EUF-CMA-Secure Structure-Preserving Signatures on Equivalence Classes

Georg Fuchsbauer[1] Christian Hanser[2†] Daniel Slamanig[2†]

[1] IST Austria
georg.fuchsbauer@ist.ac.at

[2] Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology (TUG), Inffeldgasse 16a, 8010 Graz, Austria
{christian.hanser|daniel.slamanig}@iaik.tugraz.at

Abstract

At ASIACRYPT'14 Hanser and Slamanig proposed a new primitive called structure-preserving signatures on equivalence classes (SPS-EQ) and used it to construct very efficient attribute-based anonymous credentials. They also presented a candidate construction of an SPS-EQ scheme and claimed that the scheme was existentially unforgeable under adaptive chosen message attacks (EUF-CMA). Fuchsbauer has however recently shown that the construction is insecure under adaptive queries and consequently the security claim is invalid. We fix this issue by providing an EUF-CMA-secure construction of an SPS-EQ, which is also more efficient than the original construction in every respect. We prove our scheme secure in the generic group model for Type-3 bilinear groups.

1 Introduction

At ASIACRYPT'14 Hanser and Slamanig [HS14] proposed a new type of structure-preserving signature [AFG+10], which does not sign group-element vectors as such, but projective equivalence classes defined on the corresponding vector space. This allows efficient re-randomization of message-signature pairs by switching to another representative. In particular, message vectors can be re-randomized by scalar multiplication and signatures on them can be updated consistently (and randomized themselves) in the public. A re-randomized message-signature pair is then indistinguishable from a signed random message. This enables, for instance, new, efficient constructions of attribute-based multi-show anonymous credential (ABC) systems when combined with re-randomizable polynomial commitments, as shown in [HS14].

The authors also proposed a candidate construction of an SPS-EQ scheme and claimed that the scheme was existentially unforgeable under adaptive chosen-message attacks (EUF-CMA-secure). Recently, Fuchsbauer [Fuc14] however showed an attack using adaptive message queries, meaning that the claim of EUF-CMA security in [HS14] is invalid. This is due to an erroneous generic-group-model proof which considers the adversary solely in a non-adaptive way, that is, the proof neglects to take into account adaptive message queries.

In this paper we present a new construction of an SPS-EQ scheme, which we prove EUF-CMA-secure in the generic group model. Our construction is even more efficient than the one from [HS14] (in terms of key size, signature size, as well as the number of pairing-product equations required for signature verification). This shows the existence of EUF-CMA-secure SPS-EQ schemes with respect to the generic group model and therefore the construction of an ABC system given in [HS14], which is black-box from any EUF-CMA-secure SPS-EQ scheme, can be efficiently instantiated. It moreover benefits from the improved efficiency of our signature scheme.

[†]Part of this work has been done while visiting IST Austria.

2 Preliminaries

Definition 1 (Bilinear map)**.** Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic groups of prime order p where we denote $\mathbb{G}_1$ and $\mathbb{G}_2$ additively and $\mathbb{G}_T$ multiplicatively. We write $\mathbb{G}_i^*$ for $\mathbb{G}_i \setminus \{0_{\mathbb{G}_i}\}$ where $i \in \{1,2\}$. Let P and $\hat{P}$ be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. 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: $e(aP, b\hat{P}) = e(P,\hat{P})^{ab} \quad \forall\, a, b \in \mathbb{Z}_p$.

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 called *symmetric* (Type-1) and *asymmetric* (Type-2 or Type-3) otherwise. For Type-2 pairings there is an efficiently computable isomorphism $\Psi\colon \mathbb{G}_2 \to \mathbb{G}_1$, whereas for Type-3 pairings no such efficient isomorphism is assumed to exist. Note that Type-3 pairings are currently the optimal choice [CM11] with respect to efficiency and security trade-off.

