes Game_0 from Game_1 with probability $\epsilon(\kappa)$ then for some index $j \in [\ell]$ it distinguishes Game'_{j-1} from Game'_j with probability $\frac{1}{\ell-1}\epsilon(\kappa)$, which is non-negligible if $\epsilon(\kappa)$ is non-negligible. We show how to construct a DDH* distinguisher $\mathcal{B}$ from a distinguisher between Game'_{j-1} and Game'_j.

Given a DDH* instance $(\mathsf{BG}, rP, sP, tP)$, $\mathcal{B}$ picks $(m_i)_{i\in[\ell]} \xleftarrow{R} (\mathbb{Z}_p^*)^\ell$ and $R_{j+1}, \ldots, R_\ell \xleftarrow{R} \mathbb{G}_1^*$, sets

$$M \leftarrow \big(m_1 P, \ldots\ldots, m_{j-1}P, (rP), m_{j+1}P, \ldots, m_\ell P\big) \tag{1}$$

$$M' \leftarrow \big(m_1(sP), \ldots, m_{j-1}(sP), (tP), R_{j+1}, \ldots\ldots, R_\ell\big) \tag{2}$$

and runs $\mathcal{A}$ on (BG, M, M'). If $(\mathsf{BG}, rP, sP, tP)$ is a "real" instance (i.e. $t = rs$) then the first j elements in (2) are s-multiples of the first j elements in (1), and $\mathcal{B}$ thus simulates Game'_j. If t is random then so is the j-th element in (2) and $\mathcal{B}$ simulates Game'_{j-1}. Hence, any adversary distinguishing Game'_{j-1} from Game'_j can be used to break DDH*. □

The next two definitions were used in [FHS15]. The first one formalizes the notion that signatures output by $\mathsf{ChgRep}_\mathcal{R}$ are distributed like fresh signatures on the new representative.

Definition 16 (Signature adaptation). Let $\ell > 1$. An SPS-EQ scheme SPS-EQ on $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures* if for all tuples $(\mathsf{sk}, \mathsf{pk}, M, \sigma, \mu)$ with

$$\mathsf{VKey}_\mathcal{R}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad \mathsf{Verify}_\mathcal{R}(M, \sigma, \mathsf{pk}) = 1 \qquad M \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

$\mathsf{ChgRep}_\mathcal{R}(M, \sigma, \mu, \mathsf{pk})$ and $(\mu M, \mathsf{Sign}_\mathcal{R}(\mu M, \mathsf{sk}))$ are identically distributed.

The following definition demands that this even holds for maliciously generated verification keys. As for such keys there might not even exist a corresponding secret key, we require that adapted signatures are random elements in the space of valid signatures.

Definition 17 (Signature adaptation under malicious keys). Let $\ell > 1$. An SPS-EQ scheme SPS-EQ on $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures under malicious keys* if for all tuples $(\mathsf{pk}, M, \sigma, \mu)$ with

$$\mathsf{Verify}_\mathcal{R}(M, \sigma, \mathsf{pk}) = 1 \qquad M \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^* \tag{3}$$

we have that $\mathsf{ChgRep}_\mathcal{R}(M, \sigma, \mu, \mathsf{pk})$ outputs $(\mu M, \sigma')$ such that σ' is a uniformly random element in the space of signatures, conditioned on $\mathsf{Verify}_\mathcal{R}(\mu M, \sigma', \mathsf{pk}) = 1$.

3.2 Our Construction

In Figure 1 we present our SPS-EQ construction with message space $(\mathbb{G}_1^*)^\ell$. Its signatures consist of two $\mathbb{G}_1$ elements and one $\mathbb{G}_2$ element and public keys are ℓ-tuples from $\mathbb{G}_2$. Verification is defined via two pairing-product equations. A scheme with message space $(\mathbb{G}_2^*)^\ell$ is easily obtained by swapping the group memberships of all elements.

3.3 Security of Our Construction

We prove the security of our construction using a direct proof in the generic-group model. The proofs of Theorems 1 and 2 are given in Appendix A.

Theorem 1. *The SPS-EQ scheme in Scheme 1 is correct.*

Theorem 2. *In the generic-group model for Type-3 bilinear groups, Scheme 1 is EUF-CMA secure.*

$\underline{\mathsf{BGGen}_{\mathcal{R}}}(1^\kappa)$: On input a security parameter 1^κ, output $\mathsf{BG} \overset{R}{\leftarrow} \mathsf{BGGen}(1^\kappa)$.

$\underline{\mathsf{KeyGen}_{\mathcal{R}}}(\mathsf{BG}, 1^\ell)$: On input a bilinear-group description BG and vector length $\ell > 1$ (in unary), choose $(x_i)_{i\in[\ell]} \overset{R}{\leftarrow} (\mathbb{Z}_p^*)^\ell$, set secret key $\mathsf{sk} \leftarrow (x_i)_{i\in[\ell]}$, compute public key $\mathsf{pk} \leftarrow (\hat{X}_i)_{i\in[\ell]} = (x_i\hat{P})_{i\in[\ell]}$ and output $(\mathsf{sk}, \mathsf{pk})$.

$\underline{\mathsf{Sign}_{\mathcal{R}}}(M, \mathsf{sk})$: On input a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of equivalence class $[M]_{\mathcal{R}}$ and a secret key $\mathsf{sk} = (x_i)_{i\in[\ell]} \in (\mathbb{Z}_p^*)^\ell$, choose $y \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and output $\sigma \leftarrow (Z, Y, \hat{Y})$ with

$$Z \leftarrow y \sum_{i\in[\ell]} x_i M_i \qquad\qquad Y \leftarrow \tfrac{1}{y}P \qquad\qquad \hat{Y} \leftarrow \tfrac{1}{y}\hat{P}\ .$$

$\underline{\mathsf{Verify}_{\mathcal{R}}}(M, \sigma, \mathsf{pk})$: On input a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of equivalence class $[M]_{\mathcal{R}}$, a signature $\sigma = (Z, Y, \hat{Y}) \in \mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ and public key $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$, check whether

$$\prod_{i\in[\ell]} e(M_i, \hat{X}_i) = e(Z, \hat{Y}) \qquad \wedge \qquad e(Y, \hat{P}) = e(P, \hat{Y})$$

and if this holds output 1 and 0 otherwise.

$\underline{\mathsf{ChgRep}_{\mathcal{R}}}(M, \sigma, \mu, \mathsf{pk})$: On input a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of equivalence class $[M]_{\mathcal{R}}$, a signature $\sigma = (Z, Y, \hat{Y})$, $\mu \in \mathbb{Z}_p^*$ and public key pk, return $\perp$ if $\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = 0$. Otherwise pick $\psi \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and return $(\mu \cdot M, \sigma')$ with $\sigma' \leftarrow (\psi\mu Z, \frac{1}{\psi}Y, \frac{1}{\psi}\hat{Y})$.

$\underline{\mathsf{VKey}_{\mathcal{R}}}(\mathsf{sk}, \mathsf{pk})$: On input $\mathsf{sk} = (x_i)_{i\in[\ell]} \in (\mathbb{Z}_p^*)^\ell$ and $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$, output 1 if $x_i\hat{P} = \hat{X}_i\ \forall i \in [\ell]$ and 0 otherwise.

Fig. 1. Scheme 1, an EUF-CMA secure SPS-EQ scheme

Lemma 1. *Scheme 1 has perfect adaptation of signatures and perfect adaptation of signatures under malicious keys.*

Proof. Let $M \in (\mathbb{G}_1^*)^\ell$, $\mathsf{pk} \in (\mathbb{G}_2^*)^\ell$ and $(x_i)_{i\in[\ell]}$ be such that $\mathsf{pk} = (x_i\hat{P})_{i\in[\ell]}$. A signature $(Z, Y, \hat{Y}) \in \mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ satisfying $\mathsf{Verify}_{\mathcal{R}}(M, (Z, Y, \hat{Y}), \mathsf{pk}) = 1$ is of the form $(y \sum x_i M_i, \frac{1}{y}P, \frac{1}{y}\hat{P})$ for some $y \in \mathbb{Z}_p^*$. $\mathsf{ChgRep}_{\mathcal{R}}(M, (Z, Y, \hat{Y}), \mu, \mathsf{pk})$ for $\mu \in \mathbb{Z}_p^*$ outputs $(y\psi \sum x_i \mu M_i, \frac{1}{y\psi}P, \frac{1}{y\psi}\hat{P})$, which is a uniformly random element σ in $\mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ satisfying $\mathsf{Verify}_{\mathcal{R}}(\mu M, \sigma, \mathsf{pk}) = 1$.

Scheme 1 moreover satisfies Definition 16, since $\mathsf{sk} = (x_i)_{i\in[\ell]}$ is the only element satisfying $\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1$ and $\mathsf{Sign}_{\mathcal{R}}(\mu M, \mathsf{sk})$ outputs a random element σ in $\mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ satisfying $\mathsf{Verify}_{\mathcal{R}}(\mu M, \sigma, \mathsf{pk}) = 1$. □

4 Set Commitments

We now introduce a new commitment type that allows for committing to sets and besides ordinary opening also supports opening of subsets. After formalizing the primitive, we give an efficient construction with succinct commitments and openings.

Kate, Zaverucha and Goldberg [KZG10] introduce the notion of constant-size polynomial commitments. They present two schemes, one computationally and one perfectly hiding. Following a similar approach, we construct set commitments, which allow us to commit to a set $S \subset \mathbb{Z}_p$ by committing to a monic polynomial whose roots are the elements of S. A feature we are aiming for opening of subsets of the committed set, which corresponds to opening non-trivial factors of the committed polynomial. Our scheme is perfectly hiding and computationally binding.

4.1 Definitions

We first present the model and security properties of our set-commitments scheme. They are adapted from the polynomial-commitment scheme in [HS14], tailored to sets encoded as monic polynomials.

Definition 18 (Set Commitments). A *set-commitment scheme* SC consists of the following PPT algorithms.

$\mathsf{Setup}(1^\kappa, 1^t)$: This probabilistic algorithm takes input a security parameter κ and an upper bound t for the cardinality of committed sets, both in unary form. It outputs public parameters pp (which include a description of an efficiently samplable message space $\mathcal{S}_{\mathsf{pp}}$ containing sets of maximum cardinality t).

$\mathsf{Commit}(\mathsf{pp}, S)$: This probabilistic algorithm takes input the public parameters pp defining message space $\mathcal{S}_{\mathsf{pp}}$ and a non-empty set $S \in \mathcal{S}_{\mathsf{pp}}$. It outputs a commitment C to set S and opening information O.

$\mathsf{Open}(\mathsf{pp}, C, O)$: This deterministic algorithm takes input the public parameters pp, a commitment C and opening information O. If O is a valid opening of C to $S \in \mathcal{S}_{\mathsf{pp}}$, it outputs S, and $\perp$ otherwise.

$\mathsf{OpenSubset}(\mathsf{pp}, C, O, T)$: This (deterministic) algorithm takes input the public parameters pp, a commitment C, opening information O for some set $S \in \mathcal{S}_{\mathsf{pp}}$ and a non-empty set T. It returns $\perp$ if $T \not\subseteq S$; else it returns a witness W for T being a subset of S.

$\mathsf{VerifySubset}(\mathsf{pp}, C, T, W)$: This deterministic algorithm takes input the public parameters pp, a commitment C, a non-empty set T and a witness W. If W is a witness for T being a subset of the set committed to in C, it outputs 1, and 0 otherwise.

We call a set-commitment scheme *secure* if it is *correct*, *binding*, *subset-sound* and *hiding*. The properties are as follows, where the definitions of correctness, binding and hiding are mostly straightforward.

Definition 19 (Correctness). A set-commitment scheme SC is *correct* if for all $t > 0$, all $\kappa > 0$, all $\mathsf{pp} \in [\mathsf{Setup}(1^\kappa, 1^t)]$, all $S \in \mathcal{S}_{\mathsf{pp}}$ and all non-empty $T \subseteq S$ the following holds:

1. $\Pr\left[\,\mathsf{Open}(\mathsf{pp}, \mathsf{Commit}(\mathsf{pp}, S)) = S\,\right] = 1$.
2. $\Pr\left[(C, O) \xleftarrow{R} \mathsf{Commit}(\mathsf{pp}, S) \;:\; \mathsf{VerifySubset}(\mathsf{pp}, C, T, \mathsf{OpenSubset}(\mathsf{pp}, C, O, T)) = 1\right] = 1$.

Definition 20 (Binding). A set-commitment scheme SC is *binding* if for all $t > 0$ and all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{l}\mathsf{pp} \xleftarrow{R} \mathsf{Setup}(1^\kappa, 1^t),\; (C, O, O') \xleftarrow{R} \mathcal{A}(\mathsf{pp}),\\ S \leftarrow \mathsf{Open}(\mathsf{pp}, C, O),\; S' \leftarrow \mathsf{Open}(\mathsf{pp}, C, O')\end{array} \;:\; S \neq S' \;\wedge\; S, S' \neq \perp\right] \leq \epsilon(\kappa) \ .$$

Subset soundness requires it to be infeasible to perform subset openings to sets that are not contained in the committed set.

Definition 21 (Subset-Soundness). A set-commitment scheme SC is *subset-sound* if for all $t > 0$ and all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{l}\mathsf{pp} \xleftarrow{R} \mathsf{Setup}(1^\kappa, 1^t),\; (C, O, T, W) \xleftarrow{R} \mathcal{A}(\mathsf{pp}),\\ S \leftarrow \mathsf{Open}(\mathsf{pp}, C, O)\end{array} \;:\; \begin{array}{r} S \neq \perp \;\wedge\; T \not\subseteq S \;\wedge\\ \mathsf{VerifySubset}(\mathsf{pp}, C, T, W) = 1\end{array}\right] \leq \epsilon(\kappa) \ .$$

Our hiding notion strengthens the standard one by giving the adversary access to an $\mathsf{OpenSubset}$ oracle that opens the challenge commitment to any subset in the intersection of the two candidate sets.

Definition 22 (Hiding). A set-commitment scheme SC is *hiding* if for all $t > 0$ and all PPT adversaries $\mathcal{A}$ with access to an oracle $\mathsf{OpenSubset}$ there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{l} b \xleftarrow{R} \{0,1\},\ \mathsf{pp} \xleftarrow{R} \mathsf{Setup}(1^\kappa, 1^t), \\ (S_0, S_1, \mathsf{st}) \xleftarrow{R} \mathcal{A}(\mathsf{pp}), \\ (C, O) \xleftarrow{R} \mathsf{Commit}(\mathsf{pp}, S_b), \\ b^* \xleftarrow{R} \mathcal{A}^{\mathsf{OpenSubset}(\mathsf{pp}, C, O, \cdot \cap (S_0 \cap S_1))}(\mathsf{st}, C) \end{array} : \ b^* = b \right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

In the *perfectly hiding* case, unbounded adversaries are being considered and $\epsilon \equiv 0$.

4.2 The Construction

We now give a construction SC of a set-commitment scheme. For the sake of compact representation, for $S \subset \mathbb{Z}_p$ we let $f_S(X) := \prod_{s \in S}(X - s) = \sum_{i=0}^{|S|} f_i \cdot X^i$. For a group generator P, since $f_S(a)P = \sum_{i=0}^{|S|}(f_i \cdot a^i)P$, one can efficiently compute $f_S(a)P$ when given $(a^iP)_{i=0}^{|S|}$ but not a itself.

$\mathsf{Setup}(1^\kappa, 1^t)$: On input a security parameter 1^κ and a maximum set cardinality 1^t run $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P}) \xleftarrow{R} \mathsf{BGGen}(1^\kappa)$, pick $a \xleftarrow{R} \mathbb{Z}_p$ and output $\mathsf{pp} \leftarrow (\mathsf{BG}, (a^iP, a^i\hat{P})_{i \in [t]})$, which defines message space $\mathcal{S}_{\mathsf{pp}} = \{S \subset \mathbb{Z}_p : 0 < |S| \leq t\}$.

$\mathsf{Commit}(\mathsf{pp}, S)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i \in [t]})$ and a set $S \subset \mathbb{Z}_p$ with $0 < |S| \leq t$:
- If for some $a' \in S$: $a'P = aP$, output $C \xleftarrow{R} \mathbb{G}_1^*$ and opening $O \leftarrow (1, a', S)$;
- else pick $\rho \xleftarrow{R} \mathbb{Z}_p^*$, compute $C \leftarrow \rho \cdot f_S(a)P \in \mathbb{G}_1^*$ and output (C, O) with $O \leftarrow (0, \rho, S)$.

$\mathsf{Open}(\mathsf{pp}, C, O)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i \in [t]})$, a commitment C and opening $O = (b, \rho, S)$: if $C \notin \mathbb{G}_1^*$ or $\rho \notin \mathbb{Z}_p^*$ or $S \not\subset \mathbb{Z}_p$ or $S = \emptyset$ or $|S| > t$ then return $\perp$.
- If $O = (1, a', S)$ and $a'P = aP$ then return S; else return $\perp$.
- If $O = (0, \rho, S)$ and $C = \rho \cdot f_S(a)P$, return S; else return $\perp$.

