Efficient Signatures on Randomizable Ciphertexts

Balthazar Bauer, Georg Fuchsbauer

Efficient Signatures on Randomizable Ciphertexts

Balthazar Bauer[1,2], Georg Fuchsbauer[3]

[1] Inria
[2] ENS, CNRS, PSL University
[3] TU Wien
first.last@{ens.fr, tuwien.ac.at}

Abstract

Randomizable encryption lets anyone randomize a ciphertext so it is distributed like a fresh encryption of the same plaintext. *Signatures on randomizable ciphertexts* (SoRC), introduced by Blazy et al. (PKC'11), let one adapt a signature on a ciphertext to a randomization of the latter. Since signatures can only be adapted to ciphertexts that encrypt the same message as the signed ciphertext, signatures obliviously authenticate plaintexts. SoRC have been used as a building block in e-voting, blind signatures and (delegatable) anonymous credentials.

We observe that SoRC can be seen as *signatures on equivalence classes* (JoC'19), another primitive with many applications to anonymous authentication, and that SoRC provide better anonymity guarantees. We first strengthen the unforgeability notion for SoRC and then give a scheme that provably achieves it in the generic group model. Signatures in our scheme consist of 4 bilinear-group elements, which is considerably more efficient than prior schemes.

1 Introduction

A standard approach for anonymous authentication is to combine signatures, which yield authentication, with zero-knowledge proofs, which allow to prove possession of a signature without revealing information about the latter and thus provide anonymity. This approach has been followed for (multi-show) anonymous credentials schemes, for which several showings of the same credential cannot be linked (in contrast to one-show credentials, e.g. [Bra00, BL13]).

The zero-knowledge proofs for these schemes are either instantiated using Σ-protocols [CL03, CL04] (and are thus interactive or in the random oracle model) or in the standard model [BCKL08] using Groth-Sahai proofs [GS08]. As this proof system only supports very specific types of statements in bilinear ("pairing-friendly") groups, signature schemes whose verification is of this type have been introduced: *structure-preserving signatures* [AFG+10] sign messages from a group $\mathbb{G}$ and are verified by checking equivalences of products of pairings of group elements from the verification key, the message and the signature.

Equivalence-class signatures. Hanser and Slamanig [HS14] extended this concept to *structure-preserving signatures on equivalence classes* (later improved in [FHS19]) for messages from $\mathbb{G}^2$, by adding a functionality called *signature adaptation*: given a signature on a message $\mathbf{m} \in \mathbb{G}^2$ and a scalar r, anyone can "adapt" the signature so it verifies for the message $r \cdot \mathbf{m}$. A signature thus authenticates the equivalence class of all multiples of the signed message.

Equivalence-class signatures (ECS) enable anonymous authentication that completely forgoes the layer of zero-knowledge proofs and thus yields considerable efficiency gains. Consider anonymous credentials. A credential is a signature on a message $\mathbf{m}$ (which typically contains a commitment to the user's attributes). In previous schemes, when authenticating, the user proves in zero knowledge

that she knows a message $\mathbf{m}$ (and an opening of the contained commitment to the attributes she wants to show) as well as a signature on $\mathbf{m}$; several authentications with the same credential are thus unlinkable. Using ECS, this is possible *without* using any proof system [FHS19]: the user simply shows $r \cdot \mathbf{m}$ for a fresh random r together with an adapted signature. Anonymity is implied by the following property of ECS: to someone that is given $\mathbf{m}$ and a signature on $\mathbf{m}$, the pair consisting of $\mathbf{m}' := r \cdot \mathbf{m}$ for a random r and the signature adapted to $\mathbf{m}'$ is indistinguishable from a random element $\mathbf{m}''$ from $\mathbb{G}^2$ together with a *fresh* signature on $\mathbf{m}''$.

Besides the first attribute-based anonymous credential scheme for which the complexity of showing is independent of the number of attributes [FHS19], ECS have also been used to build very efficient blind signatures with minimal interaction between the signer and the user that asks for the signature [FHS15, FHKS16], revocable anonymous credentials [DHS15], as well as efficient constructions [FGKO17, DS18] of both access-control encryption [DHO16] and dynamic group signatures [BSZ05].

The most efficient construction of ECS is the one from [FHS19], which was proven secure in the generic group model [Sho97]. A signature consist of 3 elements from a bilinear group, which the authors show to be optimal by relying on a result by Abe et al. [AGHO11]. Moreover, there is strong evidence that structure-preserving signatures of this size cannot be proved secure by a reduction to non-interactive assumptions [AGO11], meaning a proof in the generic group model is the best we can hope for. Less efficient constructions of EQS from standard assumptions have since then been given in the standard model by weakening the security guarantees [FG18] and in the common-reference string model [KSD19] (with signatures 6 times longer than [FHS19]).

Signatures with flexible public key [BHKS18] and *mercurials signatures* [CL19] are extensions of ECS that allow signatures to be adapted not only to multiples of the signed message, but also to multiples of the verification key. This has been used to build delegatable anonymous credentials [BCC+09] in [CL19]. Delegatable credentials allow for hierarchical structures, in which users can delegate obtained credentials to users at lower levels.

Shortcomings of ECS. While schemes based on ECS offer (near-)optimal efficiency, a drawback is their weak form of anonymity. Consider a user who asks for a signature on $\mathbf{m} = (m_0 G, m_1 G)$ (where G is the generator of the group $(\mathbb{G}, +)$). If the user later sees a randomization (M_0', M_1') of this message, she can easily identify it as hers by checking whether $m_1 M_0' = m_0 M_1'$. The notion of anonymity (which is called *class-hiding* in ECS) that can be achieved for these equivalence classes is thus akin to what has been called *selfless* anonymity [CG05] in the context of group signatures: in contrast to *full* anonymity [BMW03], signatures are only anonymous to those that do not know the secret values used to construct them (the signing key for group signatures; the values m_0 and m_1 in our example above).

This weakness can have concrete repercussions on the anonymity guarantees provided by schemes built from ECS, for example delegatable credentials. In previous instantiations [BCC+09, Fuc11] of the latter, the showing of a credential is anonymous to anyone, in particular to a user that has delegated said credential to the one showing it. However, in the construction from the ECS variant *mercurial signatures* [CL19], if Alice delegates a credential to Bob, she can identify Bob whenever he uses the credential to authenticate, which represents a serious infringement to Bob's privacy. In fact, anonymity towards the authority issuing (or delegating) credentials has been considered a fundamental property of anonymous credential schemes.

In [CL19], when Alice delegates a credential to Bob, she uses her secret key $(x_0, x_1) \in (\mathbb{Z}_{|\mathbb{G}|}^*)^2$ to sign Bob's pseudonym under her own pseudonym $(P_0, P_1) = (rx_0 G, rx_1 G)$ for a random r, which becomes part of Bobs credential. When Bob shows it, he randomizes Alice's pseudonym to $(P_0', P_1') := (r' P_0, r' P_1)$ for a random r', which Alice can recognize by checking whether $x_1 P_0' = x_0 P_1'$.

Signatures on randomizable ciphertexts. To overcome this weakness in anonymity in ECS, we use a different type of equivalence class. Consider an ElGamal [ElG85] encryption $(C_0, C_1) = (rG, M + rP)$ of a message M under an encryption key P. Such ciphertexts can be *randomized* by anyone, that is, without knowing the underlying message, a fresh encryption of the same message can

be computed by choosing r' and setting $(C'_0, C'_1) := (C_0 + r'G,\ C_1 + r'P) = ((r+r')G,\ M + (r+r')P)$. All possible encryptions of a message form an equivalence class, which, in contrast to multiples of pairs of group elements, satisfy a "full" anonymity notion: after randomization, the resulting ciphertext looks random *even to the one that created the original ciphertext* (see Proposition 1).

If such equivalence classes yield better anonymity guarantees, the question is whether we can have adaptable signatures on them, that is, signatures on ciphertexts that can be adapted to randomizations of the signed ciphertext. It turns out that this concept exists and even predates that of ECS and is called *signatures on randomizable ciphertexts* (SoRC) [BFPV11]. Since their introduction, SoRC have been extensively used in e-voting [CCFG16, CFL19, CGG19, HPP20] and other primitives, such as blind signatures and extensions thereof [BFPV13]. Blazy et al. [BFPV11] prove their instantiation of SoRC unforgeable under standard assumptions in bilinear groups. Its biggest drawback is that it only allows for efficiently signing messages that consist of a few bits.

Our contribution. Our aim was to construct a scheme of signatures on randomizable ciphertexts with a large message space and short signatures. But first we strengthen the notion of signature unforgeability. In SoRC, signatures are produced (and verified) on pairs of encryption keys and ciphertexts (ek, c). In the original unforgeability notion [BFPV11] the adversary is given a signature verification key and a set of encryption keys $ek_1, \ldots, ek_n$ and can then make queries (i, c) to get a signature for (ek_i, c). Its goal is to return (i^*, c^*) and a signature for (ek_{i^*}, c^*), so that c^* encrypts a message of which no encryption has been submitted to the signing oracle. Signatures thus authenticate plaintexts irrespective of the encryption key.

In more detail, once a query $(1, \mathsf{Enc}(ek_1, m))$ was made, a signature for $(ek_2, \mathsf{Enc}(ek_2, m))$ is *not* considered a forgery. In contrast, in our new definition (Def. 6), this is considered a forgery, since we view a signature as (obliviously) authenticating a message *for a particular encryption key*. That is, if from a signature on an encryption of a message for one key one can forge a signature on the same message for another key, this is considered a break of the scheme. A further difference is that, while in [BFPV11] encryption keys are generated by the challenger, we let the adversary choose (in any, possibly malicious, way) the encryption keys (in addition to the ciphertexts) on which it wishes to see a signature, as well as the key for its forgery.