Definition 2 (Decisional Diffie-Hellman assumption (DDH))**.** Let p be a prime of bitlength κ and $\mathbb{G}$ be a group of order p generated by P. Then, for every PPT adversary $\mathcal{A}$ distinguishing between $(P, aP, bP, abP) \in \mathbb{G}^4$ and $(P, aP, bP, cP) \in \mathbb{G}^4$ for $a, b, c \xleftarrow{R} \mathbb{Z}_p^*$ (i.e., uniformly random) is infeasible, i.e., there is a negligible function $\epsilon(\cdot)$ such that

$$\left|\Pr\left[\mathtt{true} \leftarrow \mathcal{A}(P, aP, bP, abP)\right] - \Pr\left[\mathtt{true} \leftarrow \mathcal{A}(P, aP, bP, cP)\right]\right| \leq \epsilon(\kappa) \ .$$

Definition 3 (Bilinear group generator)**.** A PPT algorithm BGGen is a bilinear-group generator if on input a security parameter κ (in unary representation) it generates $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$ where the common group order p of the groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ is a prime of bitlength κ, e is a pairing, and P and $\hat{P}$ are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

Definition 4 (Symmetric external Diffie-Hellman assumption (SXDH) [BGdMM05])**.** The SXDH assumption holds for BGGen if the DDH assumption holds for both groups $\mathbb{G}_1$ and $\mathbb{G}_2$ output by BGGen.

3 Structure-Preserving Signatures on Equivalence Classes

In a structure-preserving signature scheme [AFG+10] public keys, messages and signatures consist only of group elements of two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ that are equipped with a bilinear map. Furthermore, the verification algorithm evaluates a signature by verifying group membership and evaluating pairing-product equations.

An SPS-EQ-$\mathcal{R}$ scheme is a structure-preserving signature scheme that is defined either on the message space $(\mathbb{G}_1^*)^\ell$ or $(\mathbb{G}_2^*)^\ell$, where $\ell > 1$ and $\mathbb{G}_1$ and $\mathbb{G}_2$ have prime order. Additionally, the following equivalence relation

$$\mathcal{R} = \left\{(M, N) \in (\mathbb{G}_i^*)^\ell \times (\mathbb{G}_i^*)^\ell \;\middle|\; \exists\, s \in \mathbb{Z}_p^* \text{ such that } N = s \cdot M\right\} \subseteq (\mathbb{G}_i^*)^{2\ell}$$

partitions the message space $(\mathbb{G}_i^*)^\ell$ for $i \in \{1,2\}$ into equivalence classes. An SPS-EQ-$\mathcal{R}$ scheme now signs equivalence classes defined by equivalence relation $\mathcal{R}$ by signing an arbitrary representative of the respective class. Given a message-signature pair, one can later obtain a valid signature for every other representative of this class without having access to the secret key. This is done by multiplying each component of the message vector with the same scalar and consistently updating the corresponding signature. Unforgeability for an SPS-EQ-$\mathcal{R}$ scheme is then defined with respect to equivalence classes, that is, after querying signatures for messages M_i, no adversary should be able to produce a valid signature for a message M^* from a different class than the M_i's. Additionally, it is required that two representatives of the same class with corresponding signatures are unlinkable, a notion called class-hiding.

Below, we restate the syntax and the security properties of structure-preserving signatures on equivalence classes from [HS14]. We strengthen their definition of class-hiding by letting the adversary sign

a message and requiring that he is not able to distinguish a re-randomization of the message-signature pair from a random one. Since we also let the adversary choose the signature key pair, we introduce an additional algorithm $\mathsf{VKey}_{\mathcal{R}}$ that checks whether a key pair is valid.

Definition 5 (Structure-preserving signature scheme for equivalence relation $\mathcal{R}$ (SPS-EQ-$\mathcal{R}$))**.** An SPS-EQ-$\mathcal{R}$ scheme on $(\mathbb{G}_i^*)^\ell$ consists 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 κ outputs a bilinear group BG.

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$ is a probabilistic algorithm, which on input a bilinear group BG and a vector length $\ell > 1$ 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 `true` if σ is valid for M under pk and `false` 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 `true` on success and `false` otherwise.

Definition 6 (Correctness)**.** An SPS-EQ-$\mathcal{R}$ scheme $(\mathsf{BGGen}_{\mathcal{R}}, \mathsf{KeyGen}_{\mathcal{R}}, \mathsf{Sign}_{\mathcal{R}}, \mathsf{ChgRep}_{\mathcal{R}}, \mathsf{Verify}_{\mathcal{R}}, \mathsf{VKey}_{\mathcal{R}})$ on $(\mathbb{G}_i^*)^\ell$ is called *correct* if for all security parameters $\kappa \in \mathbb{N}$, for all $\ell > 1$, all bilinear groups $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$, all messages $M \in (\mathbb{G}_i^*)^\ell$ and all $\mu \in \mathbb{Z}_p^*$ we have:

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

Definition 7 (EUF-CMA)**.** An SPS-EQ-$\mathcal{R}$ scheme $(\mathsf{BGGen}_{\mathcal{R}}, \mathsf{KeyGen}_{\mathcal{R}}, \mathsf{Sign}_{\mathcal{R}}, \mathsf{ChgRep}_{\mathcal{R}}, \mathsf{Verify}_{\mathcal{R}}, \mathsf{VKey}_{\mathcal{R}})$ on $(\mathbb{G}_i^*)^\ell$ is called *existentially unforgeable under adaptively chosen-message attacks*, if for all PPT algorithms $\mathcal{A}$ having access to a signing oracle $\mathcal{O}(\mathsf{sk}, M)$, there is a negligible function $\epsilon(\cdot)$ such that:

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

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

In order to define the second security notion, we subsequently let Q be a list for keeping track of queried messages M and make use of the following oracles:

$\mathcal{O}^{RM}(\ell)$**:** A random-message oracle, which on input a message vector length ℓ picks a message $M \xleftarrow{R} (\mathbb{G}_i^*)^\ell$, appends M to Q and returns it.

$\mathcal{O}^{RoR}(\mathsf{sk}, \mathsf{pk}, b, M, \sigma)$**:** A real-or-random oracle taking input a key pair sk, pk, a bit b, a message M and a signature σ. If $M \notin Q$ or $\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = \mathtt{false}$, it returns $\perp$. On the first valid call, it records (M, σ); if later called on a different message-signature pair, it returns $\perp$. Otherwise, it picks $R \xleftarrow{R} (\mathbb{G}_i^*)^\ell$ and $\mu \xleftarrow{R} \mathbb{Z}_p^*$, sets $(M_0, \sigma_0) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$ and $(M_1, \sigma_1) \leftarrow (R, \mathsf{Sign}_{\mathcal{R}}(R, \mathsf{sk}))$ and returns (M_b, σ_b).

Definition 8 (Class-hiding)**.** An SPS-EQ-$\mathcal{R}$ scheme $(\mathsf{BGGen}_{\mathcal{R}}, \mathsf{KeyGen}_{\mathcal{R}}, \mathsf{Sign}_{\mathcal{R}}, \mathsf{ChgRep}_{\mathcal{R}}, \mathsf{Verify}_{\mathcal{R}}, \mathsf{VKey}_{\mathcal{R}})$ on $(\mathbb{G}_i^*)^\ell$ is called *class-hiding* if for all $\ell > 1$ and PPT adversaries $\mathcal{A}$ with oracle access to $\mathcal{O}^{RM}$ and $\mathcal{O}^{RoR}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l|ll} \mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa),\ b \xleftarrow{R} \{0,1\},\ (\mathsf{state}, \mathsf{sk}, \mathsf{pk}) \leftarrow \mathcal{A}(\mathsf{BG}, \ell), & : & b^* = b \ \wedge \\ \mathcal{O} \leftarrow \{\mathcal{O}^{RM}(\ell), \mathcal{O}^{RoR}(\mathsf{sk}, \mathsf{pk}, b, \cdot, \cdot)\},\ b^* \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{state}, \mathsf{sk}, \mathsf{pk}) & & \mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = \mathtt{true} \end{array}\right] - \frac{1}{2} \leq \epsilon(\kappa)\ .$$

4 An EUF-CMA Secure SPS-EQ-$\mathcal{R}$ Construction

In Scheme 1 we present our new SPS-EQ-$\mathcal{R}$ construction with message space $(\mathbb{G}_1^*)^\ell$. Its signatures are comprised of two $\mathbb{G}_1$ elements and one $\mathbb{G}_2$ element and public keys consist of ℓ elements of group $\mathbb{G}_2$. Moreover, verification is defined via only two pairing-product equations. Analogously, one can construct a scheme for message space $(\mathbb{G}_2^*)^\ell$ by swapping the group memberships of all involved elements and adapting all computations accordingly. We first state the security of the signature scheme; the proofs will be given subsequently.

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

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

$\mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$**:** 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 $\mathsf{sk} = (x_i)_{i\in[\ell]}$, choose $y \xleftarrow{R} \mathbb{Z}_p^*$ and output $\sigma = (Z, Y, \hat{Y})$ with

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

$\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk})$**:** Given 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 $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]}$, check whether

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

and if this holds output `true` and `false` otherwise.