$\mathsf{OpenSubset}(\mathsf{pp}, C, O, T)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i \in [t]})$, a commitment C, opening O and a set T, let $S \leftarrow \mathsf{Open}(\mathsf{pp}, C, O)$. If $S = \perp$, $T \nsubseteq S$ or $T = \emptyset$ then output $\perp$.
- If $O = (1, a', S)$: if $a' \in T$, return $W \leftarrow \perp$; else return $W \leftarrow f_T(a')^{-1} \cdot C$.
- If $O = (0, \rho, S)$, output $W \leftarrow \rho \cdot f_{S \setminus T}(a)P$.

$\mathsf{VerifySubset}(\mathsf{pp}, C, T, W)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i \in [t]})$, a commitment C, a set T and a witness W: if $C \notin \mathbb{G}_1^*$ or $T \not\subset \mathbb{Z}_p$ or $T = \emptyset$ or $|T| > t$, return 0.
- If for some $a' \in T$: $a'P = aP$ then: if $W = \perp$, return 1, else return 0.
- Else: if $W \in \mathbb{G}_1^*$ and $e(W, f_T(a)\hat{P}) = e(C, \hat{P})$, return 1, else return 0.

We have augmented the scheme from [HS14] by a special opening (of the form $(1, a, S)$) for the case that a set S contains the trapdoor a. (Under the t-co-DL assumption, such sets are infeasible to find.) This makes the scheme perfectly correct and perfectly hiding while still maintaining computational binding and subset-soundness.

We have defined the scheme in a way that reduces the computational complexity of the prover in the ABC system in Section 5.4. To improve the performance of $\mathsf{VerifySubset}$, one could define a scheme with $W \in \mathbb{G}_2$ (for which $\mathsf{VerifySubset}$ would have to compute $f_T(a)P$).

Security. We prove SC secure under the q-co-DL and the generalized q-co-SDH assumption. We use both assumptions in a static way, as $q \leftarrow t$ is a system parameter and fixed a priori.

Theorem 3. SC *is correct.*

Proof. Let $t, \kappa > 0$ and $(\mathsf{BG}, (a^i P, a^i \hat{P})_{i\in[t]}) \xleftarrow{R} \mathsf{Setup}(1^\kappa, 1^t)$ with $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$, let $S \subset \mathbb{Z}_p$ with $0 < |S| \leq t$ and let $\emptyset \neq T \subseteq S$. We consider two cases.
(1) $a \in S$. $\mathsf{Commit}(\mathsf{pp}, \mathsf{S})$ returns (C, O) with $C \in \mathbb{G}_1^*$ and $O = (1, a, S)$. Open on input $(C, (1, a, S))$ returns S, which shows the first property. $\mathsf{OpenSubset}(\mathsf{pp}, C, O, T)$ returns $W \leftarrow \perp$ if $a \in T$ and $W \leftarrow f_T(a)^{-1} \cdot C$ if $a \notin T$. If $a \in T$ then $\mathsf{VerifySubset}(\mathsf{pp}, C, T, W)$ returns 1 if $W = \perp$. If $a \notin T$, it returns 1 if $C, W \in \mathbb{G}_1^*$ and $e(W, f_T(a)\hat{P}) = e(C, \hat{P})$; this is satisfied, since $W \in \mathbb{G}_1^*$ and $e(W, f_T(a)\hat{P}) = e(f_T(a)^{-1} \cdot C, f_T(a)\hat{P}) = e(C, \hat{P})$.
(2) $a \notin S$. $\mathsf{Commit}(\mathsf{pp}, \mathsf{S})$ returns (C, O) with $C = \rho \cdot f_S(a)P$ and $O = (0, \rho, S)$ with $\rho \in \mathbb{Z}_p^*$. For O of this form, Open returns S, since $\rho \in \mathbb{Z}_p^*$, $S \subset \mathbb{Z}_p^*$, $0 < |S| \leq t$, $f_S(a) \neq 0$, thus $C \in \mathbb{G}_1^*$ and C has the required form. $\mathsf{OpenSubset}(\mathsf{pp}, C, O, T)$ returns $W \leftarrow \rho \cdot f_{S\setminus T}(a)P$. On input (pp, C, T, W), $\mathsf{VerifySubset}$ returns 1 if $C, W \in \mathbb{G}_1^*$ and $e(W, f_T(a)\hat{P}) = e(C, \hat{P})$. Since $\rho \in \mathbb{Z}_p^*$, $a \notin S$ we have $W = \rho \cdot f_{S\setminus T}(a)P \in \mathbb{G}_1^*$; moreover, $e(W, f_T(a)\hat{P}) = e(\rho \cdot f_S(a) \cdot f_T(a)^{-1} \cdot P, f_T(a)\hat{P}) = e(\rho \cdot f_S(a)P, \hat{P}) = e(C, \hat{P})$; so $\mathsf{VerifySubset}$ returns 1. □

Theorem 4. *If the t-co-DL assumption holds then* SC *is binding.*

Proof. We show that if $\mathcal{A}$ is able to output a commitment C and two valid openings to distinct sets S, S' then we can construct an adversary $\mathcal{B}$ that breaks t-co-DL: $\mathcal{B}$ obtains an instance $I = (\mathsf{BG}, (a^i P, a^i \hat{P})_{i\in[t]})$, sets $\mathsf{pp} \leftarrow I$ and runs $\mathcal{A}(\mathsf{pp})$. If $\mathcal{A}$ outputs a collision (C, O, O') then by $\perp \neq S \leftarrow \mathsf{Open}(\mathsf{pp}, C, O)$ and $\perp \neq S' \leftarrow \mathsf{Open}(\mathsf{pp}, C, O')$ with $S \neq S'$, it holds that $C \in \mathbb{G}_1^*$. If $O = (1, a', S)$ or $O' = (1, a', S')$ then $\mathcal{B}$ outputs a' as solution to the t-co-DL problem. Else, we have $O = (0, \rho, S), O' = (0, \rho', S')$ with $\emptyset \neq S, S' \subset \mathbb{Z}_p$, $\rho, \rho' \in \mathbb{Z}_p^*$ and:

$$\rho \cdot f_S(a)P = C = \rho' \cdot f_{S'}(a)P \ \ ,$$

from which we have $\rho \cdot f_S(a) - \rho' \cdot f_{S'}(a) = 0$. Since S and S' are both non-empty and distinct, we have $\deg f_S > 0$ and $\deg f_{S'} > 0$ and $f_S \neq f_{S'}$. Furthermore, f_S and $f_{S'}$ are monic and $\rho, \rho' \neq 0$, thus $t(X) \leftarrow \rho \cdot f_S(X) - \rho' \cdot f_{S'}(X) \neq 0$ while $t(a) = 0$. Therefore, a is a root of the non-zero polynomial $t(X) \in \mathbb{Z}_p[X]$ and $t(X)$ is known to $\mathcal{B}$. Factoring $t(X)$ yields a, which $\mathcal{B}$ outputs as solution to the t-co-DL problem. □

Theorem 5. *If the generalized t-co-SDH assumption holds then* SC *is subset-sound.*

Proof. We show that if $\mathcal{A}$ is able to output (C, O, T, W), such that O is a valid opening of C to set S, $T \nsubseteq S$ and $\mathsf{VerifySubset}(\mathsf{pp}, C, T, W) = 1$ then we can construct an adversary $\mathcal{B}$ against the generalized t-co-SDH as follows. On input an instance $I = (\mathsf{BG}, (a^i P, a^i \hat{P})_{i\in[t]})$, $\mathcal{B}$ sets $\mathsf{pp} \leftarrow I$ and runs $\mathcal{A}(\mathsf{pp})$; assume $\mathcal{A}$ breaks subset-soundness by outputting (C, O, T, W).

We first deal with the case $f_T(a) = 0$. Since $T \neq \emptyset$ (otherwise $\mathsf{Verifysubset}$ returns 0), and thus $f_T(X)$ is a non-constant polynomial with root a, $\mathcal{B}$ can efficiently obtain a by factoring $f_T(X)$. It then chooses $c \in \mathbb{Z}_p \setminus \{-a\}$, and outputs a solution $(1, X + c, \frac{1}{a+c}P)$ to generalized t-co-SDH.

For the rest of the proof, assume $f_T(a) \neq 0$, and thus $a \notin T$. As $\mathcal{A}$ is successful, we have $\perp \neq S \leftarrow \mathsf{Open}(\mathsf{pp}, C, O)$. If $O = (1, a', S)$ then $\mathcal{B}$ chooses $c \in \mathbb{Z}_p \setminus \{-a'\}$, and outputs a solution $(1, X + c, \frac{1}{a'+c}P)$ to generalized t-co-SDH. Else, we have $O = (0, \rho, S)$ with $\emptyset \neq S \subset \mathbb{Z}_p$, $|S| \leq t$, $\rho \in \mathbb{Z}_p^*$ and

$$C = \rho \cdot f_S(a)P \in \mathbb{G}_1^* \ \ . \tag{4}$$

From $\mathsf{VerifySubset}(\mathsf{pp}, C, T, W) = 1$ we have $\emptyset \neq T \subset \mathbb{Z}_p$, $|T| \leq t$, $W \in \mathbb{G}_1^*$ and $e(W, f_T(a)\hat{P}) = e(C, \hat{P})$, which by (4) equals $e(\rho \cdot f_S(a)P, \hat{P})$. Since $\rho \neq 0$, we have

$$e(\rho^{-1}W, f_T(a)\hat{P}) = e(f_S(a)P, \hat{P}) \ \ . \tag{5}$$

We further distinguish two cases:
(1) $0 < |S| < |T|$. Then $0 < \deg f_S < \deg f_T \leq t$, which together with (5) means that $(f_S, f_T, \rho^{-1}W)$ is a solution to the generalized t-co-SDH assumption.
(2) $0 < |T| \leq |S|$. Then $0 < \deg f_T \leq \deg f_S$. Since $T \not\subseteq S$, by polynomial division we obtain h, r with $f_S(X) = h(X)f_T(X) + r(X)$ and $0 \leq \deg r < \deg f_T$. Moreover, $\deg h \leq \deg f_S \leq t$. Plugging this into (5), we get:

$$e\big(\rho^{-1}W, f_T(a)\hat{P}\big) = e\big(h(a)f_T(a)P + r(a)P, \hat{P}\big) = e\big(h(a)P, f_T(a)\hat{P}\big) + e\big(r(a)P, \hat{P}\big) \ , \text{ and thus}$$
$$e\big(\rho^{-1}W - h(a)P, f_T(a)\hat{P}\big) = e\big(r(a)P, \hat{P}\big) \ .$$

Together with $0 \leq \deg r < \deg f_T \leq t$, this means that $(r, f_T, \rho^{-1}W - h(a)P)$ is a solution to the generalized t-co-SDH assumption, which $\mathcal{B}$ can efficiently compute from pp, since $\deg h \leq t$. □

Theorem 6. SC *is perfectly hiding.*

Proof. We consider the view of an unbounded adversary $\mathcal{A}$ in the hiding experiment and assume w.l.o.g. that every query T to the OpenSubset oracle satisfies $T \subset \mathbb{Z}_p$ and $\emptyset \neq T \subseteq (S_0 \cap S_1)$. We distinguish several cases.
(1) $\mathcal{A}$ chooses S_0, S_1 with $a \in S_0 \cap S_1$. Then for both $b = 0, 1$, C_b is uniformly random in $\mathbb{G}_1^*$ ($C_b \in_R \mathbb{G}_1^*$) and the jth query T_j to OpenSubset is answered with $\perp$ if $a \in T_j$, and with $W_{j,b} = f_T(a)^{-1} \cdot C_b$ if $a \notin T_j$. The bit b is thus information-theoretically hidden from $\mathcal{A}$.
(2) a is contained in one of the sets S_0, S_1; say $a \in S_0$. Note that for all queries T_j, we have $a \notin T_j$. If $b = 0$ then $\mathcal{A}$ receives a uniformly random C_0 and when it queries T_j to the OpenSubset oracle, it receives $W_{j,0} = f_{T_j}(a)^{-1} \cdot C_0$. If $b = 1$ then $\mathcal{A}$ receives $C_1 = \rho \cdot f_S(a)P$ for $\rho \in_R \mathbb{Z}_p^*$, and query T_j to the OpenSubset oracle returns witness $W_{j,1} = \rho \cdot f_{S \setminus T_j}(a) \cdot P = \rho \cdot f_S(a) \cdot f_{T_j}(a)^{-1} \cdot P = f_{T_j}(a)^{-1} \cdot C_1$. Hence, for both $b = 0, 1$ we have $C_b \in_R \mathbb{G}_1^*$ and $W_{j,b} = f_{T_j}(a)^{-1} \cdot C_b$ for all j; the bit b is thus information-theoretically hidden from $\mathcal{A}$.
(3) $\mathcal{A}$ chooses S_0, S_1 with $a \notin S_0 \cup S_1$. Then for $b = 0, 1$: $C_b = \rho \cdot f_{S_b}(a)P$ for $\rho \in_R \mathbb{Z}_p^*$ and a query for T_j is answered by $W_{j,b} = \rho \cdot f_{S_b \setminus T_j}(a)P = f_{T_j}(a)^{-1} \cdot C_b$. Again for both $b = 0$ and $b = 1$, $\mathcal{A}$ receives a uniform random element C_b and query replies that do not depend on b; the bit b is thus information-theoretically hidden from $\mathcal{A}$. □

5 Building an ABC System

In this section we present an application of SPS-EQ and set commitments introduced in the two previous sections; we use them as basic building blocks for an attribute-based credential system. ABC systems are usually constructed in one of two ways. They can be built from blind signatures: a user obtains a blind signature from an issuer on (commitments to) attributes and later shows the signature, provides the shown attributes and proves knowledge of all unrevealed attributes [Bra00, BL13, FHS15]. The drawback of this approach is that such credentials can only be shown once in an unlinkable fashion (*one-show*).

Anonymous credentials supporting an arbitrary number of unlinkable showings (*multi-show*) can be obtained in a similar vein using a different type of signatures: A user obtains a signature on (commitments to) attributes then *randomizes* the signature (so that the resulting signature is unlinkable to the issued one) and proves in zero-knowledge the correspondence of this signature to the shown attributes as well as the undisclosed attributes [CL03, CL04]. Our approach also achieves multi-show ABCs, but differs from the latter. We randomize both the signature and the message (which is a set commitment to attributes) and then use subset-opening of set commitments for selective constant-size showings of attributes. Thereby, we completely avoid costly ZKPoKs over the attributes (which are necessarily at least linear in the number of shown/encoded attributes).

We start by discussing the functionality and security of ABCs in Sections 5.1 and 5.2. After providing some intuition for our construction (Section 5.3), we present the scheme (Section 5.4) and discuss its security (Section 5.5). Finally, we give a performance and functionality comparison with other schemes in Section 5.7.

5.1 Model of ABCs

In an ABC system there are different organizations issuing credentials to users. These users can then anonymously demonstrate possession of their credentials to verifiers. The system is called *multi-show* when transactions (issuing and showings) performed by the same user cannot be linked. A credential cred for user i is issued by an organization for a set of attributes $\mathtt{A}$ and the user can show a subset of $\mathtt{A}$ while hiding the other attributes. Note that in our definition there is no setup and we do not assume any trusted parameters at all.

Definition 23 (ABC System). An *attribute-based anonymous credentials system* consists of the following PPT algorithms:

$\mathsf{OrgKeyGen}(1^\kappa, 1^t)$: A probabilistic algorithm that gets (unary representations of) a security parameter κ and an upper bound t for the size of attribute sets. It outputs a key pair $(\mathsf{osk}, \mathsf{opk})$ for an organization.

$\mathsf{UserKeyGen}(1^\kappa)$: A probabilistic algorithm that gets (the unary representation of) a security parameter κ and outputs a key pair $(\mathsf{usk}, \mathsf{upk})$ for a user.

$(\mathsf{Obtain}(\mathsf{usk}, \mathsf{opk}, \mathtt{A}), \mathsf{Issue}(\mathsf{upk}, \mathsf{osk}, \mathtt{A}))$: These algorithms are run by a user and an organization, respectively, who interact during execution. Obtain is a probabilistic algorithm that takes input the user's secret key usk, an organization's public key opk and a non-empty attribute set $\mathtt{A}$ of size $|\mathtt{A}| \leq t$. Issue is a probabilistic algorithm that takes input a user's public key upk, the organization's secret key osk and a non-empty attribute set $\mathtt{A}$ of size $|\mathtt{A}| \leq t$. At the end of this protocol, Obtain outputs a credential cred for the user for attributes $\mathtt{A}$ or $\perp$ if the execution failed.

$(\mathsf{Show}(\mathsf{opk}, \mathtt{A}, \mathtt{A}', \mathsf{cred}), \mathsf{Verify}(\mathsf{opk}, \mathtt{A}'))$: These algorithms are run by a user and a verifier, respectively, who interact during execution. Show is a probabilistic algorithm that takes input the organization's public key opk, an attribute set $\mathtt{A}$ of size $|\mathtt{A}| \leq t$, a non-empty set $\mathtt{A}' \subseteq \mathtt{A}$ (representing the attributes to be shown) and a credential cred. Verify is a deterministic algorithm that takes input the organization's public key opk and a set $\mathtt{A}'$. At the end of the protocol, Verify outputs 1 or 0 indicating whether it accepts the credential showing or not.