We then construct a scheme which signs ElGamal ciphertexts and whose signatures consist of 4 elements of an (asymmetric) bilinear group (3 elements from $\mathbb{G}_1$ and 1 from $\mathbb{G}_2$). Our scheme (given in Fig. 3) is inspired by the original equivalence-class signature scheme [FHS19], whose equivalence classes only provide "selfless" anonymity. We show that signatures adapted to a randomization of a ciphertext are equivalently distributed to fresh signatures on the new ciphertext (Proposition 2). We then prove that our scheme satisfies our strengthened unforgeability notion in the generic group model (Theorem 1).

Comparison with Blazy et al. Apart from the stronger unforgeability notion we achieve, the main improvement of our scheme over [BFPV11] concerns its efficiency. The Blazy et al. scheme builds on (a new variant of) Waters signatures [Wat05] and Groth-Sahai proofs [GS08], which allows them to prove unforgeability from standard assumptions. However, encrypting and signing a k-bit message yields a ciphertext/signature pair consisting of $12 + 12k$ group elements of an asymmetric bilinear group. In our scheme, a message is a group element (as for ElGamal encryption), which lets us encode 128-bit messages (or messages of unbounded length by hashing into the group). A ciphertext/signature pair consists of 6 group elements. We also propose a generalization to messages of n group elements for which a ciphertext/signature pair consists of $n + 5$ group elements.

The price we pay for this length reduction by a factor of over 250 (for 128-bit messages or longer) is an unforgeability proof in the generic group model. But, as we argue next, this is to be expected. Since we sign group elements and verification consists in checking pairing-product equations, our scheme is *structure-preserving* [AFG+10]. Signatures for such schemes must at least contain 3 group elements [AGHO11] and schemes with such short signatures cannot be proved from non-interactive (let alone standard) assumptions [AGO11]. Our 4-element signatures, which provide additional functionalities, and its unforgeability proof are therefore close to being optimal.

We also note that a security reduction to computational hardness assumptions for schemes satisfying our unforgeability notion seems challenging, as the challenger cannot efficiently decide whether the adversary has won (in contrast to the weaker notion [BFPV11]).

2 Premilinaries

A function $\epsilon\colon \mathbb{N} \to \mathbb{R}$ is called negligible if for all $c > 0$ there is a k_0 such that $\epsilon(k) < \frac{1}{k^c}$ for all $k > k_0$. By $a \xleftarrow{\$} S$, we denote that a is picked uniformly at random from a set S. By $y \xleftarrow{\$} A(x)$ we denote running a probabilistic algorithm A on input x and assigning the output to y. We write $A(x; r)$ to make the randomness r explicit.

Bilinear groups. We assume the existence of a probabilistic polynomial-time (p.p.t.) algorithm BGGen that takes as input an integer λ in unary and outputs a description of an (asymmetric) bilinear group $(p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e)$ consisting of groups $(\mathbb{G}, +)$ and $(\hat{\mathbb{G}}, +)$, generated by G and $\hat{G}$, resp., and $(\mathbb{G}_T, \cdot)$, all of cardinality a prime number $p \in \{2^\lambda, \ldots, 2^{\lambda+1}\}$, and a bilinear map $e\colon \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$, such that $e(G, \hat{G})$ generates $\mathbb{G}_T$, called *pairing*.

The *decisional Diffie-Hellman assumption* for BGGen states that no p.p.t. adversary $\mathcal{A}$ can distinguish a triple (dG, rG, drG) for $d, r \xleftarrow{\$} \mathbb{Z}_p$ from a random triple from $\mathbb{G}^3$ with better than negligible advantage (see also Fig. 4).

Rational fractions. We start with defining the *total degree* of a polynomial $P(X_1, \ldots, X_m) = \sum_{\vec{i} \in \mathbb{N}^m} a_{i_1,\ldots,i_m} \prod_{j=1}^m X_j^{i_j} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ as $\deg P := \max_{\vec{i} \in \mathbb{N}^m \,:\, a_{i_1,\ldots,i_m} \not\equiv_p 0} \left\{ \sum_{j=1}^m i_j \right\}$.

In our main proof (Theorem 1), we make extensive use of multivariate rational fractions from $\mathbb{Z}_p(X_1, \ldots, X_m)$ and argue using their degrees, for which we will use the "French" definition [AW98]: For $(P, Q) \in \mathbb{Z}_p[X_1, \ldots, X_m] \times \big(\mathbb{Z}_p[X_1, \ldots, X_m] \setminus \{0\}\big)$, we define

$$\deg \frac{P}{Q} := \deg P - \deg Q \ .$$

We recall some properties of this definition:

- It generalizes the one for polynomials.
- The degree does not depend on the choice of the representative.
- As for polynomials, we have $\deg(F_1 \cdot F_2) = \deg F_1 + \deg F_2$ and $\deg(F_1 + F_2) \leq \max\{\deg F_1, \deg F_2\}$.

We use subscripts for degrees in a specific indeterminate, e.g., $\deg_{x_i}$ denotes the degree in variable x_i.

3 Signatures on randomizable ciphertexts

We start with the definition of a *signatures on randomizable ciphertexts* scheme, which consists of a randomizable public-key encryption scheme and a signature scheme, whose signatures are computed and verified on pairs (encryption key, ciphertext). In addition, there is an algorithm Adapt, which lets one adapt a signature on a ciphertext to any randomization of the latter.

3.1 Syntax

Definition 1. *We denote by $\mathcal{PP}$ the set of public parameters, and for $\mathrm{pp} \in \mathcal{PP}$ we let $\mathcal{M}_{\mathrm{pp}}$ be the set of messages, $\mathcal{DK}_{\mathrm{pp}}$ the set of decryption keys, $\mathcal{EK}_{\mathrm{pp}}$, the set of encryption keys, $\mathcal{C}_{\mathrm{pp}}$ the set of ciphertexts, $\mathcal{R}_{\mathrm{pp}}$ the set of ciphertext randomness, $\mathcal{SK}_{\mathrm{pp}}$ the set of signature keys, $\mathcal{VK}_{\mathrm{pp}}$ the set of verification keys and $\mathcal{S}_{\mathrm{pp}}$ the set of signatures.*

A scheme of signatures on randomizable ciphertexts *$\mathcal{SRC}$ consists of the following probabilistic algorithms, of which all except Setup are implicitly parameterized by an element $\mathrm{pp} \in \mathcal{PP}$.*

$\mathbf{IND\text{-}CPA}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, b)$:	$\mathbf{CL\text{-}HID}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, b)$:
01 $pp \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$	01 $pp \xleftarrow{\$} \mathsf{Setup}(\lambda)$
02 $(dk, ek) \xleftarrow{\$} \mathsf{KeyGen}(pp)$	02 $(dk, ek) \xleftarrow{\$} \mathsf{KeyGen}(pp)$
03 $(m_0, m_1, st) \xleftarrow{\$} \mathcal{A}(ek)$	03 $(c, st) \xleftarrow{\$} \mathcal{A}(ek)$
04 $r \xleftarrow{\$} \mathcal{R}_{pp}$	04 $c_0 \xleftarrow{\$} \mathcal{C}_{pp}$
05 $c := \mathsf{Enc}(ek, m_b, r)$	05 $r \xleftarrow{\$} \mathcal{R}_{pp}$; $c_1 := \mathsf{Rndmz}(ek, c, r)$
06 $b' \xleftarrow{\$} \mathcal{A}(st, c)$	06 $b' \xleftarrow{\$} \mathcal{A}(st, c_b)$
07 Return b'	07 Return b'

Figure 1: Games for ciphertext-indistinguishability and class-hiding

$$\begin{aligned}
\mathsf{Setup}&: \mathbb{N} \to \mathcal{PP} \\
\mathsf{KeyGen}&: \emptyset \to \mathcal{DK}_{pp} \times \mathcal{EK}_{pp} \qquad & \mathsf{SKeyGen}&: \emptyset \to \mathcal{SK}_{pp} \times \mathcal{VK}_{pp} \\
\mathsf{Enc}&: \mathcal{EK}_{pp} \times \mathcal{M}_{pp} \times \mathcal{R}_{pp} \to \mathcal{C}_{pp} & \mathsf{Sign}&: \mathcal{SK}_{pp} \times \mathcal{EK}_{pp} \times \mathcal{C}_{pp} \to \mathcal{S}_{pp} \\
\mathsf{Rndmz}&: \mathcal{EK}_{pp} \times \mathcal{C}_{pp} \times \mathcal{R}_{pp} \to \mathcal{C}_{pp} & \mathsf{Verify}&: \mathcal{VK}_{pp} \times \mathcal{EK}_{pp} \times \mathcal{C}_{pp} \times \mathcal{S}_{pp} \to \{0,1\} \\
\mathsf{Dec}&: \mathcal{DK}_{pp} \times \mathcal{C}_{pp} \to \mathcal{M}_{pp} & \mathsf{Adapt}&: \mathcal{S}_{pp} \times \mathcal{R}_{pp} \to \mathcal{S}_{pp}
\end{aligned}$$

We define the equivalence class $[c]_{ek}$ of a ciphertext c under encryption key ek as all randomizations of c, that is, $[c]_{ek} := \{c' \mid \exists\, r \in \mathcal{R}_{pp} : c' = \mathsf{Rndmz}(ek, c, r)\}$.

3.2 Correctness and security definitions

Correctness of SoRC requires that the encryption scheme and the signature scheme are correct.

Definition 2. *A SoRC scheme is* correct *if for all $pp \in \mathcal{PP}$, for all pairs (ek, dk) and (sk, vk) in the range of $\mathsf{KeyGen}(pp)$ and $\mathsf{SKeyGen}(pp)$, respectively, and all $m \in \mathcal{M}_{pp}$, $r \in \mathcal{R}_{pp}$ and $c \in \mathcal{C}_{pp}$:*

$$\mathsf{Dec}\big(dk, \mathsf{Enc}(ek, m, r)\big) = m \qquad \text{and} \qquad \Pr\left[\mathsf{Verify}\big(vk, ek, c, \mathsf{Sign}(sk, ek, c)\big) = 1\right] = 1 \ .$$

Note that together with signature-adaptation (Def. 5 below), this implies that adapted signatures verify as well. We also require that the encryption scheme satisfies the standard security notion.

Definition 3. *Let game* **IND-CPA** *be as defined in Fig. 1. A SoRC scheme is* IND-CPA secure *if for all p.p.t. adversary $\mathcal{A}$ the following function is negligible in λ:*

$$\left|\Pr\left[\mathbf{IND\text{-}CPA}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, 1) = 1\right] - \Pr\left[\mathbf{IND\text{-}CPA}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, 0) = 1\right]\right| .$$

Class-hiding is a property of equivalence-class signatures that states that given a representative of an equivalence class, then a random member of that class is indistinguishable from a random element of the whole space. We give a stronger definition, which we call *fully class-hiding* (analogously to full anonymity). Whereas in the original notion [FHS19, Def. 18], the representative is uniformly picked by the experiment, in our notion it is chosen by the adversary.

Definition 4. *Let game* **CL-HID** *be as defined in Fig. 1. A SoRC scheme is* fully class-hiding *if for all p.p.t. adversary $\mathcal{A}$, the following function is negligible in λ:*

$$\left|\Pr\left[\mathbf{CL\text{-}HID}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, 1) = 1\right] - \Pr\left[\mathbf{CL\text{-}HID}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, 0) = 1\right]\right| .$$

Signature-adaptation requires that signatures that have been adapted to a randomization of the signed ciphertext are distributed like fresh signatures on the randomized ciphertext. A strengthening is the following variant, which also holds for maliciously generated verification keys [FHS19, Def. 20].

Definition 5. *A SoRC scheme is* signature-adaptable (under malicious keys) *if for all $pp \in \mathcal{PP}$, all $(vk, ek, c, sig) \in \mathcal{VK}_{pp} \times \mathcal{EK}_{pp} \times \mathcal{C}_{pp} \times \mathcal{S}_{pp}$ that satisfy $\mathsf{Verify}(vk, ek, c, sig) = 1$ and all $r \in \mathcal{R}_{pp}$, the output of $\mathsf{Adapt}(sig, r)$ is uniformly distributed over the set*

$$\left\{sig' \in \mathcal{S}_{pp} \;\middle|\; \mathsf{Verify}\big(vk, ek, \mathsf{Rndmz}(ek, c, r), sig'\big) = 1\right\} .$$

$\mathbf{EUF}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda)$:
01 $Q := \emptyset$; $pp \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$
02 $(sk, vk) \xleftarrow{\$} \mathsf{SKeyGen}(pp)$
03 $\big((ek^*, c^*), sig^*\big) \xleftarrow{\$} \mathcal{A}_2^{\mathtt{Sign}(sk,\cdot,\cdot)}(vk)$
04 Return $\big(\mathsf{Verify}(vk, ek^*, c^*, sig^*) = 1 \wedge (ek^*, c^*) \notin Q\big)$

$\mathtt{Sign}(sk, ek, c)$
01 $Q := Q \cup \{ek\} \times [c]_{ek}$
02 Return $\mathsf{Sign}(sk, ek, c)$

Figure 2: Unforgeability game

Note that if Sign outputs a uniform element in the set of valid signatures (which is the case in the ECS scheme from [FHS19] and our scheme) then Def. 5 implies that for all honestly generated (sk, vk) and all ek, c and r the outputs of the following two procedures are distributed equivalently:

$$\mathsf{Adapt}\big(\mathsf{Sign}(sk, ek, c), r'\big) \qquad \text{and} \qquad \mathsf{Sign}\big(sk, ek, \mathsf{Rndmz}(ek, c, r')\big) \ .$$

Together, full class-hiding and signature-adaptability under malicious keys imply that for an adversary that creates a signature verification key as well as a ciphertext and a signature on it, a randomization of this ciphertext together with an adapted signature looks like a random ciphertext with a fresh signature on it. (In contrast, for equivalence-class signatures, this was only true if the signed message was not chosen by the adversary [FHS19].)

Unforgeability. Finally, we present our strengthened notion of unforgeability, which is defined w.r.t. keys and equivalence classes. That is, after the adversary queries a signature for (ek, c), all tuples (ek, c') with $c' \in [c]_{ek}$ (that is, c' encrypts the same message as c under ek) are added to a set Q of signed objects. The adversary's goal is to produce a signature on a pair (ek^*, c^*) that is not contained in Q. (In the original definition [BFPV11], Q would contain the equivalence classes of c under *all* encryption keys, i.e., all encryptions of the plaintext of c under all keys.)

Definition 6. *Let* **EUF** *be the game defined in Fig. 2. A SoRC scheme is* unforgeable *is for all p.p.t. adversary $\mathcal{A}$ the following function is negligible in λ:*

$$\Pr\left[\mathbf{EUF}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda) = 1\right] \ .$$

4 Instantiation

Our instantiation of SoRC is given in Fig. 3. Its signatures sign ElGamal ciphertexts (C_0, C_1), and the signature elements $(Z, S, \hat{S})$ constitute a structure-preserving signature on (C_0, C_1) similar to the optimal scheme from [AGHO11]. (And removing G from the definition of Z would yield the equivalence-class scheme from [FHS19]: note that, without G, multiplying Z by r yields a signature on the message $r \cdot (C_0, C_1)$.) The new element T in our scheme allows for adaptation of signatures to randomizations of the signed ciphertext. Randomization implicitly defines the following equivalence classes: for $P \in \mathcal{EK}_{pp}$ and $(C_0, C_1), (C_0', C_1') \in \mathcal{C}_{pp}$:

$$(C_0', C_1') \in \big[(C_0, C_1)\big]_P \iff \exists\, r \in \mathbb{Z}_p : (C_0', C_1') = (C_0 + rG,\ C_1 + rP) \ .$$

5 Security of our scheme

Correctness of our scheme follows by inspection. Moreover, ElGamal encryption [ElG85] satisfies IND-CPA if the decisional Diffie-Hellman (DDH) assumption holds for BGGen.

Proposition 1. *If DDH holds for BGGen then the scheme in Fig. 3 is fully class-hiding (Def. 4).*

Proof. We first recall the game **DDH**, which formalizes the DDH assumption in Fig. 4 (left). Next, we instantiate **CL-HID** with our scheme from Fig. 3 and rewrite it in Fig. 4 (right). In particular, instead of choosing $c_0 \xleftarrow{\$} \mathbb{G}^2$, we compute it as $c + c_0'$ for a uniform $c_0' \xleftarrow{\$} \mathbb{G}^2$.

$\mathsf{Setup}(1^\lambda)$: Return $pp = (p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e) \xleftarrow{\$} \mathsf{BGGen}(1^\lambda)$, which define $\mathcal{M}_{pp} := \mathbb{G}$, $\mathcal{C}_{pp} := \mathbb{G}^2$, $\mathcal{R}_{pp} := \mathbb{Z}_p$, $\mathcal{SK}_{pp} := (\mathbb{Z}_p^*)^2$, $\mathcal{VK}_{pp} := (\hat{\mathbb{G}}^*)^2$, $\mathcal{EK}_{pp} := \mathbb{G}^*$, $\mathcal{DK}_{pp} := \mathbb{Z}_p^*$ and $\mathcal{S}_{pp} := \mathbb{G}\times\mathbb{G}^*\times\hat{\mathbb{G}}^*\times\mathbb{G}$.

$\mathsf{KeyGen}(pp)$: Parse pp as $(p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e)$
$dk := d \xleftarrow{\$} \mathbb{Z}_p^*$; $ek = P = dG$; return (dk, ek)

$\mathsf{Enc}(P, M, r)$: Return $(rG, M + rP)$

$\mathsf{Dec}(d, (C_0, C_1))$: Return $M := C_1 - dC_0$

$\mathsf{Rndmz}(P, (C_0, C_1), r')$: Return $(C_0 + r'G, C_1 + r'P)$

$\mathsf{SKeyGen}(pp)$: Parse pp as $(p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e)$
$sk := (x_0, x_1) \xleftarrow{\$} (\mathbb{Z}_p^*)^2$; $vk := (\hat{X}_0 = x_0\hat{G}, \hat{X}_1 = x_1\hat{G})$; return (sk, vk)

$\mathsf{Sign}((x_0, x_1), P, (C_0, C_1))$: $s \xleftarrow{\$} \mathbb{Z}_p^*$; return $(Z, S, \hat{S}, T)$ with

$$Z := \frac{1}{s}\big(G + x_0C_0 + x_1C_1\big) \qquad S := sG \qquad \hat{S} := s\hat{G} \qquad T := \frac{1}{s}\big(x_0G + x_1P\big)$$

$\mathsf{Adapt}\big((Z, S, \hat{S}, T), r'\big)$: $s' \xleftarrow{\$} \mathbb{Z}_p^*$; return $(Z', S', \hat{S}', T')$ with

$$Z' := \frac{1}{s'}\big(Z + r'T\big) \qquad S' := s'S \qquad \hat{S}' := s'\hat{S} \qquad T' := \frac{1}{s'}T$$

$\mathsf{Verify}((\hat{X}_0, \hat{X}_1), P, (C_0, C_1), (Z, S, \hat{S}, T))$: Return 0 if $P = 0$ or $S = 0$; return 1 if the following equations hold and 0 otherwise:

$$e(Z, \hat{S}) = e(G, \hat{G})e(C_0, \hat{X}_0)e(C_1, \hat{X}_1) \qquad e(G, \hat{S}) = e(S, \hat{G})$$
$$e(T, \hat{S}) = e(G, \hat{X}_0)e(P, \hat{X}_1)$$

Figure 3: Our instantiation $\mathcal{SRC}$ of SoRC

Let $\mathcal{A}$ be an adversary against **CL-HID**. We define an adversary $\mathcal{B}$ against **DDH**, which upon receiving a challenge (P, R, S), sends P to $\mathcal{A}$ to get c and then sends $c + (R, S)$ to $\mathcal{A}$. Finally, $\mathcal{B}$ returns $\mathcal{A}$'s output b'.