5.2 Security of ABCs

We present a security model for multi-show ABCs, which is game-based and in the vein of group signatures [BSZ05] and considers malicious organization keys. We note that there are no other comprehensive models for ABC systems (apart from independently developed very strong simulation-based notions in [CKL+14, CDHK15]). We start with a high-level overview of the required security properties and note that we consider only a single organization in our model of unforgeability and anonymity (since all organizations have independent signing keys, the extension to multiple organizations is straightforward):

Correctness: A showing of a credential with respect to a non-empty set $\mathtt{A}'$ of attributes and values always verifies if the credential was issued honestly for some attribute set $\mathtt{A}$ with $\mathtt{A}' \subseteq \mathtt{A}$.

Unforgeability: A user cannot perform a valid showing of attributes for which she does not possess a credential. Moreover, no coalition of malicious users can combine their credentials and prove possession of a set of attributes which no single member has. This holds even after seeing showings of arbitrary credentials by honest users (the notion thus covers replay attacks).

Anonymity: During a showing, no verifier and no (malicious) organization (even if they collude) should be able to identify the user or learn anything about the user, except that she owns a valid credential for the shown attributes. Furthermore, different showings of the same credential are unlinkable.

We now provide formal definitions of these properties, for which we introduce the following global variables and oracles.

Global variables. At the beginning of each experiment, either the experiment computes an organization key pair $(\mathsf{osk}, \mathsf{opk})$ or the adversary outputs opk. In the anonymity game there is a bit b, which the adversary must guess.

In order to keep track of all the users, in particular all honest and corrupt users and those whose secret keys and credentials have leaked, we introduce the sets $\mathtt{U}$, $\mathtt{HU}$, $\mathtt{CU}$ and $\mathtt{KU}$, respectively. We use the lists $\mathtt{UPK}$, $\mathtt{USK}$, $\mathtt{CRED}$, $\mathtt{ATTR}$ and $\mathtt{I2U}$ to track user public and secret keys, issued credentials and corresponding attributes and to which user they were issued. Furthermore, we use the sets J_{LoR} and I_{LoR} to store the issuance indices and corresponding users that have been set during the first call to the left-or-right oracle in the anonymity game.

Oracles. The oracles are as follows:

$\mathcal{O}^{\mathtt{HU}+}(i)$ takes input a user identity i. If $i \in \mathtt{U}$, it returns $\perp$. Otherwise, it creates a new honest user i by running $(\mathtt{USK}[i], \mathtt{UPK}[i]) \overset{R}{\leftarrow} \mathsf{UserKeyGen}(1^\kappa)$, adding i to $\mathtt{U}$ and to $\mathtt{HU}$ and returning $\mathtt{UPK}[i]$.

$\mathcal{O}^{\mathtt{CU}+}(i, \mathsf{upk})$ takes input a user identity i and a user public key upk. If $i \in \mathtt{U}$, it returns $\perp$. Otherwise, it creates a corrupted user i by adding i sets $\mathtt{U}$ and $\mathtt{CU}$, and setting $\mathtt{UPK}[i] \leftarrow \mathsf{upk}$.

$\mathcal{O}^{\mathtt{KU}+}(i)$ takes input a user identity i and corrupts it. If $i \notin \mathtt{HU}$ or $i \in I_{LoR}$, it returns $\perp$. Otherwise, it reveals the secret key and all credentials of user i by returning $\mathtt{USK}[i]$ and $\mathtt{CRED}[j]$ for all j with $\mathtt{I2U}[j] = i$. It removes i from $\mathtt{HU}$ and adds it to $\mathtt{KU}$.

$\mathcal{O}^{\mathsf{ObtIss}}(i, \mathtt{A})$ takes input a user identity i and a set of attributes $\mathtt{A}$. If $i \notin \mathtt{HU}$, it returns $\perp$. Otherwise, it issues a credential to i by running

$$(\mathsf{cred}, \top) \overset{R}{\leftarrow} (\mathsf{Obtain}(\mathtt{USK}[i], \mathsf{opk}, \mathtt{A}), \mathsf{Issue}(\mathtt{UPK}[i], \mathsf{osk}, \mathtt{A})) \ .$$

If $\mathsf{cred} = \perp$, it returns $\perp$. Else, it appends $(i, \mathsf{cred}, \mathtt{A})$ to $(\mathtt{I2U}, \mathtt{CRED}, \mathtt{ATTR})$ and returns $\top$.

$\mathcal{O}^{\mathsf{Obtain}}(i, \mathtt{A})$ lets the adversary, who impersonates a dishonest organization, issue a credential to an honest user. It takes input a user identity i and a set of attributes $\mathtt{A}$. If $i \notin \mathtt{HU}$, it returns $\perp$. Otherwise, it runs

$$(\mathsf{cred}, \cdot) \overset{R}{\leftarrow} (\mathsf{Obtain}(\mathtt{USK}[i], \mathsf{opk}, \mathtt{A}), \cdot\,) \ ,$$

where the Issue part is executed by the adversary. If $\mathsf{cred} = \perp$, it returns $\perp$. Else, it appends $(i, \mathsf{cred}, \mathtt{A})$ to $(\mathtt{I2U}, \mathtt{CRED}, \mathtt{ATTR})$ and returns $\top$.

$\mathcal{O}^{\mathsf{Issue}}(i, \mathtt{A})$ lets the adversary, who impersonates a malicious user, obtain a credential from an honest organization. It takes input a user identity i and a set of attributes $\mathtt{A}$. If $i \notin \mathtt{CU}$, it returns $\perp$. Otherwise, it runs

$$(\cdot, I) \overset{R}{\leftarrow} (\,\cdot\,, \mathsf{Issue}(\mathtt{UPK}[i], \mathsf{osk}, \mathtt{A})) \ ,$$

where the Obtain part is executed by the adversary. If $I = \perp$, it returns $\perp$. Else, it appends $(i, \perp, \mathtt{A})$ to $(\mathtt{I2U}, \mathtt{CRED}, \mathtt{ATTR})$ and returns $\top$.

$\mathcal{O}^{\mathsf{Show}}(j, \mathtt{A}')$ lets the adversary play a dishonest verifier in a showing by an honest user. It takes input an index of an issuance j and a set of attributes $\mathtt{A}'$. Let $i \leftarrow \mathtt{I2U}[j]$. If $i \notin \mathtt{HU}$, it returns $\perp$. Otherwise, it runs

$$(S, \cdot) \xleftarrow{R} (\mathsf{Show}(\mathsf{opk}, \mathtt{ATTR}[j], \mathtt{A}', \mathtt{CRED}[j]), \cdot) \ ,$$

where the Verify part is executed by adversary.

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$ is the challenge oracle in the anonymity game where the adversary must distinguish (multiple) showings of two credentials $\mathtt{CRED}[j_0]$ and $\mathtt{CRED}[j_1]$. The oracle takes two issuance indexes j_0 and j_1 and a set of attributes $\mathtt{A}'$. If $J_{LoR} \neq \emptyset$ and $J_{LoR} \neq \{j_0, j_1\}$, it returns $\perp$. Let $i_0 \leftarrow \mathtt{I2U}[j_0]$ and $i_1 \leftarrow \mathtt{I2U}[j_1]$. If $J_{LoR} = \emptyset$ then it sets $J_{LoR} \leftarrow \{j_0, j_1\}$ and $I_{LoR} \leftarrow \{i_0, i_1\}$. If $i_0, i_1 \notin \mathtt{HU}$ or $\mathtt{A}' \not\subseteq \mathtt{ATTR}[j_0] \cap \mathtt{ATTR}[j_1]$, it returns $\perp$. Else, it runs

$$(S, \cdot) \xleftarrow{R} (\mathsf{Show}(\mathsf{opk}, \mathtt{ATTR}[j_b], \mathtt{A}', \mathtt{CRED}[j_b]), \cdot) \ ,$$

(with b set by the experiment) where the Verify part is executed by the adversary.

Using the global variables and oracles just defined, we now define security of an ABC system:

Definition 24 (Correctness). An ABC system is *correct*, if for all $\kappa > 0$, all $t > 0$ and all $\mathtt{A}$ with $0 < |\mathtt{A}| \leq t$ and all $\emptyset \neq \mathtt{A}' \subseteq \mathtt{A}$ it holds that:

$$\Pr\left[\begin{array}{l} (\mathsf{osk}, \mathsf{opk}) \xleftarrow{R} \mathsf{OrgKeyGen}(1^\kappa, 1^t), \\ (\mathsf{usk}, \mathsf{upk}) \xleftarrow{R} \mathsf{UserKeyGen}(1^\kappa), \\ (\mathsf{cred}, \top) \xleftarrow{R} (\mathsf{Obtain}(\mathsf{usk}, \mathsf{opk}, \mathtt{A}), \\ \qquad\qquad\qquad \mathsf{Issue}(\mathsf{upk}, \mathsf{osk}, \mathtt{A})) \end{array} : \begin{array}{r} (\top, 1) \xleftarrow{R} (\mathsf{Show}(\mathsf{opk}, \mathtt{A}, \mathtt{A}', \mathsf{cred}), \\ \mathsf{Verify}(\mathsf{opk}, \mathtt{A}')) \end{array}\right] = 1 \ .$$

Definition 25 (Unforgeability). An ABC system is *unforgeable*, if for all $t > 0$ and all PPT adversaries $\mathcal{A}$ having oracle access to $\mathcal{O} := \{\mathcal{O}^{\mathtt{HU}+}, \mathcal{O}^{\mathtt{CU}+}, \mathcal{O}^{\mathtt{KU}+}, \mathcal{O}^{\mathsf{ObtIss}}, \mathcal{O}^{\mathsf{Issue}}, \mathcal{O}^{\mathsf{Show}}\}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l} (\mathsf{osk}, \mathsf{opk}) \xleftarrow{R} \mathsf{OrgKeyGen}(1^\kappa, 1^t), \\ (\mathtt{A}', \mathsf{st}) \xleftarrow{R} \mathcal{A}^{\mathcal{O}}(\mathsf{opk}), \\ (\cdot, b^*) \xleftarrow{R} (\mathcal{A}(\mathsf{st}), \mathsf{Verify}(\mathsf{opk}, \mathtt{A}')) \end{array} : \begin{array}{l} b^* = 1 \ \wedge \\ \forall j : \mathtt{I2U}[j] \in \mathtt{KU} \cup \mathtt{CU} \\ \qquad \Rightarrow \mathtt{A}' \not\subseteq \mathtt{ATTR}[j] \end{array}\right] \leq \epsilon(\kappa) \ .$$

Definition 26 (Anonymity). An ABC system is *anonymous*, if for all $t > 0$ and all PPT adversaries $\mathcal{A}$ having oracle access to $\mathcal{O} := \{\mathcal{O}^{\mathtt{HU}+}, \mathcal{O}^{\mathtt{CU}+}, \mathcal{O}^{\mathtt{KU}+}, \mathcal{O}^{\mathsf{Obtain}}, \mathcal{O}^{\mathsf{Show}}, \mathcal{O}^{LoR}\}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l} b \xleftarrow{R} \{0,1\}, \ (\mathsf{opk}, \mathsf{st}) \xleftarrow{R} \mathcal{A}(1^\kappa, 1^t), \\ b^* \xleftarrow{R} \mathcal{A}^{\mathcal{O}}(\mathsf{st}) \end{array} : \ b^* = b\right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

5.3 Intuition of Our Construction

Our construction of ABCs is based on SPS-EQ, on set commitments with subset openings and on a *single* constant-size proof of knowledge for guaranteeing freshness. In contrast to this, the complexity of proofs of knowledge in existing ABC systems [Bra00, CL01, CL03, CL04, CL11, CL13] is linear in the number of shown (or even issued) attributes. However, aside from selective disclosure of attributes, they usually allow to prove statements about non-revealed attribute values, such as AND, OR and NOT, interval proofs, as well as conjunctions and disjunctions of the aforementioned. We achieve less expressiveness; our construction supports selective disclosure as well as AND statements about attributes (as the constructions in [CL11, CL13, CDHK15], of which only the latter also achieves constant-size showings). A user can thus either open some attributes and their corresponding values or solely prove that some attributes are encoded in the respective credential without revealing their concrete values. Note that one can always associate sets of values to attributes, so that users are not required to reveal the full attribute value, but only predefined "statements" about the attribute value, e.g. "01.01.1980","> 16", or "> 18" for an attribute label `birthdate`. This allows emulation of proving properties about attribute values.

Example. To give an idea of the expressiveness of our construction, we include an example of an attribute set $\mathtt{A}$. We are given a user with the following set of attribute and value strings:

$$\mathtt{A} = \{\text{``}\mathtt{gender, male}\text{''}, \text{``}\mathtt{birthdate, 01.01.1980}\text{''}, \text{``}\mathtt{drivinglicense, \#}\text{''}, \text{``}\mathtt{drivinglicense, car}\text{''}\}\ .$$

Note that # indicates an attribute value that allows to prove the possession of the attribute without revealing any concrete value. A showing could, for instance, involve the following attributes $\mathtt{A}'$ and its hidden complement $\mathtt{A} \setminus \mathtt{A}'$:

$$\mathtt{A}' = \{\text{``}\mathtt{gender, male}\text{''}, \text{``}\mathtt{drivinglicense, \#}\text{''}\}$$
$$\mathtt{A} \setminus \mathtt{A}' = \{\text{``}\mathtt{birthdate, 01.01.1980}\text{''}, \text{``}\mathtt{drivinglicense, car}\text{''}\}\ .$$

Outline. We assume attributes to be values from $\mathbb{Z}_p$ and note that we can define attributes of arbitrary format by using a collision-resistant hash function $H\colon \{0,1\}^* \to \mathbb{Z}_p$. In our construction a credential cred of user i consists of a group element C, a scalar $r \in \mathbb{Z}_p^*$, a modified opening O' of C (not containing the attributes) and an SPS-EQ signature σ on $(C, r \cdot C, P)$. The element C is a set commitment to a set of attributes $\mathtt{A} \subset \mathbb{Z}_p$, whose randomness is the user secret usk (thus, its opening O' contains usk or the commitment trapdoor a, if $a \in \mathtt{A}$). Additionally, the user performs a ZKPoK $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})$ to prove knowledge of usk, which allows us to extract usk for corrupted users in the proof of unforgeability. This use of usk is important to achieve anonymity (omitting usk in our construction would immediately break anonymity).

The values C and r define an equivalence class $[(C, r \cdot C, P)]_{\mathcal{R}}$ that is unique for each credential with overwhelming probability. The scalar r and the third credential component are required to prove unforgeability. During a showing, a random representative of this class, $(C_1, C_2, C_3) \overset{R}{\leftarrow} [(C, r \cdot C, P)]_{\mathcal{R}}$, together with a consistently updated signature σ' is presented. The randomized commitment C_1 is then subset-opened to the shown attributes $\mathtt{A}' \subseteq \mathtt{A}$ (representing selective disclosure). Hence, showings additionally include a witness W and a verifier checks whether the encodings of the disclosed attributes and W give a valid subset opening of C_1. In order to guarantee freshness, the prover also performs a constant-size ZKPoK of the discrete logarithm of C_2 to base C_1 (i.e., the randomness r) and the discrete logarithm of C_3 to base P (the randomizer used for obtaining (C_1, C_2, C_3) from $(C, r \cdot C, P)$).

Freshness. We have to guarantee that no valid showing transcript can be replayed by someone not in possession of the credential. To do so, we require the user to conduct an (interactive) proof of knowledge $\mathsf{PoK}\{\beta : C_3 = \beta P\}$ of the discrete logarithm of the third component $C_3 = \mu P$ of a shown credential $\mathsf{cred}' = ((C_1, C_2, C_3), \sigma')$, i.e., the randomizer μ used in the showing protocol. This guarantees that we have a fresh challenge for every showing. For the unforgeability reduction, we have the user additionally prove knowledge of $r = \log_{C_1} C_2$ by conducting a proof of knowledge $\mathsf{PoK}\{\alpha : C_2 = \alpha C_1\}$. We use the compact notation $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3)$ for the AND-composition of both proofs, i.e., $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3) := \mathsf{PoK}\{(\alpha, \beta) : C_2 = \alpha C_1 \ \wedge\ C_3 = \beta P\}$.

Malicious Organization Keys. In contrast to anonymity notions usually considered for ABC, our model guarantees anonymity even against adversaries that generate the organization keys maliciously. Our construction is in the standard model and organization public keys consist of an SPS-EQ public key pk and the set commitment parameters $\mathsf{pp}_{\mathsf{sc}}$. We augment the issuing protocol sketched above and let the (malicious) organization prove knowledge of a secret key that is consistent with its public key (this allows us to extract the signing key in the anonymity proof).

For an SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ we define an NP-relation $\mathcal{R}_{\mathsf{VK}}$, whose statements and witnesses are public and private keys, i.e.: $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{R}'_{\mathsf{VK}} \iff \mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1$. In our proof of anonymity we also need to extract the set commitment trapdoor $a \in \mathbb{Z}_p$, so we augment the above relation to:

$$((aP, \mathsf{pk}), (w_1, w_2)) \in \mathcal{R}_{\mathsf{VK}} \iff (aP = w_1 P \ \wedge \ \mathsf{VKey}_{\mathcal{R}}(w_2, \mathsf{pk}) = 1) \ ,$$

where aP is from the set commitment parameters $\mathsf{pp}_{\mathsf{sc}}$ contained in opk. For compactness, we use the notation $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ and require the proof to be a perfect zero-knowledge proof of knowledge.