Since for all λ and b we have that $\mathbf{DDH}^{\mathcal{B}^{\mathcal{A}}}_{\mathcal{SRC}}(\lambda, b)$ and $\mathbf{CL\text{-}HID}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, b)$ follow the same distribution, $\mathcal{B}$'s advantage in breaking DDH is the same as $\mathcal{A}$'s advantage in breaking full class-hiding. □

Proposition 2. *The SoRC scheme in Fig. 3 is signature-adaptable under malicious keys (Def. 5).*

Proof. Let $pp = (p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e) \in \mathcal{PP}$, let $vk = (x_0\hat{G}, x_1\hat{G})$, $ek = dG$, $C_0 = c_0G$, $C_1 = c_1G$ and $sig = (Z = zG, S = sG, \hat{S} = \hat{s}\hat{G}, T = tG)$ be such that $\mathsf{Verify}(vk, ek, (C_0, C_1), sig) = 1$. Taking the logarithms in basis $e(G, \hat{G})$ of the verification equations yields $\hat{s} = s$ and, using this,

$$zs = z\hat{s} = 1 + c_0x_0 + c_1x_1 \tag{1}$$
$$ts = t\hat{s} = x_0 + dx_1 \tag{2}$$

$\mathbf{DDH}^{\mathcal{B}}_{\mathsf{BGGen}}(\lambda, b)$:	$\mathbf{CL\text{-}HID}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda, b)$:
01 $(p, \mathbb{G}, G, \hat{\mathbb{G}}, \hat{G}, \mathbb{G}_T, e) \xleftarrow{\$} \mathsf{BGGen}(\lambda)$	01 $pp \xleftarrow{\$} \mathsf{Setup}(\lambda)$
02 $P \xleftarrow{\$} \mathbb{G}$	02 $(d, P) \xleftarrow{\$} \mathsf{KeyGen}(pp)$
03 $r \xleftarrow{\$} \mathbb{Z}_p$	03 $(c, st) \xleftarrow{\$} \mathcal{A}(P)$
04 $S_1 := rP$	04 $c'_0 \xleftarrow{\$} \mathbb{G} \times \mathbb{G}$
05 $S_0 \xleftarrow{\$} \mathbb{G}$	05 $r \xleftarrow{\$} \mathcal{R}_{pp}$; $c'_1 := (rG, rP)$
06 $b' \xleftarrow{\$} \mathcal{B}(pp, (P, rG, S_b))$; Return b'	06 $b' \xleftarrow{\$} \mathcal{A}(st, c + c'_b)$; Return b'

Figure 4: Games for decisional Diffie-Hellman and class-hiding instantiated with $\mathcal{SRC}$ from Fig. 3

Let us now consider a uniform random element $sig' = (Z' = z'G, S' = s'G, \hat{S}' = \hat{s}'\hat{G}, T' = t'G)$ from the set $\{sig' \in \mathcal{S}_{pp} \mid \mathsf{Verify}(vk, ek, \mathsf{Rndmz}(ek, c, r), sig') = 1\}$. Again considering logarithms of the verification equation yields $\hat{s}' = s'$ and

$$z's' = 1 + (c_0 + r)x_0 + (c_1 + rd)x_1 = 1 + c_0x_0 + c_1x_1 + r(x_0 + dx_1) \overset{(1),(2)}{=} zs + rts$$
$$t's' = x_0 + dx_1 \overset{(2)}{=} ts$$

Moreover, by signature validity, we have $s \neq 0$ and $s' \neq 0$. We thus have $Z' = \frac{s}{s'}(Z + rT)$ and $T' = \frac{s}{s'}T$, as well as $S' = \frac{s'}{s}S$ and $\hat{S}' = \frac{s'}{s}\hat{S}$ (since $\hat{s} = s$ and $\hat{s}' = s'$). In other words, sig' is a uniform element from the set $\{(\frac{1}{s^*}(Z + rT), s^*S, s^*\hat{S}, T' = \frac{1}{s^*}T) \mid s^* \in \mathbb{Z}_p^*\}$. Since $\mathsf{Adapt}(sig, r)$ outputs a uniform random element from that set, this concludes the proof. □

Proof of unforgeability

Our main technical result is to prove that our scheme satisfies unforgeability (Def. 6) in the generic group model [Sho97] for asymmetric ("Type-3") bilinear groups (for which there are no efficiently computable homomorphisms between $\mathbb{G}$ and $\hat{\mathbb{G}}$). In this model, the adversary is only given *handles* of group elements, which are just uniform random strings. To perform group operations, it uses an oracle to which it can submit handles and is given back the handle of the sum, inversion, etc of the group elements for which it submitted handles.

Theorem 1. *A generic adversary $\mathcal{A}$ that computes at most q group operations and makes up to k queries to its signature oracle cannot win the game $\mathbf{EUF}^{\mathcal{A}}_{\mathcal{SRC}}(\lambda)$ from Fig. 2 for $\mathcal{SRC}$ defined in Fig. 3 with probability greater than $2^{-\lambda}(2k+1)(q+3k+3)^2$.*

Proof. We consider an adversary that only uses generic group operations on the group elements it receives. After getting a verification key $(\hat{X}_0 = x_0\hat{G}, \hat{X}_1 = x_1\hat{G})$ and signatures $(Z_i, S_i, \hat{S}_i, T_i)_{i=1}^k$ computed with randomness s_i on queries $((P^{(i)}, (C_0^{(i)}, C_1^{(i)})))_{i=1}^k$, the adversary outputs an encryption key $P^{(k+1)}$, a ciphertext $((C_0^{(k+1)}, C_1^{(k+1)}))$ and a signature $(Z^*, S^*, \hat{S}^*, T^*)$ for them. As it must compute any new group element by combining received group elements, it must choose coefficients $\psi^{(i)}, \psi_{z,1}^{(i)}, \ldots, \psi_{z,i-1}^{(i)}, \psi_{s,1}^{(i)}, \ldots, \psi_{s,i-1}^{(i)}, \psi_{t,1}^{(i)}, \ldots, \psi_{t,i-1}^{(i)}, \gamma^{(i)}, \gamma_{z,1}^{(i)}, \ldots, \gamma_{z,i-1}^{(i)}, \gamma_{s,1}^{(i)}, \ldots, \gamma_{s,i-1}^{(i)}, \gamma_{t,1}^{(i)}, \ldots, \gamma_{t,i-1}^{(i)}$, $\kappa^{(i)}, \kappa_{z,1}^{(i)}, \ldots, \kappa_{z,i-1}^{(i)}, \kappa_{s,1}^{(i)}, \ldots, \kappa_{s,i-1}^{(i)}, \kappa_{t,1}^{(i)}, \ldots, \kappa_{t,i-1}^{(i)}$ for all $i \in \{1, \ldots, k+1\}$, as well as $\sigma, \sigma_{z,1}, \ldots, \sigma_{z,k}, \sigma_{s,1}, \ldots, \sigma_{s,k}, \sigma_{t,1}, \ldots, \sigma_{t,k}$, $\tau, \tau_{z,1}, \ldots, \tau_{z,k}, \tau_{s,1}, \ldots, \tau_{s,k}, \tau_{t,1}, \ldots, \tau_{t,k}$, $\zeta, \zeta_{z,1}, \ldots, \zeta_{z,k}, \zeta_{s,1}, \ldots, \zeta_{s,k}, \zeta_{t,1}, \ldots, \zeta_{t,k}$, $\phi, \phi_0, \phi_1, \phi_{s,1}, \ldots, \phi_{s,k}$, which define

$$P^{(i)} = \psi^{(i)}G + \sum_{j=1}^{i-1}(\psi_{z,j}^{(i)}Z_j + \psi_{s,j}^{(i)}S_j + \psi_{t,j}^{(i)}T_j) \qquad Z^* = \zeta G + \sum_{j=1}^{k}(\zeta_{z,j}Z_j + \zeta_{s,j}S_j + \zeta_{t,j}T_j)$$
$$C_0^{(i)} = \gamma^{(i)}G + \sum_{j=1}^{i-1}(\gamma_{z,j}^{(i)}Z_j + \gamma_{s,j}^{(i)}S_j + \gamma_{t,j}^{(i)}T_j) \qquad S^* = \sigma G + \sum_{j=1}^{k}(\sigma_{z,j}Z_j + \sigma_{s,j}S_j + \sigma_{t,j}T_j)$$
$$C_1^{(i)} = \kappa^{(i)}G + \sum_{j=1}^{i-1}(\kappa_{z,j}^{(i)}Z_j + \kappa_{s,j}^{(i)}S_j + \kappa_{t,j}^{(i)}T_j) \qquad T^* = \tau G + \sum_{j=1}^{k}(\tau_{z,j}Z_j + \tau_{s,j}S_j + \tau_{t,j}T_j)$$
$$\hat{S}^* = \phi\hat{G} + \phi_0\hat{X}_0 + \phi_1\hat{X}_1 + \sum_{j=1}^{k}\phi_{s,j}\hat{S}_j$$

Using this, we can write, for all $1 \leq i \leq k$, the discrete logarithms z_i and t_i in basis G of the elements $Z_i = \frac{1}{s_i}(G + x_0C_0^{(i)} + x_1C_1^{(i)})$ and $T_i = \frac{1}{s_i}(x_0G + x_1P^{(i)})$ from the oracle answers.

$$z_i = \frac{1}{s_i}\Big(1 + x_0\Big(\gamma^{(i)} + \sum_{j=1}^{i-1}(\gamma_{z,j}^{(i)}z_j + \gamma_{s,j}^{(i)}s_j + \gamma_{t,j}^{(i)}t_j)\Big) + x_1\Big(\kappa^{(i)} + \sum_{j=1}^{i-1}(\kappa_{z,j}^{(i)}z_j + \kappa_{s,j}^{(i)}s_j + \kappa_{t,j}^{(i)}t_j)\Big)\Big) \quad (3)$$
$$t_i = \frac{1}{s_i}\Big(x_0 + x_1\Big(\psi^{(i)} + \sum_{j=1}^{i-1}(\psi_{z,j}^{(i)}z_j + \psi_{s,j}^{(i)}s_j + \psi_{t,j}^{(i)}t_j)\Big)\Big) \quad (4)$$

We interpret these values as multivariate rational fractions in variables $x_0, x_1, s_1, \ldots, s_k$. A successful forgery $(Z^*, S^*, \hat{S}^*, T^*)$ on $\left(P^{(k+1)}, (C_0^{(k+1)}, C_1^{(k+1)})\right)$ satisfies the verification equations

$$e(Z^*, \hat{S}^*) = e(G, \hat{G})e(C_0^{(k+1)}, \hat{X}_0)e(C_1^{(k+1)}, \hat{X}_1) \qquad e(G, \hat{S}^*) = e(S^*, \hat{G})$$
$$e(T^*, \hat{S}^*) = e(G, \hat{X}_0)e(P^{(k+1)}, \hat{X}_1)$$

Using the coefficients defined above and considering the logarithms in base $e(G, \hat{G})$ we obtain:

$$\left(\zeta + \sum_{j=1}^{k} \left(\zeta_{z,j} z_j + \zeta_{s,j} s_j + \zeta_{t,j} t_j\right)\right)\left(\phi + \phi_0 x_0 + \phi_1 x_1 + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = 1 + x_0 c_0^{(k+1)} + x_1 c_1^{(k+1)} \tag{5}$$

$$\phi + \phi_0 x_0 + \phi_1 x_1 + \sum_{i=1}^{k} \phi_{s,i} s_i = \sigma + \sum_{j=1}^{k} \left(\sigma_{z,j} z_j + \sigma_{s,j} s_j + \sigma_{t,j} t_j\right) \tag{6}$$

$$\left(\tau + \sum_{j=1}^{k} \left(\tau_{z,j} z_j + \tau_{s,j} s_j + \tau_{t,j} t_j\right)\right)\left(\phi + \phi_0 x_0 + \phi_1 x_1 + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = x_0 + x_1 d^{(k+1)} \tag{7}$$

where for all $i \in \{1, \ldots, k+1\} : c_0^{(i)} = \log C_0^{(i)} = \gamma^{(i)} + \sum_{j=1}^{i-1} \left(\gamma_{z,j}^{(i)} z_j + \gamma_{s,j}^{(i)} s_j + \gamma_{t,j}^{(i)} t_j\right)$, (8)

$$c_1^{(i)} = \kappa^{(i)} + \sum_{j=1}^{i-1} \left(\kappa_{z,j}^{(i)} z_j + \kappa_{s,j}^{(i)} s_j + \kappa_{t,j}^{(i)} t_j\right) \text{ and } d^{(i)} = \log P^{(i)} = \psi^{(i)} + \sum_{j=1}^{i-1} \left(\psi_{z,j}^{(i)} z_j + \psi_{s,j}^{(i)} s_j + \psi_{t,j}^{(i)} t_j\right).$$

We follow the standard proof technique for results in the generic group model and now consider an "ideal" game in which the challenger treats all the (handles of) group elements as elements of $\mathbb{Z}_p(s_1, \ldots, s_k, x_0, x_1)$, that is, rational fractions whose indeterminates represent the secret values chosen by the challenger.

We first show that in the ideal game if the adversary's output satisfies the verification equations, then the second winning condition, $\left(P^{(k+1)}, (C_0^{(k+1)}, C_1^{(k+1)})\right) \notin Q$, is not satisfied, which demonstrates that the ideal game cannot be won. We then compute the statistical distance from the adversary's point of view between the real and the ideal game at the end of the proof.

In the ideal game we thus interpret the three equalities (5), (6) and (7) as polynomial equalities over the field $\mathbb{Z}_p(s_1, \ldots, s_k, x_0, x_1)$. More precisely, we consider the equalities in the ring $\mathbb{Z}_p(s_1, \ldots, s_k)[x_0, x_1]$, that is, the polynomial ring with x_0 and x_1 as indeterminates over the field $\mathbb{Z}_p(s_1, \ldots, s_k)$. (Note that this interpretation is possible because x_0 and x_1 never appear in the denominators of any expressions.) As one of our proof techniques, we will also consider the equalities over the ring factored by (x_0, x_1), the ideal generated by x_0 and x_1:[1]

$$\mathbb{Z}_p(s_1, \ldots, s_k)[x_0, x_1]/(x_0, x_1) \cong \mathbb{Z}_p(s_1, \ldots, s_k) \ .$$

From (3) and (4), over this quotient we have $z_i = \frac{1}{s_i}$ and $t_i = 0$ and thus (5)–(7) become

$$\left(\zeta + \sum_{j=1}^{k} \left(\zeta_{z,j} \frac{1}{s_j} + \zeta_{s,j} s_j\right)\right)\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = 1 \tag{9}$$

$$\phi + \sum_{i=1}^{k} \phi_{s,i} s_i = \sigma + \sum_{i=1}^{k} \left(\sigma_{z,i} \frac{1}{s_i} + \sigma_{s,i} s_i\right) \tag{10}$$

$$\left(\tau + \sum_{i=1}^{k} \left(\tau_{z,i} \frac{1}{s_i} + \tau_{s,i} s_i\right)\right)\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = 0 \tag{11}$$

[1] Considering an equation of rational fractions over this quotient can also be seen as simply setting $x_0 = x_1 = 0$. Everything we infer about the coefficients from these modified equations is also valid for the original equation, since these must hold for all values $(x_0, x_1, s_1, \ldots, s_k)$ and so in particular for $(0, 0, s_1, \ldots, s_k)$.

Yet another interpretation when equating coefficients in equations modulo (x_0, x_1) is that one equates coefficients only of monomials that do not contain x_0 or x_1.

We first consider (10). By equating coefficients, we deduce:

$$\phi = \sigma \qquad \forall i \in \{1, \ldots, k\} : \ \phi_{s,i} = \sigma_{s,i} \quad \text{and} \quad \sigma_{z,i} = 0 \tag{12}$$

We now turn to (9) and first notice that

$$\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) \neq 0 \ , \tag{13}$$

because it is a factor of a non-zero product in (9). We next consider the degrees of the factors in (9), using the fact that the degree of a product is the sum of the degrees of the factors. Let $i \in \{1, \ldots, k\}$. Since $\deg_{s_i}(1) = 0$ and $\deg_{s_i}\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) \geq 0$, we have $\deg_{s_i}\left(\zeta + \sum_{j=1}^{k} (\zeta_{z,j} \frac{1}{s_j} + \zeta_{s,j} s_j)\right) \leq 0$, from which we get

$$\forall\, i \in \{1, \ldots, k\} : \zeta_{s,i} = 0 \ . \tag{14}$$

(Note that $\deg_{s_i}\left(\frac{1}{s_i} + s_i\right) = \deg_{s_i}\left(\frac{1+s_i^2}{s_i}\right) = 1$.) We next show that there is at most one $\phi_{s,i}$ that is non-zero. Suppose there exist $i_1 \neq i_2 \in \{1, \ldots, k\}$ such that $\phi_{s,i_1} \neq 0$ and $\phi_{s,i_2} \neq 0$. This implies that $\deg_{s_{i_1}}\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = \deg_{s_{i_2}}\left(\phi + \sum_{i=1}^{k} \phi_{s,i} s_i\right) = 1$. By considering these degrees in (9), the left factor must be of degree -1, that is (recall that $\zeta_{s,i} = 0$ for all i by (14)):

$$\deg_{s_{i_1}}\left(\zeta + \sum_{j=1}^{k} \zeta_{z,j} \frac{1}{s_j}\right) = -1 \quad \text{and} \quad \deg_{s_{i_2}}\left(\zeta + \sum_{j=1}^{k} \zeta_{z,j} \frac{1}{s_j}\right) = -1 \ . \tag{15}$$

This is a contradiction since the former implies that $\zeta_{z,i_1} \neq 0$, while the latter implies that $\zeta_{z,i_1} = 0$, as we show next. Consider the expression $\deg_{s_{i_2}}\left((\zeta + \sum_{j=1, j\neq i_2}^{k} \zeta_{z,j} \frac{1}{s_j}) s_{i_2} + \zeta_{z,i_2}\right) = \deg_{s_{i_2}}\left((\zeta + \sum_{j=1}^{k} \zeta_{z,j} \frac{1}{s_j}) s_{i_2}\right) = -1 + \deg_{s_{i_2}}(s_{i_2}) = 0$, by using (15). This implies $\left(\zeta + \sum_{j=1, j\neq i_2}^{k} \zeta_{z,j} \frac{1}{s_j}\right) = 0$ and thus $\zeta_{z,i_1} = 0$, which was our goal.