ZKPoKs and Concurrent Security. We will consider all ZKPoKs in a black-box way. They can be efficiently instantiated using, e.g., the 4-move ZKPoK proof systems from [CDM00], which is based on Σ-protocols and features rewindable black-box access to the verifier.

Note however that the ZKPoKs from [CDM00] are not concurrently secure and so neither is any instantiation of Scheme 2 using them. Thus, each organization, each user and each verifier must not run more than one protocol execution at once. In Section 5.6, we will discuss a concurrently secure scheme variant in the CRS model.

5.4 The Construction of the ABC System

Our ABC system is based on any perfectly adapting structure-preserving signature scheme on equivalence classes $\mathsf{SPS\text{-}EQ}$ and the set-commitment scheme SC from Section 4.2 (which we are going to modify slightly) and is described in Scheme 2. In particular, since the organization public key is fully determined by the adversary (for malicious-key anonymity), we assume the bilinear group generation algorithm of $\mathsf{SPS\text{-}EQ}$ and the one inside the set commitment setup algorithm to be deterministic[4,5] and produce the same bilinear group for each security parameter. We will base our proofs on assumptions that are modified accordingly, i.e., that are with respect to a deterministic BGGen producing the same bilinear group for each security parameter.

Modified Set Commitment Algorithms. For the sake of a modular presentation, we use custom variants of the set commitment algorithms Commit and $\mathsf{OpenSubset}$ of scheme SC, denoted by Commit' and $\mathsf{OpenSubset}'$.

Commit' gives partial control over the randomness ρ used during the computation of the commitment and returns a modified opening not containing the set. In particular, it returns a commitment with randomness ρ if $a \notin S$ and a uniformly random commitment otherwise.

$\mathsf{Commit}'(\mathsf{pp}, S, \rho)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^i P, a^i \hat{P})_{i \in [t]})$, a set $S \subset \mathbb{Z}_p$, $0 < |S| \leq t$, and a scalar $\rho \in \mathbb{Z}_p^*$:

- If for some $a' \in S$: $a'P = aP$, output $C \xleftarrow{R} \mathbb{G}_1^*$ and short opening $O' \leftarrow (1, a')$. *(as in* Commit *except for not including S in O')*
- Else compute $C \leftarrow \rho \cdot f_S(a)P \in \mathbb{G}_1^*$ and output (C, O') with $O' \leftarrow (0, \rho)$. *(using ρ from the input instead of drawing it internally)*

[4] This is for example the case for BN-curves [BN06], the most common choice for Type-3 pairings.

[5] Hence, the only randomness used by the set commitment setup algorithm is the one used for picking the commitment trapdoor. Inside $\mathsf{OrgKeyGen}$, we will make this randomness explicit.

$\mathsf{OrgKeyGen}(1^\kappa, 1^t)$: Given $\kappa, t > 0$, pick $a \xleftarrow{R} \mathbb{Z}_p$, run $\mathsf{pp_{sc}} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i\in[t]}) \leftarrow \mathsf{Setup}(1^\kappa, 1^t; a)$, run $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)$ for $\ell = 3$ and return $(\mathsf{osk}, \mathsf{opk}) \leftarrow ((a, \mathsf{sk}), (\mathsf{pp_{sc}}, \mathsf{pk}))$.

$\mathsf{UserKeyGen}(1^\kappa)$: Given security parameter $\kappa > 0$, run $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, pick $\mathsf{usk} \xleftarrow{R} \mathbb{Z}_p^*$, set $\mathsf{upk} \leftarrow \mathsf{usk}\cdot P$ and return $(\mathsf{usk}, \mathsf{upk})$.

$(\mathsf{Obtain}, \mathsf{Issue})$: Using $\Pi^{\mathcal{R}_{\mathsf{VK}}}\big(\mathsf{opk} = ((\mathsf{BG}, (a^iP, a^i\hat{P})_i), \mathsf{pk})\big) := \mathsf{PoK}\big\{(\alpha, \boldsymbol{\beta}) : \alpha P = aP \wedge \mathsf{VKey}_{\mathcal{R}}(\boldsymbol{\beta}, \mathsf{pk}) = 1\big\}$ and $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk}) := \mathsf{PoK}\{\alpha : \alpha P = \mathsf{upk}\}$, Obtain and Issue interact as follows:

$\mathsf{Obtain}(\mathsf{usk}, \mathsf{opk}, \mathtt{A})$		$\mathsf{Issue}(\mathsf{upk}, \mathsf{osk}, \mathtt{A})$
If $\mathtt{A} = \emptyset \vee \mathtt{A} \not\subset \mathbb{Z}_p \vee \lvert\mathtt{A}\rvert > t$, return $\perp$		If $\mathtt{A} = \emptyset \vee \mathtt{A} \not\subset \mathbb{Z}_p \vee \lvert\mathtt{A}\rvert > t$, return $\perp$
$\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$	$\xleftrightarrow{\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})}$	If $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})$ fails, return $\perp$
	$\xleftrightarrow{\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})}$	
If $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ fails, return $\perp$		
$(C, O') \xleftarrow{R} \mathsf{Commit}'(\mathsf{pp_{sc}}, \mathtt{A}, \mathsf{usk})$		
$r \xleftarrow{R} \mathbb{Z}_p^*,\ R \leftarrow r \cdot C$	$\xrightarrow{C, R}$	If $e(C, \hat{P}) \neq e(\mathsf{upk}, f_{\mathtt{A}}(a)\hat{P})$ and $\forall a' \in \mathtt{A} : a'P \neq aP$ then return $\perp$
If $\mathsf{Verify}_{\mathcal{R}}((C, R, P), \sigma, \mathsf{pk}) = 0$ return $\perp$	$\xleftarrow{\sigma}$	Else $\sigma \xleftarrow{R} \mathsf{Sign}_{\mathcal{R}}((C, R, P), \mathsf{sk})$
Else return $\mathsf{cred} \leftarrow (C, \sigma, r, O')$		

$(\mathsf{Show}, \mathsf{Verify})$: Using $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3) := \mathsf{PoK}\{(\alpha, \beta) : C_2 = \alpha C_1 \wedge C_3 = \beta P\}$, Show and Verify interact as follows:

$\mathsf{Show}(\mathsf{opk}, \mathtt{A}, \mathtt{A}', \mathsf{cred})$		$\mathsf{Verify}(\mathsf{opk}, \mathtt{A}')$
Let $\mathsf{cred} = (C, \sigma, r, O')$; $\quad \mu \xleftarrow{R} \mathbb{Z}_p^*$		Let $\mathsf{opk} = (\mathsf{pp_{sc}}, \mathsf{pk})$
$\mathsf{cred}' \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}((C, r \cdot C, P), \sigma, \mu, \mathsf{pk})$		
If $\mathsf{cred}' = \perp$, return $\perp$		
Let $\mathsf{cred}' = ((C_1, C_2, C_3), \sigma')$		
$W \leftarrow \mathsf{OpenSubset}'(\mathsf{pp_{sc}}, C_1, (O', \mathtt{A}), \mu, \mathtt{A}')$	$\xrightarrow{\mathsf{cred}', W}$	
	$\xleftrightarrow{\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3)}$	If $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3)$ fails, return 0
		Return $\big(\mathsf{Verify}_{\mathcal{R}}(\mathsf{cred}', \mathsf{pk}) \wedge \mathsf{VerifySubset}(\mathsf{pp_{sc}}, C_1, \mathtt{A}', W)\big)$

Fig. 2. Scheme 2, a multi-show ABC system

We adapt $\mathsf{OpenSubset}'$ to deal with rerandomized commitments (taking input an original opening).

$\mathsf{OpenSubset}'(\mathsf{pp}, C, O, \mu, T)$: On input $\mathsf{pp} = (\mathsf{BG}, (a^iP, a^i\hat{P})_{i\in[t]})$, commitment C, opening O, scalar $\mu \in \mathbb{Z}_p^*$ and a set T, let $S \leftarrow \mathsf{Open}(\mathsf{pp}, \mu^{-1} \cdot C, O)$. If $S = \perp$, $T \nsubseteq S$ or $T = \emptyset$ then output $\perp$. *(contrary to* $\mathsf{OpenSubset}$*,* Open *is being run on* $\mu^{-1} \cdot C$ *instead of* C*)*

- If $O = (1, a', S)$: if $a' \in T$, return $W \leftarrow \perp$; else return $W \leftarrow f_T(a')^{-1} \cdot C$. *(as in* $\mathsf{OpenSubset}$*)*
- If $O = (0, \rho, S)$, output $W \leftarrow \mu \cdot \rho \cdot f_{S\setminus T}(a)P$. *($W$ gets additionally multiplied by μ)*

Optimizations. Note that the first move in the showing protocol can be combined with the first move of $\Pi^{\mathcal{R}_\mathsf{F}}$, meaning the showing protocol consists of a total of 4 moves, when using 4-move ZKPoKs. Furthermore, note that issuing can be made more efficient with regard to both communication complexity and computational effort, as osk contains set commitment trapdoor a: instead of using a paring to check C for consistency, the issuer can compute it herself as $C \leftarrow f_\mathsf{A}(a) \cdot \mathsf{upk}$. (We wrote our scheme so that a is never used and pp_sc can then be moved to public parameters in the concurrently secure variant discussed below.)

5.5 Security

The correctness of Scheme 2 follows by inspection. In Appendix B, we formally prove the following.

Theorem 7. *Let $\Pi^{\mathcal{R}_\mathsf{F}}$, $\Pi^{\mathcal{R}_\mathsf{UK}}$ and $\Pi^{\mathcal{R}_\mathsf{VK}}$ be ZKPoKs. If the t-co-DL assumption holds,* SC *is subset-sound and* $\mathsf{SPS\text{-}EQ}$ *is EUF-CMA-secure then Scheme 2 is unforgeable.*

Theorem 8. *Let $\Pi^{\mathcal{R}_\mathsf{F}}$, $\Pi^{\mathcal{R}_\mathsf{UK}}$ and $\Pi^{\mathcal{R}_\mathsf{VK}}$ be ZKPoKs. If the* $\mathsf{SPS\text{-}EQ}$ *has a class-hiding message space and perfectly adapts signatures then Scheme 2 is anonymous.*

5.6 A Concurrently Secure Scheme Variant

We now sketch a more efficient and concurrently secure variant of our scheme, which uses public parameters. Damgård [Dam00] proposes a generic transformation of any Σ-protocol for an arbitrary NP-relation $\mathcal{R}$ into a 3-move concurrent ZKPoK (without any timing constraints), under the assumption of one-way functions and using a CRS. By introducing a setup algorithm and replacing the ZKPoKs used in our construction with those from [Dam00] (the statements proven stay the same), we obtain an ABC that is concurrently secure in the CRS model (and, in particular, anonymous under malicious organization keys in the CRS model) and uses four moves during issuing and only three moves during showing (when interleaving the ZKPoK moves with the other protocol moves).

The introduction of system parameters pp further allows us to move the set-commitment parameters from the organization keys to pp, which reduces the size of organization public keys.

5.7 Efficiency Analysis and Comparison

We provide a brief comparison with other ABC approaches. As other candidates for multi-show ABCs, we consider the Camenisch-Lysyanskaya schemes [CL01, CL03, CL04] as well as schemes from BBS$^+$ signatures [BBS04, ASM06], which cover a broad class of ABC schemes from randomizable signature schemes with efficient proofs of knowledge. Furthermore, we look at two alternative multi-show ABC constructions [CL11, CL13] as well as Brands' approach [Bra00] (also covering the provable secure version [BL13]) for the sake of completeness, although the latter only provides one-show ABCs. We omit other approaches such as [AMO08] that only allow a single attribute per credential. We also omit approaches that achieve more efficient showings for existing ABC systems only in very special cases such as for attribute values that come from a very small set (and are, thus, hard to compare).[6] Finally, we also include the recent approach in [CDHK15] that has the same asymptotic parameter sizes as our approach. They achieve security in the UC framework [Can01], but consequently far less efficient constructions in a concrete setting. Their approach is equally expressive as ours (selective disclosure), but additionally supports pseudonyms and context-specific pseudonyms for showings.

[6] For instance, the approach in [CG12] for CL credentials in the strong-RSA setting (encoding attributes as prime numbers) or in a pairing-based setting using BBS$^+$ credentials [SNF11] (encoding attributes using accumulators) where the latter additionally requires very large public parameters (one F-secure BB signature [BCKL08] for every possible attribute value).

Table 1. Comparison of various approaches to ABC systems.

Scheme	**Parameter Size** (L attr.)			**Issuing**			**Showing** (k-of-L attr.)			MK	P
	Setting	CRS	Credential Size	Issuer	User	Comm	Verifier	User	Comm		
[CL03]	sRSA	$O(L)$	$O(1)$	$3\vert\mathbb{Z}_N\vert$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	$O(L-k)$	×	r
[CL04]	Type-1	$O(L)$	$O(L)$	$(2L+2)\vert\mathbb{G}_1\vert$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	×	r
[BBS04]	Type-2	$O(L)$	$O(1)$	$\vert\mathbb{G}_1\vert + 22\vert\mathbb{Z}_q\vert$	$O(L)$	$O(L)$	$O(1)$	$O(L)$	$O(L)$	$O(L)$	×	r
[CL11]	Type-2	$O(1)$	$O(L)$	$L\vert\mathbb{G}_1\vert + 1\vert\mathbb{G}_2\vert$	$O(L)$	$O(L)$	$O(L)$	$O(L)$	$O(1)$	$O(1)$	×	s
[CL13]	XDH	$O(L)$	$O(L)$	$(2L+2)(1\vert\mathbb{G}_1\vert + 1\vert\mathbb{Z}_p\vert)$	$O(L)$	$O(L)$	$O(L)$	$O(k)$	$O(k)$	$O(k)$	×	s
[Bra00]	$\mathbb{G}_q$	$O(L)$	$O(1)$	$2\vert\mathbb{G}_q\vert + 2\vert\mathbb{Z}_q\vert$	$O(L)$	$O(L)$	$O(1)$	$O(k)$	$O(k)$	$O(L-k)$	×	r
[CDHK15]	SXDH	$O(L)$	$O(1)$	$6\vert\mathbb{G}_1\vert + 2\vert\mathbb{G}_2\vert + 1\vert\mathbb{Z}_p\vert$	$O(L)$	$O(L)$	$O(1)$	$O(k)$	$O(L-k)$	$O(1)$	○	s
Scheme 2	SXDH	×	$O(1)$	$3\vert\mathbb{G}_1\vert + 1\vert\mathbb{G}_2\vert + 2\vert\mathbb{Z}_p\vert$	$O(L)$	$O(L)$	$O(1)$	$O(k)$	$O(L-k)$	$O(1)$	✓	s

For our comparison in Table 1 we take their most efficient instantiation (which does not provide secret key extractability) and note that our showings require less than 10 group elements (when instantiated with Scheme 1 and the ZKPoK protocol from [CDM00]), whereas the cheapest variant in [CDHK15] requires around 100 group elements.

Table 1 gives an overview of these systems, where *Type-1* and *Type-2* refer to the type of bilinear group; in a stronger sense, *XDH* and *SXDH* requires the respective assumption to hold. Furthermore, $\mathbb{G}_q$ denotes a group of prime order q (e.g., a subgroup of large order q of $\mathbb{Z}_p^*$ or an elliptic curve group of order q). By $|\mathbb{G}|$, denote the bitlength of the representation of an element from group $\mathbb{G}$, by MK we indicate whether anonymity (privacy) holds with respect to maliciously generated issuer keys and by P we indicate whether the schemes support selective disclosure (s) or also proving relations about attributes (r). We note that $\circ$ indicates that the most efficient construction from [CDHK15] used in Table 1 does not consider malicious keys, while the other less efficient ones in [CDHK15] do.

We emphasize that, in contrast to other approaches, such as [CL04, CL13], our construction only requires a small and constant number of pairing evaluations in all protocol steps. We stress that the model introduced in [CKL$^+$14] allows to instantiate constructions, for instance based on [CL03], that can deal with malicious organization keys (although at the cost of efficiency).

6 Future Work

Some challenging issues with respect to SPS-EQ remain open. Primarily, the construction of an instantiation secure in the standard model (or CRS model) that relies on simple assumptions and perfectly adapts signatures (under malicious keys) is an open problem. A first step was done in [FHS15], which give a standard-model construction of SPS-EQ under a q-type assumption, but which only provides a weaker form of privacy. Furthermore, it is an interesting question whether such signatures when built for other more general equivalence relations yield alternative and further applications.

Acknowledgments. Work done while the first author was at IST Austria and supported by the European Research Council, ERC Starting Grant (259668-PSPC). The work of the second author has been supported by the European Commission through project FP7-MATTHEW (GA No. 610436). The work of the last two authors has been supported by the European Commission through project FP7-FutureID, grant agreement number 318424 and by EU Horizon 2020 through project Prismacloud, grant agreement number 644962.