Therefore, there exists i_0 such that, for all $i \neq i_0$, $\phi_{s,i} = 0$ and by (12):

$$\forall\, i \in \{1, \ldots, k\} \setminus \{i_0\} : \sigma_{s,i} = \phi_{s,i} = 0 \ . \tag{16}$$

Together with (14), this means that we can rewrite (9) as $\left(\zeta + \sum_{j=1}^{k} \zeta_{z,j} \frac{1}{s_j}\right)(\phi + \phi_{s,i_0} s_{i_0}) = 1$. Since for all $i \neq i_0$, s_i does not appear in 1, we have

$$\forall\, i \in \{1, \ldots, k\} \setminus \{i_0\} : \zeta_{z,i} = 0 \ . \tag{17}$$

We now consider equation (6) modulo (x_1). Since, by (12), $\phi = \sigma$ and $\phi_{s,i} = \sigma_{s,i}$ for all i, two terms cancel on both sides. Moreover, by (12), $\sigma_{z,i} = 0$ for all i and thus, using $t_i \bmod (x_1) = \frac{x_0}{s_i}$ for all i, yields

$$\phi_0 x_0 = \sum_{i=1}^{k} \sigma_{t,i} \frac{x_0}{s_i} \ . \tag{18}$$

By identifying coefficients, we deduce that

$$\forall\, i \in \{1, \ldots, k\} : \sigma_{t,i} = \phi_0 = 0 \ . \tag{19}$$

Using all of this in the original equation (6) (that is, "putting back" x_1 in (18) and applying (19)) yields $\phi_1 x_1 = 0$ and thus

$$\phi_1 = 0 \ . \tag{20}$$

We now turn to (11), in which by (13) we have $\big(\tau + \sum_{i=1}^{k}(\tau_{z,i}\frac{1}{s_i} + \tau_{s,i}s_i)\big) = 0$. From this we get by equating coefficients:

$$\forall\, i \in \{1,\ldots,k\} : \tau_{z,i} = \tau_{s,i} = \tau = 0\ .$$

Going back to equation (7) and applying the latter, as well as (19), (20) and (16) yields

$$\Big(\sum_{i=1}^{k}\tau_{t,i}t_i\Big)(\phi + \phi_{s,i_0}s_{i_0}) = x_0 + x_1\Big(\psi^{(k+1)} + \sum_{j=1}^{k}\big(\psi_{z,j}^{(k+1)}z_j + \psi_{s,j}^{(k+1)}s_j + \psi_{t,j}^{(k+1)}t_j\big)\Big)\ . \tag{21}$$

Computing this modulo (x_1) and recalling $t_i \bmod (x_1) = \frac{x_0}{s_i}$ yields $\big(\sum_{i=1}^{k}\tau_{t,i}\frac{x_0}{s_i}\big)(\phi + \phi_{s,i_0}s_{i_0}) = x_0$, and thus

$$\sum_{i=1}^{k}\phi\tau_{t,i}\frac{x_0}{s_i} + \sum_{i=1,i\neq i_0}^{k}\phi_{s,i_0}\tau_{t,i}s_{i_0}\frac{x_0}{s_i} + \phi_{s,i_0}\tau_{t,i_0}x_0 = x_0\ .$$

By equating the coefficients for x_0, we deduce that

$$\phi_{s,i_0}\tau_{t,i_0} = 1 \quad (\text{and thus } \phi_{s,i_0} \neq 0 \text{ and } \tau_{t,i_0} \neq 0)\,. \tag{22}$$

Moreover, for all $i \in \{1,\ldots,k\}\setminus\{i_0\}$, we deduce $\phi_{s,i_0}\tau_{t,i} = 0$ and $\phi\tau_{t,i_0} = 0$, which by applying (22) to both yields

$$\forall\, i \in \{1,\ldots,k\}\setminus\{i_0\} : \tau_{t,i} = 0 \quad \text{and} \quad \phi = 0\ . \tag{23}$$

Using this, the left-hand side of (21) becomes $\phi_{s,i_0}\tau_{t,i_0}t_{i_0}s_{i_0}$, which, applying (22) and (4), becomes $\frac{1}{s_{i_0}}(x_0 + x_1 d^{(i_0)})s_{i_0}$. This means that (21) becomes $x_0 + x_1 d^{(i_0)} = x_0 + x_1 d^{(k+1)}$, which implies $x_1(d^{(i_0)} - d^{(k+1)}) = 0$. Since a polynomial ring over a integral domain such as $\mathbb{Z}_p(s_1,\ldots,s_k)$ is an integral domain, and $x_1 \neq 0$, the last equality implies $d^{(i_0)} = d^{(k+1)}$. This means

$$P^{(i_0)} = P^{(k+1)}\ , \tag{24}$$

that is, the encryption key of the forgery is the same as used in the i_0-th query. We next show that the ciphertext $\big(C_0^{(k+1)}, C_1^{(k+1)}\big)$ of the forgery is a randomization of the one from the i_0-th query.

Consider equation (9). Since $\zeta_{z,i} = 0$ for $i \neq i_0$ (by (17)), all $\zeta_{s,i} = 0$ (by (14)), $\phi = 0$ (by (23)) and $\phi_{s,i} = 0$ for $i \neq i_0$ (by (16)), it simplifies to

$$\Big(\zeta + \zeta_{z,i_0}\frac{1}{s_{i_0}}\Big)\phi_{s,i_0}s_{i_0} = \zeta\phi_{s,i_0}s_{i_0} + \zeta_{z,i_0}\phi_{s,i_0} = 1\ , \tag{25}$$

from which we deduce

$$\zeta_{z,i_0}\phi_{s,i_0} = 1 \quad \text{and} \quad \zeta = 0\ . \tag{26}$$

We now consider (5) modulo (x_1) and apply what we have deduced so far, that is $\zeta = 0$ by (26), the coefficients previously mentioned above (25) and $\phi_0 = 0$ by (19). The left-hand side of (5) modulo (x_1) becomes thus $\Big(\zeta_{z,i_0}z_{i_0} + \sum_{j=1}^{k}\zeta_{t,j}t_j\Big)\phi_{s,i_0}s_{i_0} \bmod (x_1)$. Using moreover (26), we get that (5) modulo (x_1) becomes

$$\begin{aligned} &z_{i_0}s_{i_0} + \Big(\sum_{j=1}^{k}\zeta_{t,j}t_j\Big)\phi_{s,i_0}s_{i_0} \bmod (x_1) \\ &\qquad = 1 + x_0\Big(\gamma^{(k+1)} + \sum_{j=1}^{k}\big(\gamma_{z,j}^{(k+1)}z_j + \gamma_{s,j}^{(k+1)}s_j + \gamma_{t,j}^{(k+1)}t_j\big)\Big) \bmod (x_1)\ , \end{aligned} \tag{27}$$

and using $z_i \bmod (x_1) = \frac{1+c_0^{(i)}x_0}{s_i} \bmod (x_1)$ and $t_i \bmod (x_1) = \frac{x_0}{s_i}$ for all i (cf. (3) and (4)) we get

$$\begin{aligned}&\big(1+c_0^{(i_0)}\big)x_0 + \Big(\sum_{j=1}^{k} \zeta_{t,j}\frac{x_0}{s_j}\Big)\phi_{s,i_0}s_{i_0} \bmod (x_1)\\ &\qquad = 1 + x_0\Big(\gamma^{(k+1)} + \sum_{j=1}^{k}\Big(\gamma_{z,j}^{(k+1)}\frac{1+c_0^{(j)}x_0}{s_j} + \gamma_{s,j}^{(k+1)}s_j + \gamma_{t,j}^{(k+1)}\frac{x_0}{s_j}\Big)\Big) \bmod (x_1)\ . \quad (28)\end{aligned}$$

Let $i > i_0$ and let us consider the monomials of degree -1 in s_i and degree 0 in s_j, for all $j > i$. Note that all monomials of $c_0^{(j)} = \gamma^{(j)} + \sum_{\ell=1}^{j-1}\big(\gamma_{z,\ell}^{(j)}z_\ell + \gamma_{s,\ell}^{(j)}s_\ell + \gamma_{t,\ell}^{(j)}t_\ell\big)$ are of degree 0 in s_ℓ, for $\ell \geq j$. Therefore, we do not consider any $\frac{c_0^{(j)}}{s_j}$ for $j < i$ (because they do not contain the term s_i) nor $\frac{c_0^{(j)}}{s_j}$ for $j > i$ (since the contained monomials are of degree -1 in s_j for $j > i$). For the monomials of degree -1 in s_i and degree 0 in s_j for $j > i$ in (28) we thus have

$$\forall\, i > i_0:\ \frac{\zeta_{t,i}x_0\phi_{s,i_0}s_{i_0}}{s_i} = x_0\Big(\gamma_{z,i}^{(k+1)}\frac{1+c_0^{(i)}x_0}{s_i} + \gamma_{t,i}^{(k+1)}\frac{x_0}{s_i}\Big) \bmod (x_1) = 0\ .$$

Multiplying by s_i yields $\zeta_{t,i}x_0\phi_{s,i_0}s_{i_0} - x_0\big(\gamma_{z,i}^{(k+1)}(1+x_0c_0^{(i)}) + \gamma_{t,i}^{(k+1)}x_0\big) \bmod (x_1) = 0$ and after reordering the monomials according to their degree in x_0 we get

$$\forall\, i > i_0: -x_0^2\big(\gamma_{z,i}^{(k+1)}c_0^{(i)} + \gamma_{t,i}^{(k+1)}\big) + x_0\big(\zeta_{t,i}\phi_{s,i_0}s_{i_0} - \gamma_{z,i}^{(k+1)}\big) \bmod (x_1) = 0\ . \quad (29)$$