References

ABC$^+$12. Jae Hyun Ahn, Dan Boneh, Jan Camenisch, Susan Hohenberger, abhi shelat, and Brent Waters. Computing on authenticated data. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 1–20, Taormina, Sicily, Italy, March 19–21, 2012. Springer, Heidelberg, Germany.

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, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

AFG$^+$10. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany.

AGHO11. Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany.

AGOT14a. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Structure-preserving signatures from type II pairings. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 390–407, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

AGOT14b. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 688–712, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany.

AHO10. Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. http://eprint.iacr.org/2010/133.

AKOT15. Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Fully structure-preserving signatures and shrinking commitments. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 35–65, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

ALP12. Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Computing on authenticated data: New privacy definitions and constructions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 367–385, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

ALP13. Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 386–404, Nara, Japan, February 26 – March 1, 2013. Springer, Heidelberg, Germany.

AMO08. Norio Akagi, Yoshifumi Manabe, and Tatsuaki Okamoto. An efficient anonymous credential system. In Gene Tsudik, editor, *FC 2008: 12th International Conference on Financial Cryptography and Data Security*, volume 5143 of *Lecture Notes in Computer Science*, pages 272–286, Cozumel, Mexico, January 28–31, 2008. Springer, Heidelberg, Germany.

ASM06. Man Ho Au, Willy Susilo, and Yi Mu. Constant-size dynamic k-TAA. In Roberto De Prisco and Moti Yung, editors, *SCN 06: 5th International Conference on Security in Communication Networks*, volume 4116 of *Lecture Notes in Computer Science*, pages 111–125, Maiori, Italy, September 6–8, 2006. Springer, Heidelberg, Germany.

BB04. Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.

BBS04. Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

BC14. Dan Boneh and Henry Corrigan-Gibbs. Bivariate polynomials modulo composites and their applications. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 42–62, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer, Heidelberg, Germany.

BCC$^+$09. Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 108–125, Santa Barbara, CA, USA, August 16–20, 2009. Springer, Heidelberg, Germany.

BCKL08. Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374, San Francisco, CA, USA, March 19–21, 2008. Springer, Heidelberg, Germany.

BFF$^+$15. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In Jonathan Katz, editor, *PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography*, volume 9020 of *Lecture Notes in Computer Science*, pages 355–376, Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, Heidelberg, Germany.

BFKW09. Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters. Signing a linear subspace: Signature schemes for network coding. In Stanislaw Jarecki and Gene Tsudik, editors, *PKC 2009: 12th International Conference on Theory and Practice of Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 68–87, Irvine, CA, USA, March 18–20, 2009. Springer, Heidelberg, Germany.

BFPV11. Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011: 14th International Conference on Theory and Practice of Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 403–422, Taormina, Italy, March 6–9, 2011. Springer, Heidelberg, Germany.

BL13. Foteini Baldimtsi and Anna Lysyanskaya. Anonymous credentials light. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 13: 20th Conference on Computer and Communications Security*, pages 1087–1098, Berlin, Germany, November 4–8, 2013. ACM Press.

BN06. Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005: 12th Annual International Workshop on Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331, Kingston, Ontario, Canada, August 11–12, 2006. Springer, Heidelberg, Germany.

Boy08. Xavier Boyen. The uber-assumption family (invited talk). In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008: 2nd International Conference on Pairing-based Cryptography*, volume 5209 of *Lecture Notes in Computer Science*, pages 39–56, Egham, UK, September 1–3, 2008. Springer, Heidelberg, Germany.

Bra00. Stefan Brands. *Rethinking public-key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, 2000.

BSZ05. Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *Topics in Cryptology – CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 136–153, San Francisco, CA, USA, February 14–18, 2005. Springer, Heidelberg, Germany.

Can01. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science*, pages 136–145, Las Vegas, Nevada, USA, October 14–17, 2001. IEEE Computer Society Press.

CDHK15. Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss. Composable and modular anonymous credentials: Definitions and practical constructions. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 262–288, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

CDM00. Ronald Cramer, Ivan Damgård, and Philip D. MacKenzie. Efficient zero-knowledge proofs of knowledge without intractability assumptions. In Hideki Imai and Yuliang Zheng, editors, *PKC 2000: 3rd International Workshop on Theory and Practice in Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pages 354–372, Melbourne, Victoria, Australia, January 18–20, 2000. Springer, Heidelberg, Germany.

CF13. Dario Catalano and Dario Fiore. Vector commitments and their applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 55–72, Nara, Japan, February 26 – March 1, 2013. Springer, Heidelberg, Germany.

CFW12. Dario Catalano, Dario Fiore, and Bogdan Warinschi. Efficient network coding signatures in the standard model. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 680–696, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany.

CG12. Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. *ACM Transactions on Information and System Security*, 15(1):4, 2012.

CKL$^+$14. Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, and Michael Østergaard Pedersen. Formal treatment of privacy-enhancing credential systems. Cryptology ePrint Archive, Report 2014/708, 2014. http://eprint.iacr.org/2014/708.

CKLM12. Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable proof systems and applications. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 281–300, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany.

CKLM14. Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable signatures: New definitions and delegatable anonymous credentials. In *IEEE 27th Computer Security Foundations Symposium, CSF 2014*, pages 199–213, 2014.

CL01. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118, Innsbruck, Austria, May 6–10, 2001. Springer, Heidelberg, Germany.

CL03. Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02: 3rd International Conference on Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289, Amalfi, Italy, September 12–13, 2003. Springer, Heidelberg, Germany.

CL04. Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

CL11. Sébastien Canard and Roch Lescuyer. Anonymous credentials from (indexed) aggregate signatures. In *DIM'11, Proceedings of the 2013 ACM Workshop on Digital Identity Management, Chicago, IL, USA - October 21, 2011*, pages 53–62, 2011.

CL13. Sébastien Canard and Roch Lescuyer. Protecting privacy by sanitizing personal data: a new approach to anonymous credentials. In Kefei Chen, Qi Xie, Weidong Qiu, Ninghui Li, and Wen-Guey Tzeng, editors, *ASIACCS 13: 8th ACM Symposium on Information, Computer and Communications Security*, pages 381–392, Hangzhou, China, May 8–10, 2013. ACM Press.

CM11. Sanjit Chatterjee and Alfred Menezes. On cryptographic protocols employing asymmetric pairings - the role of Ψ revisited. *Discrete Applied Mathematics*, 159(13):1311–1322, 2011.

CP93. David Chaum and Torben P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology – CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105, Santa Barbara, CA, USA, August 16–20, 1993. Springer, Heidelberg, Germany.

Dam00. Ivan Damgård. Efficient concurrent zero-knowledge in the auxiliary string model. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 418–430, Bruges, Belgium, May 14–18, 2000. Springer, Heidelberg, Germany.

DHS15a. 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 *Lecture Notes in Computer Science*, pages 57–74, Oxford, UK, December 15–17, 2015. Springer, Heidelberg, Germany.

DHS15b. David Derler, Christian Hanser, and Daniel Slamanig. Revisiting cryptographic accumulators, additional properties and relations to other primitives. In Kaisa Nyberg, editor, *Topics in Cryptology – CT-RSA 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 127–144, San Francisco, CA, USA, April 20–24, 2015. Springer, Heidelberg, Germany.

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, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 233–253, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

FO98. Eiichiro Fujisaki and Tatsuaki Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 32–46, Espoo, Finland, May 31 – June 4, 1998. Springer, Heidelberg, Germany.

Fre12. David Mandell Freeman. Improved security for linearly homomorphic signatures: A generic framework. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 697–714, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany.

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 Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 224–245, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany.

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

Gha16. Essam Ghadafi. Short structure-preserving signatures. In Kazue Sako, editor, *Topics in Cryptology – CT-RSA 2016*, volume 9610 of *Lecture Notes in Computer Science*, pages 305–321, San Francisco, CA, USA, February 29 – March 4, 2016. Springer, Heidelberg, Germany.

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

Gro10. Jens Groth. Short pairing-based non-interactive zero-knowledge arguments. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 321–340, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany.

Gro15. Jens Groth. Efficient fully structure-preserving signatures for large messages. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 239–259, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

GS08. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432, Istanbul, Turkey, April 13–17, 2008. Springer, Heidelberg, Germany.

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: 20th European Symposium on Research in Computer Security, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 146–164, Vienna, Austria, September 21–25, 2015. Springer, Heidelberg, Germany.

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, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 491–511, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer, Heidelberg, Germany.

ILV11. Malika Izabachène, Benoît Libert, and Damien Vergnaud. Block-wise P-signatures and non-interactive anonymous credentials with efficient attributes. In Liqun Chen, editor, *13th IMA International Conference on Cryptography and Coding*, volume 7089 of *Lecture Notes in Computer Science*, pages 431–450, Oxford, UK, December 12–15, 2011. Springer, Heidelberg, Germany.

JMSW02. Robert Johnson, David Molnar, Dawn Xiaodong Song, and David Wagner. Homomorphic signature schemes. In Bart Preneel, editor, *Topics in Cryptology – CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 244–262, San Jose, CA, USA, February 18–22, 2002. Springer, Heidelberg, Germany.

KPW15. Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 275–295, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

KZG10. Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-size commitments to polynomials and their applications. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 177–194, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany.

Lip12. Helger Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 169–189, Taormina, Sicily, Italy, March 19–21, 2012. Springer, Heidelberg, Germany.

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, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 289–307, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

Mer88. Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378, Santa Barbara, CA, USA, August 16–20, 1988. Springer, Heidelberg, Germany.

MRK03. Silvio Micali, Michael O. Rabin, and Joe Kilian. Zero-knowledge sets. In *44th Annual Symposium on Foundations of Computer Science*, pages 80–91, Cambridge, Massachusetts, USA, October 11–14, 2003. IEEE Computer Society Press.

Ped92. Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140, Santa Barbara, CA, USA, August 11–15, 1992. Springer, Heidelberg, Germany.

PS16. David Pointcheval and Olivier Sanders. Short randomizable signatures. In Kazue Sako, editor, *Topics in Cryptology – CT-RSA 2016*, volume 9610 of *Lecture Notes in Computer Science*, pages 111–126, San Francisco, CA, USA, February 29 – March 4, 2016. Springer, Heidelberg, Germany.

SBZ02. Ron Steinfeld, Laurence Bull, and Yuliang Zheng. Content extraction signatures. In Kwangjo Kim, editor, *ICISC 01: 4th International Conference on Information Security and Cryptology*, volume 2288 of *Lecture Notes in Computer Science*, pages 285–304, Seoul, Korea, December 6–7, 2002. Springer, Heidelberg, Germany.

SNF11. Amang Sudarsono, Toru Nakanishi, and Nobuo Funabiki. Efficient proofs of attributes in pairing-based anonymous credential system. In *Privacy Enhancing Technologies - 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27-29, 2011. Proceedings*, pages 246–263, 2011.

Ver01. Eric R. Verheul. Self-blindable credential certificates from the Weil pairing. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 533–551, Gold Coast, Australia, December 9–13, 2001. Springer, Heidelberg, Germany.

Wat05. Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

A Security of Scheme 1

Here, we prove the security of Scheme 1, that is, its correctness and EUF-CMA security.

A.1 Proof of Theorem 1 (Correctness)

We have to show that for all $\kappa \in \mathbb{N}$, all $\ell > 1$, all choices of bilinear groups $\mathsf{BG} \overset{R}{\leftarrow} \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, all choices of key pairs $(\mathsf{sk}, \mathsf{pk}) \overset{R}{\leftarrow} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)$, all $M \in (\mathbb{G}_1^*)^\ell$ and all $\mu \in \mathbb{Z}_p^*$ the following holds:

$$\begin{gathered}\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1 \quad \wedge \\ \mathsf{Verify}_{\mathcal{R}}\big(M, \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk}), \mathsf{pk};\, y\big) = 1 \quad \forall\, y \in \mathbb{Z}_p^* \quad \wedge \\ \mathsf{Verify}_{\mathcal{R}}\big(\mathsf{ChgRep}_{\mathcal{R}}(M, \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk};\, y), \mu, \mathsf{pk};\, \psi), \mathsf{pk}\big) = 1 \quad \forall\, y, \psi \in \mathbb{Z}_p^* \ .\end{gathered}$$

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)$ returns $\mathsf{sk} \leftarrow (x_i)_{i\in[\ell]} \overset{R}{\leftarrow} (\mathbb{Z}_p^*)^\ell$ and $\mathsf{pk} \leftarrow (x_i\hat{P})_{i\in[\ell]}$, which shows the first equation.

$\mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk}; y)$ returns $Z = y\sum_{i\in[\ell]} x_i M_i$, $Y = \frac{1}{y}P$ and $\hat{Y} = \frac{1}{y}\hat{P}$. Plugging this into the first relation in $\mathsf{Verify}_{\mathcal{R}}$, we get

$$e(Z, \hat{Y}) = e\big(y\textstyle\sum_{i\in[\ell]} x_i M_i, \frac{1}{y}\hat{P}\big) = e\big(\textstyle\sum_{i\in[\ell]} x_i M_i, \hat{P}\big)^{y\cdot\frac{1}{y}} = \textstyle\prod_{i\in[\ell]} e(x_i M_i, \hat{P}) = \prod_{i\in[\ell]} e(M_i, \hat{X}_i) \ .$$

Since $e(Y, \hat{P}) = e(\frac{1}{y}P, \hat{P}) = e(P, \frac{1}{y}\hat{P}) = e(P, \hat{Y})$, the second verification equation is also satisfied.

Finally, $\mathsf{ChgRep}_{\mathcal{R}}\big(M, (Z = y\sum_{i\in[\ell]} x_i M_i, Y = \frac{1}{y}P, \hat{Y} = \frac{1}{y}\hat{P}), \mu, \mathsf{pk};\, \psi\big)$ outputs μM and

$$\sigma' = \big(\psi\mu Z,\ \tfrac{1}{\psi}Y,\ \tfrac{1}{\psi}\hat{Y}\big) = \big(\psi y \textstyle\sum_{i\in[\ell]} x_i \mu M_i,\ \frac{1}{\psi}\frac{1}{y}P,\ \frac{1}{\psi}\frac{1}{y}\hat{P}\big) \ ,$$

which is the same as $\mathsf{Sign}_{\mathcal{R}}(\mu M, \mathsf{sk}; (\psi y))$, and thus verifies by correctness of $\mathsf{Sign}_{\mathcal{R}}$. □

A.2 Proof of Theorem 2 (Unforgeability)

In the generic-group model an adversary only performs generic group operations (operations in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, pairings and equality tests) by querying the respective group oracle.

We first consider the messages submitted to the signing oracle and the forgery output by the adversary as formal multivariate Laurent polynomials whose variables correspond to the secret values chosen by the challenger, and show that an adversary is unable to symbolically produce an existential forgery (even when message elements are adaptively chosen). Then, in the second part we show that the probability for an adversary to produce an existential forgery by chance is negligible.

The values chosen by the challenger in the unforgeability game, which are unknown to the adversary, are $x_1, \dots, x_\ell$ used in the public keys $(\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$ and the values y_j, $j \in [q]$, picked for the j-th signature, that is, when the j-th signing query for a message $(M_{j,i})_{i\in[\ell]}$ is answered as

$$(Z_j, Y_j, \hat{Y}_j) = (y_j \textstyle\sum_{i\in[\ell]} x_i M_{j,i}, \frac{1}{y_j} P, \frac{1}{y_j} \hat{P}) \ .$$

When outputting a forgery $(Z^*, Y^*, \hat{Y}^*)$ for a message $(M_i^*)_{i\in[\ell]}$, the elements the adversary has seen are $(Z_j, Y_j)_{j\in[q]}$ in $\mathbb{G}_1$, and $(\hat{Y}_j)_{j\in[q]}$ as well as $(\hat{X}_i)_{i\in[\ell]}$ in $\mathbb{G}_2$. The forgery must thus have been computed by choosing

$$\pi_z, \pi_y, \pi_{\hat{y}}, \pi_{m^*,i}, \rho_{z,j}, \rho_{y,j}, \rho_{m^*,i,j}, \psi_{y,j}, \psi_{\hat{y},j}, \psi_{m^*,i,j}, \chi_{\hat{y},i} \in \mathbb{Z}_p \ \text{ for } \ j \in [q] \text{ and } i \in [\ell]$$

and setting

$$Z^* = \pi_z P + \sum_{j\in[q]} \rho_{z,j} Z_j + \sum_{j\in[q]} \psi_{z,j} Y_j \qquad Y^* = \pi_y P + \sum_{j\in[q]} \rho_{y,j} Z_j + \sum_{j\in[q]} \psi_{y,j} Y_j$$
$$\hat{Y}^* = \pi_{\hat{y}} \hat{P} + \sum_{i\in[\ell]} \chi_{\hat{y},i} \hat{X}_i + \sum_{j\in[q]} \psi_{\hat{y},j} \hat{Y}_j \qquad M_i^* = \pi_{m^*,i} P + \sum_{j\in[q]} \rho_{m^*,i,j} Z_j + \sum_{j\in[q]} \psi_{m^*,i,j} Y_j$$

Similarly, for all $j \in [q]$ the message $(M_{j,i})_{i\in[\ell]}$ submitted in the j-th query is computed as a linear combination of all the $\mathbb{G}_1$ elements the adversary has seen so far, that is,

$$P, Z_1, Y_1, \dots, Z_{j-1}, Y_{j-1} \ .$$

By considering all these group elements and taking their discrete logarithms to the bases P and $\hat{P}$, respectively, we obtain the following linear combinations:

$$z^* = \pi_z + \sum_{j\in[q]} \rho_{z,j} z_j + \sum_{j\in[q]} \psi_{z,j} \frac{1}{y_j}$$
$$y^* = \pi_y + \sum_{j\in[q]} \rho_{y,j} z_j + \sum_{j\in[q]} \psi_{y,j} \frac{1}{y_j}$$
$$\hat{y}^* = \pi_{\hat{y}} + \sum_{i\in[\ell]} \chi_{\hat{y},i} x_i + \sum_{j\in[q]} \psi_{\hat{y},j} \frac{1}{y_j}$$
$$m_i^* = \pi_{m^*,i} + \sum_{j\in[q]} \rho_{m^*,i,j} z_j + \sum_{j\in[q]} \psi_{m^*,i,j} \frac{1}{y_j}$$
$$m_{j,i} = \pi_{m,j,i} + \sum_{k\in[j-1]} \rho_{m,j,i,k} z_k + \sum_{k\in[j-1]} \psi_{m,j,i,k} \frac{1}{y_k}$$

Observe that all message elements as well as the elements $Y^*, \hat{Y}^*$ of the forgery must be different from $0_{\mathbb{G}_1}$ and $0_{\mathbb{G}_2}$, respectively, by definition. Plugging the forgery into the verification relations yields:

$$\prod_{i\in[\ell]} e(M_i^*, \hat{X}_i) = e(Z^*, \hat{Y}^*) \quad \wedge \quad e(Y^*, \hat{P}) = e(P, \hat{Y}^*)$$

and taking discrete logarithms to the basis $e(P, \hat{P})$ in $\mathbb{G}_T$, we obtain the following equations:

$$\sum_{i\in[\ell]} m_i^* x_i = z^* \hat{y}^* \tag{6}$$

$$y^* = \hat{y}^* \tag{7}$$

The values m_i^*, z^*, $\hat{y}^*$, y^* are multivariate Laurent polynomials of total degree $O(q)$ in $x_1, \ldots, x_\ell, y_1, \ldots,$ y_q. Our further analysis will be simplified by the following fact.

Claim 1. *For all $n \geq 1$, the monomials that constitute z_n have the form*

$$\frac{1}{y_s^b} \prod_{k\in[t]} y_{j_k} \prod_{k\in[t]} x_{i_k} \tag{8}$$

with $1 \leq t \leq n$; for all $k_1 \neq k_2$: $j_{k_1} \neq j_{k_2}$; for all k: $j_k \leq n \wedge s < j_k$; $j_t = n$; and $b \in \{0, 1\}$.

Proof. We prove the claim by induction on n.

$\underline{n = 1}$: As before the first signing query, the only element from $\mathbb{G}_1$ available to the adversary is P, we have $m_{1,i} = \pi_{m,1,i}$ and therefore

$$z_1 = \sum_{i\in[\ell]} \pi_{m,1,i} y_1 x_i \quad ,$$

which proves the base case.

$\underline{n \to n+1}$: Assume for all $k \in [n]$ the monomials of all z_k are of the form in (8). Since

$$m_{n+1,i} = \pi_{m,n+1,i} + \textstyle\sum_{k\in[n]} \rho_{m,n+1,i,k} z_k + \sum_{k\in[n]} \psi_{m,n+1,i,k} \frac{1}{y_k} \quad ,$$

by the definition of $\mathsf{Sign}_{\mathcal{R}}$ we have

$$z_{n+1} = \sum_{i\in[\ell]} \pi_{m,n+1,i}\, y_{n+1} x_i + \sum_{i\in[\ell]} \sum_{k\in[n]} \rho_{m,n+1,i,k}\, y_{n+1} z_k x_i + \sum_{i\in[\ell]} \sum_{k\in[n]} \psi_{m,n+1,i,k}\, y_{n+1} \frac{1}{y_k} x_i \quad . \tag{9}$$

The monomials in the first and the last sum are as claimed in the statement. By the induction hypothesis any monomial contained in any z_k is of the form $\frac{1}{y_s^b} \prod_{p\in[t]} y_{j_p} \prod_{p\in[t]} x_{i_p}$, with $t \leq n$, $j_t = k$ and $s < j_p$ for all j_p as well as $j_p < k$, for all j_p with $p < t$ (which are all different). Each such monomial leads thus to a monomial in the 2nd sum in (9) of the form $\frac{1}{y_s^b} \left(y_{n+1} \prod_{p\in[t]} y_{j_p}\right)\left(x_i \prod_{p\in[t]} x_{i_p}\right) = \frac{1}{y_s^b} \prod_{p\in[t']} y_{j_p} \prod_{p\in[t']} x_{i_p}$, with $t' := t+1 \leq n+1$, $j_{t'} := n+1$, $i_{t+1} := i$. Moreover $t' \leq n+1$, all j_p are still different and $\leq n$ and $s < j_p$ for all j_p, which proves the induction step.

Together this proves the claim. □

We will in particular use that by Claim 1 in any monomial in z_k there are always exactly as many y's as x's in the numerator and there are at least one y and one x; moreover there is at most one y in the denominator (and which does not cancel down). Moreover, we have:

Corollary 1. *Any monomial can only occur in one unique z_n.*

Proof. This is implied by Claim 1 as follows: For any monomial, let i^* be maximal such that the monomial contains y_{i^*}. Then the monomial does not occur in z_n with $n > i^*$, since z_n contains y_n contradicting maximality. It does not occur in z_n with $n < i^*$ either, since all y_j contained in z_n have $j \leq n$, meaning y_{i^*} does not occur in z_n; a contradiction. □

We start by investigating Equation (7):

$$y^* = \hat{y}^*$$

$$\pi_y + \sum_{j\in[q]} \rho_{y,j} z_j + \sum_{j\in[q]} \psi_{y,j} \frac{1}{y_j} = \pi_{\hat{y}} + \sum_{i\in[\ell]} \chi_{\hat{y},i} x_i + \sum_{j\in[q]} \psi_{\hat{y},j} \frac{1}{y_j}$$

By equating coefficients, and taking into account that by Claim 1 no z_j contains monomials of the form $1, x_i$, or $\frac{1}{y_j}$, we obtain $\rho_{y,j} = 0$ for all $j \in [q]$ and

(i) $\pi_{\hat{y}} = \pi_y$
(ii) $\chi_{\hat{y},i} = 0 \quad \forall i \in [\ell]$
(iii) $\psi_{\hat{y},j} = \psi_{y,j} \quad \forall j \in [q]$

Let us now investigate Equation (6) (where in $\hat{y}^*$ we replace $\pi_{\hat{y}}, \chi_{\hat{y},i}$ and $\psi_{\hat{y},j}$ as per (i), (ii) and (iii), respectively):

$$\sum_{i\in[\ell]} m_i^* x_i = z^* \hat{y}^*$$

$$\sum_{i\in[\ell]} \Big(\pi_{m^*,i} + \sum_{j\in[q]} \rho_{m^*,i,j} z_j + \sum_{j\in[q]} \psi_{m^*,i,j} \frac{1}{y_j}\Big) x_i = \Big(\pi_z + \sum_{j\in[q]} \rho_{z,j} z_j + \sum_{j\in[q]} \psi_{z,j} \frac{1}{y_j}\Big)\Big(\pi_y + \sum_{k\in[q]} \psi_{y,k} \frac{1}{y_k}\Big)$$

$$= \pi_z \pi_y + \sum_{j\in[q]} \rho_{z,j} \pi_y \, z_j + \sum_{j\in[q]} \big(\psi_{z,j}\pi_y + \pi_z \psi_{y,j}\big) \frac{1}{y_j} + \sum_{j\in[q]} \sum_{k\in[q]} \rho_{z,j} \psi_{y,k} \frac{1}{y_k} z_j + \sum_{j\in[q]} \sum_{k\in[q]} \psi_{z,j} \psi_{y,k} \frac{1}{y_j y_k}$$

Equating coefficients for 1, we get:

(iv) $\pi_z \pi_y = 0$

Since by Claim 1, no terms in $z_j x_i$, z_j and $\frac{1}{y_k} z_j$ are of the form $\frac{1}{y_j}$ or $\frac{1}{y_j y_k}$, equating coefficients for $\frac{1}{y_j}$ and $\frac{1}{y_j y_k}$ yields:

(v) $\psi_{z,j}\pi_y + \pi_z \psi_{y,j} = 0 \quad \forall j \in [q]$
(vi) $\psi_{z,j} \psi_{y,k} = 0 \quad \forall j, k \in [q]$

By (iv)–(vi), we have simplified Equation (6) to the following:

$$\sum_{i\in[\ell]} \Big(\pi_{m^*,i} + \sum_{j\in[q]} \rho_{m^*,i,j} z_j + \sum_{j\in[q]} \psi_{m^*,i,j} \frac{1}{y_j}\Big) x_i = \sum_{j\in[q]} \rho_{z,j} \pi_y \, z_j + \sum_{j\in[q]} \sum_{k\in[q]} \rho_{z,j} \psi_{y,k} \frac{1}{y_k} z_j \quad . \tag{10}$$

Let us analyze the monomials contained in the z_j's. By (8) in Claim 1, there is an equal number of y's and x's in numerators of such monomials. Therefore, on the LHS the number of x's in all monomials is always greater than that of y's, meaning monomials of type (8) only occur on the RHS of (10).

We now show that $\rho_{z,n} \pi_y \, z_n = 0$ for all $n \in [q]$. Assume that for some $n \in [q]$ this is not the case. Since none of the monomials in z_n can appear on the LHS and by Corollary 1, they do not appear in any other z_i, $i \neq n$, z_n must be subtracted by a term contained in $\frac{1}{y_k} z_j$ for some $j, k \in [q]$. The term in this z_j must not have y_k in the numerator, as otherwise it would cancel down and the number of y's and x's would be different, meaning it would not correspond to any monomial in z_n (which are of the form (8)). This also means that any monomial contained in z_n (in the first sum on the RHS) must have y_k in the denominator if it is to be equal to a term in $\frac{1}{y_k} z_j$.

Next, we observe that monomials in z_n can only be equal to terms in $\frac{1}{y_k} z_j$ if $j = n$. This is because the maximal i^* with y_{i^*} appearing in z_n would be different for any other z_j, $j \neq n$ (cf. the proof of Corollary 1). But this means that any monomial in z_n, which by the above must have y_k in the denominator, also occurs in the z_n in the double sum, yielding a term with y_k^2 in the denominator. Since this cannot occur anywhere else in the equation by Corollary 1, we arrived at a contradiction. We have thus:

(vii) $\rho_{z,j} \pi_y \, z_n = 0 \quad \forall j \in [q]$

Equation (6) has now the following, simplified representation:

$$\sum_{i \in [\ell]} \Big(\pi_{m^*,i} + \sum_{j \in [q]} \rho_{m^*,i,j} z_j + \sum_{j \in [q]} \psi_{m^*,i,j} \frac{1}{y_j} \Big) x_i = \sum_{j \in [q]} \sum_{k \in [q]} \rho_{z,j} \psi_{y,k} \frac{1}{y_k} z_j \tag{11}$$

From Claim 1 we have that every monomial of z_j has an equal number of y's and x's in the numerator; for all monomials of the LHS we thus have: (number of y's) = (number of x's) − 1. For such a term to occur on the RHS, this has to be a monomial N in z_j that has y_k in the numerator, so it cancels down and leads to a term with more x's than y's. We show that this must be z_k, that is, we show that $\rho_{z,j} \psi_{y,k} = 0$ for all $j \neq k$.

First this holds for $k > j$, since the "largest" y contained in z_j is y_j and thus y_k does not cancel. Second for $k < j$, let us assume that there is at least one pair of coefficients $\rho_{z,j} \psi_{y,k} \neq 0$ with $k < j$. Observe that $\frac{1}{y_k} z_j$ on the RHS still contains y_j as "largest" y-value (by Claim 1). The monomials composing $\frac{1}{y_k} z_j$ do thus only occur in z_j on the LHS, thus $\rho_{m^*,i,j} \neq 0$ for some $i \in [\ell]$. Thus the monomial N from z_j on the RHS which contains y_k also occurs on the LHS. However, as by Claim 1 every y occurs only once in every monomial, after canceling out y_k from z_j no y_k remains in N on the RHS. As however, y_k is present in the corresponding monomial in z_j on the LHS, there is no corresponding term on the RHS. A contradiction. We thus obtain:

(viii) $\rho_{z,j} \psi_{y,k} = 0 \quad \forall j, k \in [q], j \neq k$

Since the RHS of (11) cannot be 0 (otherwise all m_i^* on the LHS would be 0, which is not a valid forgery), we have:

(ix) $\exists\, k \in [q] : \rho_{z,k} \psi_{y,k} \neq 0$

We now argue that there exists exactly one such k, which follows from the following basic fact:

Claim 2. *Let $a, b \in \mathbb{Z}_p^q$ be two non-zero vectors. If $C = a \cdot b^\top$ is a diagonal matrix then at most one element in C is non-zero.*

Proof. C is diagonal, so rank(C) = #(non-zero rows in C) = #(non-zero elements in C). From basic linear algebra we have rank(a) = rank($b^\top$) = 1 and rank(C) ≤ min{rank(a), rank($b^\top$)} = 1. □

Applying this to $C := (\rho_{z,j})_{j \in [q]} \cdot (\psi_{y,k})_{k \in [q]}^\top$, which by (viii) and (ix) is a non-zero diagonal matrix, we get that all but one element of the diagonal $(\rho_{z,k} \psi_{y,k})_{k \in [q]}$ are zero, that is:

(x) $\exists!\, n \in [q] : \rho_{z,n} \psi_{y,n} \neq 0$

By (viii) and (x), Equation (6) simplifies to

$$\begin{aligned}\sum_{i\in[\ell]}\Big(\pi_{m^*,i}+\sum_{j\in[q]}\rho_{m^*,i,j}z_j+\sum_{j\in[q]}\psi_{m^*,i,j}\frac{1}{y_j}\Big)x_i &= \rho_{z,n}\psi_{y,n}\frac{1}{y_n}z_n\\ &= \rho_{z,n}\psi_{y,n}\sum_{i\in[\ell]}m_{n,i}x_i\\ &= \rho_{z,n}\psi_{y,n}\sum_{i\in[\ell]}\Big(\pi_{m,n,i}+\sum_{j\in[n-1]}\rho_{m,n,i,j}z_j+\sum_{j\in[n-1]}\psi_{m,n,i,j}\frac{1}{y_j}\Big)x_i\ ,\end{aligned}$$

where in the 2nd line we substituted z_n by its definition, namely $y_n\sum_{k\in[\ell]}m_{n,k}x_k$, and in the 3rd line we replaced $m_{n,i}$ by its definition. Since by Claim 1, x_i, z_jx_i and $\frac{1}{y_j}x_i$, for all $i\in[\ell], j\in[q]$, do not have common monomials, equating coefficients yields (with $\alpha := \rho_{z,n}\psi_{y,n}$):

$$\pi_{m^*,i}=\alpha\,\pi_{m,n,i}\qquad\qquad \rho_{m^*,i,j}=\alpha\,\rho_{m,n,i,j}\qquad\qquad \psi_{m^*,i,j}=\alpha\,\psi_{m,n,i,j}$$

This finally means that the message for the forgery is just a multiple of the previously queried message M_n, which completes the first part of the proof.

It remains to show that the probability that an adversary produces an existential forgery by "accident", i.e., that two formally different polynomials collide by evaluating to the same value (or, equivalently, that the difference polynomial evaluates to zero), is negligible. Suppose that the adversary makes q queries to the signing oracle and $O(q)$ queries to the group oracles. Then, all involved formal polynomials resulting from querying the group oracles are of degree $O(q)$ and overall there are $O(\binom{q}{2})=O(q^2)$ polynomials that could collide (i.e. whose difference polynomial evaluates to zero). Then, by the Schwartz-Zippel lemma and the collision argument, the probability of such an error in the simulation of the generic group is $O(\frac{q^3}{p})$ and is, therefore negligible in the security parameter. □

B Security of Scheme 2

B.1 Proof of Theorem 7 (Unforgeability)

In the proof of unforgeability we distinguish whether the adversary wins the game by forging a signature, breaking subset-opening soundness of the commitment scheme or computing a discrete logarithm. We can efficiently determine which was the case since the knowledge extractor of the ZKPoK $\Pi^{\mathcal{R}_\mathsf{F}}$ lets us extract the credential used by the adversary.

Proof. We first introduce the following syntactic changes to the experiment, which let us distinguish different types of forgeries: (1) We include the value R in credentials cred output by Obtain (these belong to honest users and are now of the form $\mathsf{cred}=((C,R),\sigma,r,O'))$. (2) When the adversary makes a valid call to $\mathcal{O}^{\mathsf{Issue}}$, the experiment receives the values C,R and produces a signature σ; instead of appending $\perp$ to the list $\mathtt{CRED}$, the oracle now appends $((C,R),\sigma,\perp,\perp)$. Note that the adversary's view in the experiment remains unchanged.