Considering the linear coefficient in x_0, and recalling that $\phi_{s,i_0} \neq 0$ by (22), we deduce

$$\forall\, i > i_0:\ \gamma_{z,i}^{(k+1)} = \zeta_{t,i} = 0\ . \quad (30)$$

Applying this to equation (29) yields $x_0^2\gamma_{t,i}^{(k+1)} \bmod (x_1) = 0$ for all $i > i_0$, and therefore

$$\forall\, i > i_0:\ \gamma_{t,i}^{(k+1)} = 0\ . \quad (31)$$

Since by (30) and (31) for all $i > i_0 : \zeta_{t,i} = \gamma_{z,i}^{(k+1)} = \gamma_{t,i}^{(k+1)} = 0$, we can rewrite (27) as

$$\begin{aligned}&z_{i_0}s_{i_0} + \Big(\sum_{i=1}^{i_0}\zeta_{t,i}t_i\Big)\phi_{s,i_0}s_{i_0} \bmod (x_1)\\ &\qquad = 1 + x_0\Big(\gamma^{(k+1)} + \sum_{i=1}^{i_0}\big(\gamma_{z,i}^{(k+1)}z_i + \gamma_{t,i}^{(k+1)}t_i\big) + \sum_{i=1}^{k}\gamma_{s,i}^{(k+1)}s_i\Big) \bmod (x_1)\ . \quad (32)\end{aligned}$$

For $i > i_0$, from the coefficients of x_0s_i we get $\gamma_{s,i}^{(k+1)} = 0$. Applying this, (30) and (31) to (8) yields

$$c_0^{(k+1)} = \gamma^{(k+1)} + \sum_{i=1}^{i_0}\big(\gamma_{z,i}^{(k+1)}z_i + \gamma_{s,i}^{(k+1)}s_i + \gamma_{t,i}^{(k+1)}t_i\big)\ ; \quad (33)$$

and the right-hand side of (32) becomes $1+x_0\Big(\gamma^{(k+1)}+\sum_{i=1}^{i_0}\big(\gamma_{z,i}^{(k+1)}z_i+\gamma_{s,i}^{(k+1)}s_i+\gamma_{t,i}^{(k+1)}\frac{x_0}{s_i}\big)\Big) \bmod (x_1)$.

Since $z_i \bmod (x_1) = \frac{1+x_0c_0^{(i)}}{s_i} \bmod (x_1)$ and $t_i \bmod (x_1) = \frac{x_0}{s_i}$, for all i, (32) becomes

$$\begin{aligned}&1 + x_0c_0^{(i_0)} + \Big(\sum_{i=1}^{i_0}\zeta_{t,i}\frac{x_0}{s_i}\Big)\phi_{s,i_0}s_{i_0} \bmod (x_1)\\ &\qquad = 1 + x_0\Big(\gamma^{(k+1)} + \sum_{i=1}^{i_0}\Big(\gamma_{z,i}^{(k+1)}\frac{1+x_0c_0^{(i)}}{s_i} + \gamma_{s,i}^{(k+1)}s_i + \gamma_{t,i}^{(k+1)}\frac{x_0}{s_i}\Big)\Big) \bmod (x_1)\ .\end{aligned}$$

We will now look at the coefficients of s_{i_0} and of $\frac{1}{s_{i_0}}$. For this, we first note that for $j \geq i$ no s_j appears in $c_0^{(i)}$ (cf. (8)) and therefore for all $i \leq i_0 : c_0^{(i)}$ is constant in s_{i_0}. From the coefficients of s_{i_0} and of $\frac{1}{s_{i_0}}$ we thus get, respectively:

$$\phi_{s,i_0} \sum_{i=1}^{i_0-1} \zeta_{t,i} \frac{x_0}{s_i} = x_0 \gamma_{s,i_0}^{(k+1)} \tag{34}$$

$$0 = x_0 \big(\gamma_{z,i_0}^{(k+1)}(1 + x_0 c_0^{(i_0)}) + \gamma_{t,i_0}^{(k+1)} x_0\big) \bmod (x_1) \tag{35}$$

From (34) we get $\gamma_{s,i_0}^{(k+1)} = 0$ and, since $\phi_{s,i_0} \neq 0$ by (22),

$$\forall i < i_0 : \zeta_{t,i} = 0 \ , \tag{36}$$

and from (35) we get $\gamma_{z,i_0}^{(k+1)} = 0$ (from the coefficient of x_0) and therefore $\gamma_{t,i_0}^{(k+1)} = 0$. Together, this lets us rewrite (33) as

$$c_0^{(k+1)} = \gamma^{(k+1)} + \sum_{i=1}^{i_0-1} \big(\gamma_{z,i}^{(k+1)} z_i + \gamma_{s,i}^{(k+1)} s_i + \gamma_{t,i}^{(k+1)} t_i\big) \big) \ . \tag{37}$$

Recall that $\hat{S}^* = \phi \hat{G} + \phi_0 \hat{X}_0 + \phi_1 \hat{X}_1 + \sum_{j=1}^{k} \phi_{s,j} \hat{S}_j$ and $Z^* = \zeta G + \sum_{j=1}^{k} \big(\zeta_{z,j} Z_j + \zeta_{s,j} S_j + \zeta_{t,j} T_j\big)$. By (23), (19), (20) and (16) we have $\hat{S}^* = \phi_{s,i_0} \hat{S}_{i_0}$ Moreover, by (26), (17), (14), (30) and (36) we have $Z^* = \zeta_{z,i_0} Z_{i_0} + \zeta_{t,i_0} T_{i_0}$. We can now rewrite (5) as:

$$(\zeta_{z,i_0} z_{i_0} + \zeta_{t,i_0} t_{i_0})(\phi_{s,i_0} s_{i_0}) = 1 + x_0 c_0^{(k+1)} + x_1 c_1^{(k+1)} \ .$$

Since, by (26), $\zeta_{z,i_0} \phi_{s,i_0} = 1$ and plugging in the definitions of z_{i_0} and t_{i_0}, this yields

$$\begin{aligned} 1 + x_0 c_0^{(i_0)} + x_1 c_1^{(i_0)} + \zeta_{t,i_0} \phi_{s,i_0} \big(x_0 + x_1 d^{(i_0)}\big) &= 1 + x_0 c_0^{(k+1)} + x_1 c_1^{(k+1)} \ , \quad \text{and thus} \\ x_0 \big(c_0^{(i_0)} + \zeta_{t,i_0} \phi_{s,i_0} - c_0^{(k+1)}\big) &= -x_1 \big(c_1^{(i_0)} + \zeta_{t,i_0} \phi_{s,i_0} d^{(i_0)} - c_1^{(k+1)}\big) \ . \end{aligned} \tag{38}$$

By considering the above modulo (x_1), plugging in the definition of $c_0^{(i)}$ from (8) and using (37), we get

$$\begin{aligned} 0 &= \zeta_{t,i_0} \phi_{s,i_0} + c_0^{(i_0)} - c_0^{(k+1)} \bmod (x_1) \\ &= \zeta_{t,i_0} \phi_{s,i_0} + \gamma^{(i_0)} - \gamma^{(k+1)} + \sum_{j=1}^{i_0-1} \big((\gamma_{z,j}^{(i_0)} - \gamma_{z,j}^{(k+1)}) z_j + (\gamma_{s,j}^{(i_0)} - \gamma_{s,j}^{(k+1)}) s_j + (\gamma_{t,j}^{(i_0)} - \gamma_{t,j}^{(k+1)}) t_j\big) \\ &\qquad \bmod (x_1) \\ &= \zeta_{t,i_0} \phi_{s,i_0} + \gamma^{(i_0)} - \gamma^{(k+1)} \\ &\quad + \sum_{j=1}^{i_0-1} \Big((\gamma_{z,j}^{(i_0)} - \gamma_{z,j}^{(k+1)}) \frac{(1 + x_0 c_0^{(j)})}{s_j} + (\gamma_{s,j}^{(i_0)} - \gamma_{s,j}^{(k+1)}) s_j + (\gamma_{t,j}^{(i_0)} - \gamma_{t,j}^{(k+1)}) \frac{x_0}{s_j}\Big) \bmod (x_1) \ . \end{aligned} \tag{39}$$

Taking the above modulo (x_0) we get

$$\zeta_{t,i_0} \phi_{s,i_0} + \gamma^{(i_0)} - \gamma^{(k+1)} + \sum_{j=1}^{i_0-1} ((\gamma_{z,j}^{(i_0)} - \gamma_{z,j}^{(k+1)}) \frac{1}{s_j} + (\gamma_{s,j}^{(i_0)} - \gamma_{s,j}^{(k+1)}) s_j) \bmod (x_0, x_1) = 0 \ .$$

By looking at the coefficients of the constant monomial and of $\frac{1}{s_i}$ and s_i for all $i < i_0$, we deduce the following:

$$\zeta_{t,i_0} \phi_{s,i_0} + \gamma^{(i_0)} - \gamma^{(k+1)} = 0 \tag{40}$$

$$\forall i < i_0 : \ \gamma_{z,i}^{(i_0)} - \gamma_{z,i}^{(k+1)} = 0 \quad \text{and} \quad \gamma_{s,i}^{(i_0)} - \gamma_{s,i}^{(k+1)} = 0 \tag{41}$$