Assume now an efficient adversary $\mathcal{A}$ wins the unforgeability game (Definition 25) with non-negligible probability and let $((C_1^*,C_2^*,C_3^*),\sigma^*)$ be the message-signature pair it uses and W^* be the witness for an attribute set $\mathtt{A}'^*\not\subseteq\mathtt{ATTR}[j]$, for all j with $\mathtt{I2U}[j]\in\mathtt{KU}\cup\mathtt{CU}$; moreover, the ZKPoK $\Pi^{\mathcal{R}_\mathsf{F}}(C_1^*,C_2^*,C_3^*)$ verifies. We distinguish the following cases:

Type 1: $[(C_1^*, C_2^*, C_3^*)]_{\mathcal{R}} \neq [(C, R, P)]_{\mathcal{R}}$ for $((C, R), \sigma, *, *) = \mathtt{CRED}[j]$ for all issuance indexes j (i.e., $\mathtt{I2U}[j] \in \mathtt{HU} \cup \mathtt{KU} \cup \mathtt{CU}$). The pair $((C_1^*, C_2^*, C_3^*), \sigma^*)$ is thus a signature forgery and using $\mathcal{A}$ we construct an adversary $\mathcal{B}$ that breaks the EUF-CMA security of the SPS-EQ scheme.

Type 2: $[(C_1^*, C_2^*, C_3^*)]_{\mathcal{R}} = [(C, R, P)]_{\mathcal{R}}$ where $((C, R), \sigma, *, *) = \mathtt{CRED}[j]$ for some index j with $\mathtt{I2U}[j] \in \mathtt{KU} \cup \mathtt{CU}$. Since $\mathcal{A}$ only wins if $\mathtt{A}' \not\subseteq \mathtt{ATTR}[j]$, it must have broken subset soundness. We use $\mathcal{A}$ to construct an adversary $\mathcal{B}$ that breaks subset soundness of the set-commitment scheme SC.

Type 3: $[(C_1^*, C_2^*, C_3^*)]_{\mathcal{R}} = [(C, R, P)]_{\mathcal{R}}$ where $((C, R), \sigma, r, O') = \mathtt{CRED}[j]$ for some index j with $\mathtt{I2U}[j] \in \mathtt{HU}$. Then, we use $\mathcal{A}$ to break q-co-DLP.

Type 1. This reduction is straightforward. $\mathcal{B}$ interacts with a challenger $\mathcal{C}$ in the EUF-CMA game for SPS-EQ and $\mathcal{B}$ simulates the ABC-unforgeability game for $\mathcal{A}$.

$\mathcal{C}$ runs $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^3)$ and gives pk to $\mathcal{B}$. Then, $\mathcal{B}$ picks $a \xleftarrow{R} \mathbb{Z}_p$, defines $\mathsf{pp_{sc}} \leftarrow (\mathsf{BG}, (a^i P, a^i \hat{P})_{i \in [t]})$ and sets $(\mathsf{osk}, \mathsf{opk}) \leftarrow ((a, \perp), (\mathsf{pp_{sc}}, \mathsf{pk}))$. It next runs $\mathcal{A}(\mathsf{opk})$ and simulates the environment and the oracles. All oracles are as in the real game, except for the following oracles, which use the signing oracle instead of the signing key sk:

$\mathcal{O}^{\mathsf{ObtIss}}(i, \mathtt{A})$: $\mathcal{B}$ computes $(C,' O) \xleftarrow{R} \mathsf{Commit}'(\mathsf{pp_{sc}}, \mathtt{A}, \mathtt{USK}[i])$, chooses $r \xleftarrow{R} \mathbb{Z}_p^*$ and queries its oracle $\mathsf{Sign}_{\mathcal{R}}(\cdot, \mathsf{sk})$ on $(C, r \cdot C, P)$ to obtain σ; $\mathcal{B}$ appends $(i, ((C, r \cdot C), \sigma, r, O'), \mathtt{A})$ to $(\mathtt{I2U}, \mathtt{CRED}, \mathtt{ATTR})$.

$\mathcal{O}^{\mathsf{Issue}}(i, \mathtt{A})$: $\mathcal{B}$ runs this oracle by running the simulator $\mathcal{S}$ of ZKPoK $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ (as it does not know $\mathsf{sk} = \mathsf{osk}[2]$), and instead of signing (C, R, P), $\mathcal{B}$ obtains the signature σ from $\mathcal{C}$'s signing oracle. If successful, $\mathcal{B}$ appends $(i, ((C, R), \sigma, \perp, \perp), \mathtt{A})$ to $(\mathtt{I2U}, \mathtt{CRED}, \mathtt{ATTR})$ and returns $\top$.

Note that by perfect zero-knowledge of $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ the simulation of $\mathcal{O}^{\mathsf{Issue}}$ is perfect, and so is that of $\mathcal{O}^{\mathsf{ObtIss}}$. When $\mathcal{A}$ outputs $(\mathtt{A}'^*, \mathsf{st})$, $\mathcal{B}$ runs $\mathcal{A}(\mathsf{st})$ and interacts with $\mathcal{A}$ as verifier in a showing protocol. If $\mathcal{A}$ delivers a valid showing using $((C_1^*, C_2^*, C_3^*), \sigma^*)$ and conducting $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1^*, C_2^*, C_3^*)$ then $\mathcal{B}$ runs the knowledge extractor of $\Pi^{\mathcal{R}_{\mathsf{F}}}$ to obtain a witness $w = (r'', \mu)$ with $C_3^* = \mu P$. If there is a credential $\perp \neq ((C', R'), \sigma', *, *) \in \mathtt{CRED}$ such that $(C', R', P) = \mu^{-1} \cdot (C_1^*, C_2^*, C_3^*)$ then $\mathcal{B}$ aborts. (In this case, the forgery is not of Type 1.) Otherwise, $\mathcal{B}$ has never queried a signature for class $[(C_1^*, C_2^*, C_3^*)]_{\mathcal{R}}$ and outputs $((C_1^*, C_2^*, C_3^*), \sigma^*)$, which is a forgery. $\mathcal{B}$ breaks thus EUF-CMA of $\mathsf{SPS\text{-}EQ}$.

Type 2. $\mathcal{B}$ interacts with the challenger $\mathcal{C}$ in the subset-soundness game for SC for some $t > 0$. First, $\mathcal{C}$ generates set-commitment parameters $\mathsf{pp_{sc}} \leftarrow (\mathsf{BG}, (a^i P, a^i \hat{P})_{i \in [t]})$ with $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$ $= \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$ and sends $\mathsf{pp_{sc}}$ to $\mathcal{B}$. $\mathcal{B}$ generates a key pair $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^3)$, sets $(\mathsf{osk}, \mathsf{opk})$ $\leftarrow ((\perp, \mathsf{sk}), (\mathsf{pp_{sc}}, \mathsf{pk}))$ and runs $\mathcal{A}(\mathsf{opk})$, simulating the oracles. All oracles are as in the real game, except for $\mathcal{O}^{\mathsf{ObtIss}}$, in which $\mathcal{B}$ simply ignores the first two moves, and $\mathcal{O}^{\mathsf{Issue}}$, which is simulated as follows (as $\mathcal{B}$ does not know $a = \mathsf{osk}[1]$):

$\mathcal{O}^{\mathsf{Issue}}(i, \mathtt{A})$: The oracle is simulated as prescribed except for running the simulator for $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$. When $\mathcal{A}$ conducts $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})$, $\mathcal{B}$ runs the extractor for $\Pi^{\mathcal{R}_{\mathsf{UK}}}$ to extract usk and sets $\mathtt{USK}[i] \leftarrow \mathsf{usk}$.

By perfect zero-knowledge of $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ the simulation of the oracle $\mathcal{O}^{\mathsf{Issue}}$ is perfect. Moreover, note that $\mathcal{B}$ stores the secret keys of all users (all $i \in \mathtt{HU} \cup \mathtt{KU} \cup \mathtt{CU}$).

When $\mathcal{A}$ outputs $(\mathtt{A}'^*, \mathsf{st})$, $\mathcal{B}$ runs $\mathcal{A}(\mathsf{st})$ and interacts with $\mathcal{A}$ as verifier in a showing protocol. Assume $\mathcal{A}$ delivers a valid showing using $((C_1^*, C_2^*, C_3^*), \sigma^*)$ and a witness W^* for the attribute set $\mathtt{A}'^*$ such that $\mathtt{A}'^* \not\subseteq \mathtt{ATTR}[j]$ for all j with $\mathtt{I2U}[j] \in \mathtt{KU} \cup \mathtt{CU}$ and by conducting $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1^*, C_2^*, C_3^*)$. Then $\mathcal{B}$ runs the knowledge extractor of $\Pi^{\mathcal{R}_{\mathsf{F}}}$ to obtain a witness $w = (r'', \mu)$ such that $C_3^* = \mu P$. Let $(C', R', P) = \mu^{-1} \cdot (C_1^*, C_2^*, C_3^*)$; if there is no credential $\perp \neq ((C', R'), *, *, *) \in \mathtt{CRED}$ then $\mathcal{B}$ aborts (the forgery was of Type 1). Otherwise, let j^* be such that $((C', R'), *, *, *) = \mathtt{CRED}[j^*]$. If $\mathtt{I2U}[j^*] \in \mathtt{HU}$ then $\mathcal{B}$ aborts (the forgery was of Type 3). Else, we have $\mathtt{I2U}[j^*] \in \mathtt{KU} \cup \mathtt{CU}$ and $\mathtt{A}'^* \not\subseteq \mathtt{ATTR}[j^*]$. If for some $a' \in \mathtt{ATTR}[j^*] : a'P = aP$ then $\mathcal{B}$ sets $O^* \leftarrow (1, a', \mathtt{ATTR}[j^*])$. Else, $\mathcal{B}$ sets

$O^* \leftarrow (0, \mu \cdot \mathtt{USK}[\mathtt{I2U}[j^*]], \mathtt{ATTR}[j^*])$. $\mathcal{B}$ outputs $(C_1^*, O^*, \mathtt{A}'^*, W^*)$, which satisfies $\mathtt{A}'^* \not\subseteq \mathtt{ATTR}[j^*] \neq \perp$ and $\mathsf{VerifySubset}(\mathsf{pp_{sc}}, C_1^*, \mathtt{A}'^*, W^*) = 1$. $\mathcal{B}$'s output breaks thus subset soundness of SC.

Type 3. We assume the forgery to be of Type 3 and use a sequence of games which are indistinguishable under q-co-DL. Henceforth, we denote the event that an adversary wins Game i by S_i.

Game 0: The original game, which only outputs 1 if the forgery is of Type 3.

Game 1: As Game 0, except for the following oracles:

$\mathcal{O}^{\mathsf{ObtIss}}(i, \mathtt{A})$: As in Game 0, except that the experiment aborts if set commitment trapdoor $a \in \mathtt{A}$.

$\mathcal{O}^{\mathsf{Issue}}(i, \mathtt{A})$: Analogous to $\mathcal{O}^{\mathsf{ObtIss}}$.

Game 0 → Game 1: If $\mathcal{A}$ queries a set $\mathtt{A}$ with $a \in \mathtt{A}$ to one of the two oracles then this breaks the q-co-DL assumption for $q = t$ and $\mathsf{BG} = \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$. Denoting by $\epsilon_{qDL}(\kappa)$ the advantage of solving the q-co-DL assumption, we have thus

$$|\Pr[S_0] - \Pr[S_1]| \leq \epsilon_{qDL}(\kappa) \ . \tag{12}$$

Game 2: As Game 1, with the difference that the oracle $\mathcal{O}^{\mathsf{Show}}$ is run as follows:

$\mathcal{O}^{\mathsf{Show}}(j, \mathtt{A}')$: As in Game 0, but the ZKPoK $\Pi^{\mathcal{R}_\mathsf{F}}(C_1, C_2, C_3)$ is simulated.

Game 1 → Game 2: By the perfect zero-knowledge property of $\Pi^{\mathcal{R}_\mathsf{F}}$, we have that

$$\Pr[S_1] = \Pr[S_2] \ . \tag{13}$$

Game 3: As Game 2, except that oracle $\mathcal{O}^{\mathtt{HU}+}$ is run as follows:

$\mathcal{O}^{\mathtt{HU}+}(i)$: As in Game 0, but when executing $\mathsf{UserKeyGen}(1^\kappa)$, the experiment draws $\mathsf{usk} \xleftarrow{R} \mathbb{Z}_p$ instead of $\mathsf{usk} \xleftarrow{R} \mathbb{Z}_p^*$ and it aborts if $\mathsf{usk} = 0$.

Game 2 → Game 3: Denoting by q_u the number of queries to $\mathcal{O}^{\mathtt{HU}+}$, we have

$$|\Pr[S_2] - \Pr[S_3]| \leq \tfrac{q_u}{p} \ . \tag{14}$$

Game 4: As Game 3, except that when $\mathcal{A}$ eventually delivers a valid showing by conducting $\Pi^{\mathcal{R}_\mathsf{F}}(C_1^*, C_2^*, C_3^*)$, the experiment runs the knowledge extractor of $\Pi^{\mathcal{R}_\mathsf{F}}$ and extracts a witness w.

Game 3 → Game 4: This change is only conceptual and we have

$$\Pr[S_3] = \Pr[S_4] \ . \tag{15}$$

Game 5: As Game 4, except that we pick an index $k \xleftarrow{R} [q_o]$, where q_o is the number of queries to $\mathcal{O}^{\mathsf{ObtIss}}$. The extracted witness w is such that $w = (r, \mu) \in (\mathbb{Z}_p^*)^2$ and $C_2^* = rC_1^*$ and $C_3^* = \mu P$ and if credential $((C', R'), \sigma', r', O') \leftarrow \mathtt{CRED}[k]$ is such that $(C', R', P) \neq \mu^{-1} \cdot (C_1^*, C_2^*, C_3^*)$ then the experiment aborts. Furthermore, we change the executions of the following oracle:

$\mathcal{O}^{\mathtt{KU}+}(i)$: As in Game 0, except that the experiment aborts when $i = \mathtt{I2U}[k]$.

Game 4 → Game 5: Note that when the forgery is of Type 3 then there exists some j s.t. for $\mathtt{CRED}[j] = ((C', R'), \sigma', r', O')$ we have $(C', R', P) = \mu^{-1} \cdot (C_1^*, C_2^*, C_3^*)$; moreover, $\mathtt{I2U}[j] \in \mathtt{HU}$. With probability $\frac{1}{q_o}$ we have $k = j$, in which case the experiment does not abort, i.e., we have

$$\Pr[S_5] \geq \tfrac{1}{q_o} \Pr[S_4] \ . \tag{16}$$

We will now show that $\Pr[S_5] \leq \epsilon_{DL}(\kappa)$, where $\epsilon_{DL}(\kappa)$ is the advantage of solving the DLP. $\mathcal{B}$ plays the role of the challenger for $\mathcal{A}$ in Game 5 and obtains a $\mathbb{G}_1$-DLP instance (BG, xP) with $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P}) = \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, generates $\mathsf{pp_{sc}} \leftarrow (\mathsf{BG}, (a^i P, a^i \hat{P})_{i \in [t]})$ by picking $a \xleftarrow{R} \mathbb{Z}_p$, generates $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^3)$ and sets $(\mathsf{osk}, \mathsf{opk}) \leftarrow ((a, \mathsf{sk}), (\mathsf{pp_{sc}}, \mathsf{pk}))$. Then, $\mathcal{B}$ runs $\mathcal{A}(\mathsf{opk})$ and simulates the oracles as in Game 5, except for $\mathcal{O}^{\mathsf{ObtIss}}$, whose simulation is as follows:

$\mathcal{O}^{\mathsf{ObtIss}}(i, \mathtt{A})$: Let this be the jth query. $\mathcal{B}$ first computes $C \leftarrow \mathtt{USK}[i] \cdot f_{\mathtt{A}}(a) \cdot P$. If $j = k$ then it sets $R \leftarrow \mathtt{USK}[i] \cdot f_{\mathtt{A}}(a) \cdot xP \; (= x \cdot C)$, $O' = (0, \mathtt{USK}[i])$ and appends $\mathsf{cred} = ((C, R), \sigma, \perp, O')$ to $\mathtt{CRED}$. Otherwise $\mathcal{B}$ proceeds as in Game 5.