This lets us rewrite (39) as $\sum_{j=1}^{i_0-1}(\gamma_{t,j}^{(i_0)} - \gamma_{t,j}^{(k+1)})\frac{x_0}{s_j} \bmod (x_1) = 0$, and equating the coefficients of $\frac{x_0}{s_j}$ for all $j < i_0$ yields

$$\forall i < i_0 : \gamma_{t,i}^{(i_0)} = \gamma_{t,i}^{(k+1)} \ . \tag{42}$$

Applying (40), (41) and (42) to (37) yields

$$c_0^{(k+1)} = \zeta_{t,i_0}\phi_{s,i_0} + \gamma^{(i_0)} + \sum_{i=1}^{i_0-1}\left(\gamma_{z,i}^{(i_0)} z_i + \gamma_{s,i}^{(i_0)} s_i + \gamma_{t,i}^{(i_0)} t_i\right) \ .$$

Recalling the definition of $c_0^{(i_0)}$ form (8), we can conclude that:

$$c_0^{(k+1)} = \zeta_{t,i_0}\phi_{s,i_0} + c_0^{(i_0)} \ .$$

Therefore (38) becomes $0 = -x_1\left(c_1^{(i_0)} + \zeta_{t,i_0}\phi_{s,i_0} d^{(i_0)} - c_1^{(k+1)}\right)$, in other words

$$c_1^{(k+1)} = \zeta_{t,i_0}\phi_{s,i_0} d^{(i_0)} + c_1^{(i_0)} \ .$$

The last two equations mean that $\left(C_0^{(k+1)}, C_1^{(k+1)}\right) = \left(C_0^{(i_0)} + rG,\ C_1^{(i_0)} + rP^{(i_0)}\right)$, for $r = \zeta_{t,i_0}\phi_{s,i_0}$, which together with (24) means that

$$\left(P^{(k+1)}, (C_0^{(k+1)}, C_1^{(k+1)})\right) \in \left\{P^{(i_0)}\right\} \times \left[(C_0^{(i_0)}, C_1^{(i_0)})\right]_{P^{(i_0)}} \subset Q \ .$$

We have thus shown that in the "ideal" model, the attacker cannot win the game. It remains to upper-bound the statistical distance from the adversary point of view between these two models.

Difference between ideal and real game. We start with upper-bounding the degree of the denominators and numerators of the rational fractions that can be generated by the adversary.

We first show that by induction on the number of queries k, that all the elements returned by the challenger in the ideal game are divisors of $\prod_{i=1}^{k} s_i$. In the base case, when no queries are made, no s_i appears and the elements returned by the adversary are polynomials. For the induction step, assume the statement holds for ℓ queries. Consider the reply to the $(\ell+1)$-th query: $S_{\ell+1}$ and $\hat{S}_{\ell+1}$ are monomials; $Z_{\ell+1}$ and $T_{\ell+1}$ are sums of polynomials and elements output by the adversary divided by $s_{\ell+1}$. Using the induction hypothesis on the adversary's outputs, we deduce that the denominators divide $\prod_{i=1}^{\ell+1} s_i$. □

Similarly, we can show that the numerators of each element output by the challenger can be written as a sum of divisors of $x_0^{k+1}\, x_1^{k+1} \prod_{i=1}^{k} s_i$.

The "ideal" model and the generic group model differ if and only if two elements are distinct as rational fractions but identical as (handle of a) group element. That is, if we evaluate two different rational fractions at scalar values $x_0, x_1, s_1, \ldots, s_k$ and obtain the same result.

Any such equality of rational fractions generated during the game can be rewritten as a polynomial equation of degree $3k + k + 2$ ($3k + 2$ upper-bounding the degree of the numerator and k that of the denominator). Because the values $x_0, x_1, s_1, \ldots, s_k$ are uniformly random (and hidden from the adversary), the Schwartz-Zippel lemma [Sch80] yields that the probability of this equality holding is at most $\frac{4k+2}{p-1}$.

If the adversary computes at most q group operations, then there are at most $q + 3 + 3k$ group elements, where 3 comes from the generator and the verification key, and $3k$ corresponds to the answers to the signing queries (note that $\hat{S}$ and S correspond to the same monomial). There are therefore

$$\tfrac{1}{2}(q + 3k + 3)(q + 3k + 2)$$

pairs of rational fractions. Using the union bound, we conclude that the adversary can distinguish the two models with probability at most $\frac{4k+2}{2(p-1)}(q + 3k + 3)(q + 3k + 2) < \frac{2k+1}{2^\lambda}(q + 3k + 3)^2$, since $p - 1 > 2^\lambda$, which is the bound claimed by the theorem. □

Generalization of our scheme. We conclude by mentioning that our scheme easily generalizes to ElGamal encryptions of vectors of group elements without increasing the size of signatures: for an encryption key $(P_1, \ldots, P_n)$ and a signing key $(x_0, \ldots, x_n)$, a ciphertext consisting of $C_0 = rG$ and $C_i = M_i + rP_i$ for $1 \leq i \leq n$, a signature on randomizable ciphertexts is defined as:

$$Z := \frac{1}{s}\Big(G + \sum_{i=0}^{n} x_i C_i\Big) \qquad S := sG \qquad \hat{S} := s\hat{G} \qquad T := \frac{1}{s}\Big(x_0 G + \sum_{i=1}^{n} x_i P_i\Big)$$

Acknowledgements. This is work is funded in part by the MSR–Inria Joint Centre. Fuchsbauer is supported by the Vienna Science and Technology Fund (WWTF) through project VRG18-002.

References

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

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

[AGO11] Masayuki Abe, Jens Groth and Miyako Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In D.H. Lee and X. Wang, editors, *ASIACRYPT 2011*, vol. 7073 of *LNCS*, pp. 628–646. Springer, 2011.

[AW98] Claude Deschamps André Warusfel, François Moulin. *Mathématiques 1ère année : Cours et exercices corrigés.* Editions Dunod, 1998.

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

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss and Anna Lysyanskaya. P-signatures and non-interactive anonymous credentials. In R. Canetti, editor, *TCC 2008*, vol. 4948 of *LNCS*, pp. 356–374. Springer, 2008.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval and Damien Vergnaud. Signatures on randomizable ciphertexts. In D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, editors, *PKC 2011*, vol. 6571 of *LNCS*, pp. 403–422. Springer, 2011.

[BFPV13] Olivier Blazy, Georg Fuchsbauer, David Pointcheval and Damien Vergnaud. Short blind signatures. *Journal of computer security*, 21(5):627–661, 2013.

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

[BL13] Foteini Baldimtsi and Anna Lysyanskaya. Anonymous credentials light. In A.R. Sadeghi, V.D. Gligor and M. Yung, editors, *ACM CCS 2013*, pp. 1087–1098. ACM Press, 2013.

[BMW03] M. Bellare, D. Micciancio and B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Eli Biham, editor, *EUROCRYPT 2003*, vol. 2656 of *LNCS*, pp. 614–629. Springer, 2003.

[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 A. Menezes, editor, *CT-RSA 2005*, vol. 3376 of *LNCS*, pp. 136–153. Springer, 2005.

[CCFG16] Pyrros Chaidos, Véronique Cortier, Georg Fuchsbauer and David Galindo. BeleniosRF: A non-interactive receipt-free electronic voting scheme. In E.R. Weippl, S. Katzenbeisser, C. Kruegel, A.C. Myers and S. Halevi, editors, *ACM CCS 2016*, pp. 1614–1625. ACM 2016.

[CFL19] Véronique Cortier, Alicia Filipiak and Joseph Lallemand. Beleniosvs: Secrecy and verifiability against a corrupted voting device. In *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*, pp. 367–36714. IEEE, 2019.

[CG05] Jan Camenisch and Jens Groth. Group signatures: Better efficiency and new theoretical aspects. In C. Blundo and S. Cimato, editors, *SCN 04*, vol. 3352 of *LNCS*, pp. 120–133. Springer, 2005.

[CGG19] Véronique Cortier, Pierrick Gaudry and Stephane Glondu. Belenios: a simple private and verifiable electronic voting system. In *Foundations of Security, Protocols, and Equational Reasoning*, pp. 214–238. Springer, 2019.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In S. Cimato, C. Galdi and G. Persiano, editors, *SCN 02*, vol. 2576 of *LNCS*, pp. 268–289. Springer, 2003.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In M. Franklin, editor, *CRYPTO 2004*, vol. 3152 of *LNCS*, pp. 56–72. Springer, 2004.

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

[DHO16] Ivan Damgård, Helene Haagh and Claudio Orlandi. Access control encryption: Enforcing information flow with cryptography. In M. Hirt and A.D. Smith, editors, *TCC 2016-B, Part II*, vol. 9986 of *LNCS*, pp. 547–576. Springer, 2016.

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

[DS18] David Derler and Daniel Slamanig. Highly-efficient fully-anonymous dynamic group signatures. In J. Kim, G.J. Ahn, S. Kim, Y. Kim, J. López and T. Kim, editors, *ASIACCS 18*, pp. 551–565. ACM Press, 2018.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

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

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

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

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

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

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

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In N.P. Smart, editor, *EUROCRYPT 2008*, vol. 4965 of *LNCS*, pp. 415–432. Springer, 2008.

[HPP20] Chloé Hébant, Duong Hieu Phan and David Pointcheval. Linearly-homomorphic signatures and scalable mix-nets. In *PKC 2020*, LNCS. Springer, 2020.

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

[KSD19] Mojtaba Khalili, Daniel Slamanig and Mohammad Dakhilalian. Structure-preserving signatures on equivalence classes from standard assumptions. In S.D. Galbraith and S. Moriai, editors, *ASIACRYPT 2019, Part III*, vol. 11923 of *LNCS*, pp. 63–93. Springer, 2019.

[Sch80] Jacob T Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 27(4):701–717, 1980.

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

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT 2005*, vol. 3494 of *LNCS*, pp. 114–127. Springer, 2005.