Note that since Game 2, the third component (r) of the credential is not required to simulate $\mathcal{O}^{\mathsf{Show}}$ queries. When $\mathcal{A}$ outputs $(\mathtt{A}'^{*}, \mathsf{st})$ then $\mathcal{B}$ runs $\mathcal{A}(\mathsf{st})$ and interacts with $\mathcal{A}$ as verifier in a showing protocol. If $\mathcal{A}$ wins Game 5 using (C_1^*, C_2^*, C_3^*) and conducting $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1^*, C_2^*, C_3^*)$ then $\mathcal{B}$ runs the knowledge extractor of $\Pi^{\mathcal{R}_{\mathsf{F}}}$ and extracts a witness $w = (r', \mu) \in (\mathbb{Z}_p^*)^2$ such that $C_2^* = r'C_1^*$ and $C_3^* = \mu P$. Further, we have that $((C', R'), \sigma', \perp, O') = \mathtt{CRED}[k]$. In the end, $\mathcal{B}$ outputs r' as a solution to the DLP in $\mathbb{G}_1$. We thus have

$$\Pr[S_5] \leq \epsilon_{DL}(\kappa) \ . \tag{17}$$

Equations (12)–(17) together yield $\Pr[S_0] \leq q_o \cdot \epsilon_{DL}(\kappa) + \frac{q_u}{p} + \epsilon_{qDL}(\kappa)$, where $q = t$ and q_o and q_u are the number of queries to $\mathcal{O}^{\mathsf{ObtIss}}$ and $\mathcal{O}^{\mathtt{HU}+}$, respectively. □

B.2 Proof of Theorem 8 (Anonymity)

The proof proceeds by defining a sequence of indistinguishable games in the last of which the answers of oracle $\mathcal{O}^{LoR}$ are independent of the bit b. Such an answer contains (C_1, C_2, C_3), σ' and the proof $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1, C_2, C_3)$. We first replace the signature σ' by a fresh signature (Game 2) and simulate the proof $\Pi^{\mathcal{R}_{\mathsf{F}}}$ (Game 3). In Games 5 and 6 we replace C_1 and C_2 by random elements. Since $C_3 = \mu \cdot P$ for $\mu \overset{R}{\leftarrow} \mathbb{Z}_p^*$, in the final game the adversary receives a fresh signature σ' on a random tuple (C_1, C_2, C_3) and a simulated proof, resulting in a game that is independent of b.

Proof. We assume that adversary $\mathcal{A}$ at some point calls $\mathcal{O}^{LoR}$ for some $(j_0, j_1, \mathtt{A}')$ with both $\mathtt{I2U}[j_0]$, $\mathtt{I2U}[j_1] \in \mathtt{HU}$. This is w.l.o.g., as otherwise the bit b is perfectly hidden from $\mathcal{A}$. Henceforth, we denote the event that an adversary wins Game i by S_i.

Game 0: The original game as given in Definition 26.

Game 1: As Game 0, except for the oracle $\mathcal{O}^{\mathsf{Obtain}}$. On the first successful completion of the ZKPoK $\Pi^{\mathcal{R}_{\mathsf{VK}}}(\mathsf{opk})$ (of which there must be at least one by the above assumption), the experiment runs the knowledge extractor for $\Pi^{\mathcal{R}_{\mathsf{VK}}}$, which extracts a witness (w_1, w_2).

Game 0 → Game 1: This change is only conceptual and we have $\Pr[S_0] = \Pr[S_1]$.

Game 2: As Game 1, except that the experiment sets $a \leftarrow w_1$ and $\mathsf{sk} \leftarrow w_2$ and runs $\mathcal{O}^{LoR}$ as follows:

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 0, except that all executions of $\mathsf{ChgRep}_{\mathcal{R}}((C, r \cdot C, P), \sigma, \mu, \mathsf{pk})$ for credential $(C, \sigma, r, O') \leftarrow \mathtt{CRED}[j_b]$ and $\mu \overset{R}{\leftarrow} \mathbb{Z}_p^*$ are replaced by $(\mu \cdot (C, r \cdot C, P), \mathsf{Sign}_{\mathcal{R}}(\mu \cdot (C, r \cdot C, P), \mathsf{sk}))$.

Game 1 → Game 2: By soundness of $\Pi^{\mathcal{R}_{\mathsf{VK}}}$, we have $\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1$, and by perfect adaptation of signatures of SPS-EQ (Definition 16), $\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$ and $(\mu M, \mathsf{Sign}_{\mathcal{R}}(\mu M, \mathsf{sk}))$ are identically distributed for all $M \in (\mathbb{G}_1^*)^3$. We thus have $\Pr[S_1] = \Pr[S_2]$.

Game 3: As Game 2, except that the experiment runs $\mathcal{O}^{LoR}$ as follows:

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 2, but the ZKPoK $\Pi^{\mathcal{R}_{\mathsf{F}}}(C_1^*, C_2^*, C_3^*)$ is simulated.

Game 2 → Game 3: By perfect zero-knowledge of $\Pi^{\mathcal{R}_{\mathsf{F}}}$, we have that $\Pr[S_2] = \Pr[S_3]$ and thus

$$\Pr[S_0] = \Pr[S_1] = \Pr[S_2] = \Pr[S_3] \ . \tag{18}$$

Game 4: As Game 3, except for the following changes. Let q_u be (an upper bound on) the number of queries made to $\mathcal{O}^{\mathtt{HU}+}$. At the beginning Game 4 picks $k \overset{R}{\leftarrow} [q_u]$ and runs $\mathcal{O}^{\mathtt{KU}+}$ and $\mathcal{O}^{LoR}$ as follows:

$\mathcal{O}^{\mathtt{KU}+}(i)$: If $i \notin \mathtt{HU}$ or $i \in I_{LoR}$, it returns $\perp$ (as in the previous games). If $i = k$ then the experiment stops and outputs a random bit $b' \xleftarrow{R} \{0,1\}$; otherwise it returns user i's usk and credentials and moves i from $\mathtt{HU}$ to $\mathtt{KU}$.

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 3, except that if $k \neq \mathtt{I2U}[j_b]$, the experiment stops outputting $b' \xleftarrow{R} \{0,1\}$.

Game 3 → Game 4: By assumption, $\mathcal{O}^{LoR}$ is called at least once with some input $(j_0, j_1, \mathtt{A}')$ with $\mathtt{I2U}[j_0], \mathtt{I2U}[j_1] \in \mathtt{HU}$. If $k = \mathtt{I2U}[j_b]$ then $\mathcal{O}^{LoR}$ does not abort and neither does $\mathcal{O}^{\mathtt{KU}+}$ (it cannot have been called on $\mathtt{I2U}[j_b]$ before that call to $\mathcal{O}^{LoR}$ (otherwise $\mathtt{I2U}[j_b] \notin \mathtt{HU}$), if called afterwards, it returns $\perp$, since $k \in I_{LoR}$). Since $k = \mathtt{I2U}[j_b]$ with probability $\frac{1}{q_u}$, the probability that the experiment does not abort is at least $\frac{1}{q_u}$, and thus

$$\Pr[S_4] \geq (1 - \tfrac{1}{q_u})\tfrac{1}{2} + \tfrac{1}{q_u} \cdot \Pr[S_3] \ . \tag{19}$$

Game 5: As Game 4, except for $\mathcal{O}^{LoR}$:

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 4, except that in addition to $\mu \xleftarrow{R} \mathbb{Z}_p^*$, it picks $C_1 \xleftarrow{R} \mathbb{G}_1^*$ and performs the showing using $\mathsf{cred}' \xleftarrow{R} ((C_1, r \cdot C_1, \mu \cdot P), \mathsf{Sign}_{\mathcal{R}}((C_1, r \cdot C_1, \mu \cdot P), \mathsf{sk}))$, with $r \leftarrow \mathtt{CRED}[j_b][3]$, and $W \leftarrow \perp$ (if $a \in \mathtt{A}'$) or $W \leftarrow f_{\mathtt{A}'}(a)^{-1} \cdot C_1$ (if $a \notin \mathtt{A}'$).

Note that the only difference is the choice of C_1; W is distributed as in Game 4, in particular, if $a \notin \mathtt{A}'$, it is the unique element satisfying $\mathsf{VerifySubset}(\mathsf{pp}, C, \mathtt{A}', W)$.

Game 4 → Game 5: Let $(\mathsf{BG}, xP, yP, zP)$ be a DDH instance with $\mathsf{BG} = \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$. After initializing the environment, the simulation initializes a list $L \leftarrow \emptyset$. The oracles are simulated as in Game 4, except for the subsequent oracles, which are simulated as follows:

$\mathcal{O}^{\mathtt{HU}+}(i)$: As in Game 4, but if $i = k$ it sets $\mathtt{USK}[i] \leftarrow \perp$ and $\mathtt{UPK}[i] \leftarrow xP$. (We have thus implicitly set $\mathsf{usk} \leftarrow x$.)

$\mathcal{O}^{\mathsf{Obtain}}(i, \mathtt{A})$: As in Game 4, except for the computation of the following values if $i = k$. Let this be the jth call to this oracle. If $a \notin \mathtt{A}$, it computes C as $C \leftarrow f_{\mathtt{A}}(a) \cdot xP$ and sets $L[j] \leftarrow \perp$. If $a \in \mathtt{A}$ it picks $\rho \xleftarrow{R} \mathbb{Z}_p^*$, computes C as $C \leftarrow \rho \cdot xP$, sets $L[j] \leftarrow \rho$ and simulates the ZKPoK $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})$ (by the perfect ZK property of $\Pi^{\mathcal{R}_{\mathsf{UK}}}(\mathsf{upk})$ the simulation is perfect). (In both cases C is thus distributed as in the original game.)

$\mathcal{O}^{\mathsf{Show}}(j, \mathtt{A}')$: As in Game 4, with the difference that if $\mathtt{I2U}[j] = k$ and $a \notin \mathtt{A}'$ it computes the witness $W \leftarrow \mu f_{\mathtt{A} \setminus \mathtt{A}'}(a) \cdot xP$. ($W$ is thus distributed as in the original game.)

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 4, with the following difference. Using self-reducibility of DDH, it picks $s, t \xleftarrow{R} \mathbb{Z}_p$ and computes $Y' \leftarrow t \cdot yP + sP = y'P$ with $y' \leftarrow ty + s$, and $Z' \leftarrow t \cdot zP + s \cdot xP = (t(z - xy) + xy')P$. (If $z \neq xy$ then Y' and Z' are independently random; otherwise $Z' = y'X$.) It performs the showing using the following values (implicitly setting $\mu \leftarrow y'$):

- If $a \notin \mathtt{ATTR}[j_b]$: $C_1 \leftarrow f_{\mathtt{A}}(a) \cdot Z'$ and $W \leftarrow f_{\mathtt{A}'}(a)^{-1} \cdot C_1$;
- If $a \in \mathtt{ATTR}[j_b]$ and $a \notin \mathtt{A}'$: $C_1 \leftarrow \rho \cdot Z'$ with $\rho \leftarrow L[j_b]$ and $W \leftarrow f_{\mathtt{A}'}(a)^{-1} \cdot C_1$;
- If $a \in \mathtt{A}'$: $C_1 \leftarrow \rho \cdot Z'$ with $\rho \leftarrow L[j_b]$ and $W \leftarrow \perp$;

$C_2 \leftarrow r \cdot C_1$, $C_3 \leftarrow Y'$ and $r \leftarrow \mathtt{CRED}[j_b][3]$.

Apart from an error event happening with negligible probability, we have simulated Game 4 if the DDH instance was "real" and Game 5 otherwise. If $xP = 0_{\mathbb{G}_1}$, or if during the simulation of $\mathcal{O}^{LoR}$ it occurs that $Y' = 0_{\mathbb{G}_1}$ or $Z' = 0_{\mathbb{G}_1}$ then the distribution of values is not as in one of the two games. Otherwise, we have implicitly set $\mathsf{usk} \leftarrow x$ and $\mu \leftarrow y'$ (for a fresh value y' at every call of $\mathcal{O}^{LoR}$). In case of a DDH instance, we have (depending on the case) $C_1 \leftarrow \mathsf{usk}\mu f_{\mathtt{A}}(a) \cdot P$ (or $C_1 = \rho \cdot x\mu \cdot P = \mu \cdot C$);

otherwise C_1 is independently random. Letting $\epsilon_{DDH}(\kappa)$ denote the advantage of solving the DDH problem and q_l the number of queries to the $\mathcal{O}^{LoR}$, we have

$$|\Pr[S_4] - \Pr[S_5]| \leq \epsilon_{DDH}(\kappa) + (1 + 2q_l)\frac{1}{p} \ . \tag{20}$$

Game 6: As Game 5, except for $\mathcal{O}^{LoR}$:

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 5, except that in addition to μ and C_1 it also picks $C_2 \overset{R}{\leftarrow} \mathbb{G}_1^*$ and performs the showing using $\mathsf{cred}' \overset{R}{\leftarrow} ((C_1, C_2, \mu \cdot P), \mathsf{Sign}_{\mathcal{R}}((C_1, C_2, \mu \cdot P), \mathsf{sk}))$ and W as in Game 5.

Game 5 → Game 6: Let $(\mathsf{BG}, xP, yP, zP)$ be a DDH instance with $\mathsf{BG} = \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$. After initializing the environment, the simulation initializes a list $L \leftarrow \emptyset$. The oracles are simulated as in Game 5, except for the subsequent oracles, which are simulated as follows:

$\mathcal{O}^{\mathsf{Obtain}}(i, \mathtt{A})$: As in Game 5, except for the computation of the following values if $i = k$. Let this be the jth call to this oracle. It first picks $u \overset{R}{\leftarrow} \mathbb{Z}_p$ and sets $X' \leftarrow xP + u \cdot P$ and $L[j] \leftarrow u$. If $a \notin \mathtt{A}$, it computes $C \leftarrow f_{\mathtt{A}}(a) \cdot \mathtt{USK}[i] \cdot P$ and $R \leftarrow f_{\mathtt{A}}(a) \cdot \mathtt{USK}[i] \cdot X'$. If $a \in \mathtt{A}$, it picks $\rho \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and computes $C \leftarrow \rho \cdot P$ and $R \leftarrow \rho \cdot X'$. In both cases it sets $r \leftarrow \perp$ (r is implicitly set to $r \leftarrow x' := x + u$ and C and $R = r \cdot C$ are distributed as in the original game; unless $X' = 0_{\mathbb{G}_1}$). Note that, since the ZKPoK in $\mathcal{O}^{\mathsf{Show}}$ is simulated, r is not used anywhere in the game.

$\mathcal{O}^{LoR}(j_0, j_1, \mathtt{A}')$: As in Game 5, with the difference that it fetches $u \leftarrow L[j_b]$, picks $s, t \overset{R}{\leftarrow} \mathbb{Z}_p$ and computes $Y' \leftarrow t \cdot yP + s \cdot P = y'P$ with $y' \leftarrow ty + s$, and $Z' \leftarrow t \cdot zP + s \cdot xP + ut \cdot yP + us \cdot P = (t(z - xy) + x'y')P$. It picks $\mu \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and performs the showing using $C_1 \leftarrow Y'$, $C_2 \leftarrow Z'$ and $C_3 \leftarrow \mu \cdot P$. Witness W is computed from C_1 as in the previous simulation.

Apart from an error event happening with negligible probability, we have simulated Game 5 if the DDH instance was valid and Game 6 otherwise. If $X' = 0_{\mathbb{G}_1}$ during the simulation of $\mathcal{O}^{\mathsf{Obtain}}$, or if during the simulation of $\mathcal{O}^{LoR}$ it occurs that $Y' = 0_{\mathbb{G}_1}$ or $Z' = 0_{\mathbb{G}_1}$ then the distribution of values is not as in one of the two games. Otherwise, we have implicitly set $r \leftarrow x'$ (for a fresh value x' at every call of $\mathcal{O}^{\mathsf{Obtain}}$) and $C_1 \leftarrow Y'$ (for a fresh value Y' at every call of $\mathcal{O}^{LoR}$). In case of a DDH instance, we have $C_2 = r \cdot C_1$ (as in Game 5); otherwise C_2 is independently random (as in Game 6). Letting $\epsilon_{DDH}(\kappa)$ denote the advantage of solving the DDH problem, and q_o and q_l be the number of queries to $\mathcal{O}^{\mathsf{Obtain}}$ and $\mathcal{O}^{LoR}$, respectively, we get

$$|\Pr[S_5] - \Pr[S_6]| \leq \epsilon_{DDH}(\kappa) + (q_o + 2q_l)\frac{1}{p} \ . \tag{21}$$

In Game 6 the $\mathcal{O}^{LoR}$ oracle returns a fresh signature σ on a random triple $(C_1, C_2, C_3) \overset{R}{\leftarrow} (\mathbb{G}_1^*)^3$ and a simulated proof; the bit b is thus information-theoretically hidden from $\mathcal{A}$ and we have $\Pr[S_6] = \frac{1}{2}$. From this and Equations (21), (20), (18) and (19) we have

$$\begin{aligned}
\Pr[S_5] &\leq \Pr[S_6] + \epsilon_{DDH}(\kappa) + (q_o + 2q_l)\tfrac{1}{p} = \tfrac{1}{2} + \epsilon_{DDH}(\kappa) + (q_o + 2q_l)\tfrac{1}{p} \ , \\
\Pr[S_4] &\leq \Pr[S_5] + \epsilon_{DDH}(\kappa) + (1 + 2q_l)\tfrac{1}{p} \leq \tfrac{1}{2} + 2 \cdot \epsilon_{DDH}(\kappa) + (1 + q_o + 4q_l)\tfrac{1}{p} \ , \\
\Pr[S_0] = \Pr[S_3] &\leq \tfrac{1}{2} + q_u \cdot \Pr[S_4] - \tfrac{1}{2} \cdot q_u \leq \tfrac{1}{2} + q_u \cdot \left(2 \cdot \epsilon_{DDH}(\kappa) + (1 + q_o + 4q_l)\tfrac{1}{p}\right) \ ,
\end{aligned}$$

where q_u, q_o and q_l are the number of queries to the $\mathcal{O}^{\mathtt{HU}+}$, $\mathcal{O}^{\mathsf{Obtain}}$ and the $\mathcal{O}^{LoR}$ oracle, respectively. Assuming DDH, the adversary's advantage is thus negligible. □