$\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$**:** 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 $\mathtt{false} \leftarrow \mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk})$. Otherwise pick $\psi \xleftarrow{R} \mathbb{Z}_p^*$ and return $(\mu \cdot M, \sigma')$ with $\sigma' \leftarrow (\psi\mu Z, \frac{1}{\psi} Y, \frac{1}{\psi} \hat{Y})$.

$\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$**:** Given $\mathsf{sk} = (x_i)_{i\in[\ell]} \in (\mathbb{Z}_p^*)^\ell$ and $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$, output `true` if $x_i\hat{P} \stackrel{?}{=} \hat{X}_i\ \forall i \in [\ell]$ and `false` otherwise.

Scheme 1: An EUF-CMA Secure Construction of an SPS-EQ-$\mathcal{R}$ Scheme.

Theorem 1. *The SPS-EQ-$\mathcal{R}$ scheme in Scheme 1 is correct.*

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

Theorem 3. *If the DDH assumption holds in $\mathbb{G}_1$ then Scheme 1 is class-hiding.*

4.1 Proof of Theorem 1 (Correctness)

We have to show that for all $\kappa \in \mathbb{N}$, all $\ell > 1$, all bilinear groups $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, key pairs $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$, all $M \in (\mathbb{G}_1^*)^\ell$ and all $\mu \in \mathbb{Z}_p^*$ the following holds (where for a probabilistic algorithm A we denote running A on input x with randomness r by $\mathsf{A}(\mathsf{x}; r)$):

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

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$ returns $\mathsf{sk} \leftarrow (x_i)_{i\in[\ell]} \xleftarrow{R} (\mathbb{Z}_p^*)^\ell$ 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

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

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 $\mathsf{Sign}_{\mathcal{R}}$. □

4.2 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 incident is negligible.

The values chosen by the challenger in the unforgeability game, which are unknown to the adversary, are $x_1, \ldots, x_\ell$ 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

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

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,

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

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:

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

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:

$$\sum_{i\in[\ell]} m_i^* x_i = z^* \hat{y}^* \tag{1}$$

$$y^* = \hat{y}^* \tag{2}$$

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*

$$\frac{1}{y_s^b} \prod_{k\in[t]} y_{j_k} \prod_{k\in[t]} x_{i_k} \tag{3}$$

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.

<u>$n = 1$:</u> 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

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

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 (3). Since

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

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

$$z_{n+1} = \sum_{i\in[\ell]} \pi_{m,n+1,i}\, y_{n+1} x_i + \sum_{i\in[\ell]} \sum_{k\in[n]} \rho_{m,n+1,i,k}\, y_{n+1} z_k x_i + \sum_{i\in[\ell]} \sum_{k\in[n]} \psi_{m,n+1,i,k}\, y_{n+1} \frac{1}{y_k} x_i \ . \quad (4)$$

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 $t \le n$, $j_t = k$ 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 (4) of the form $\frac{1}{y_s^b} \big(y_{n+1} \prod_{p\in[t]} y_{j_p}\big)\big(x_i \prod_{p\in[t]} x_{i_p}\big) = \frac{1}{y_s^b} \prod_{p\in[t']} y_{j_p} \prod_{p\in[t']} x_{i_p}$, with $t' \coloneqq t+1 \le n+1$, $j_{t'} \coloneqq n+1$, $i_{t+1} \coloneqq i$. Moreover $t' \le n+1$, all j_p are still different and $\le n$ 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 $j \le n$, meaning y_{i^*} does not occur in z_n; a contradiction. □

We start by investigating Equation (2):

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

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

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 (1) (where in $\hat{y}^*$ we replace $\pi_{\hat{y}}, \chi_{\hat{y},i}$ and $\psi_{\hat{y},j}$ as per (i), (iii) and (iv), 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 (vi)–(viii), we have simplified Equation (1) to the following:

$$\sum_{i \in [\ell]} \Big(\pi_{m^*,i} + \sum_{j \in [q]} \rho_{m^*,i,j} z_j + \sum_{j \in [q]} \psi_{m^*,i,j} \frac{1}{y_j} \Big) x_i \;=\; \sum_{j \in [q]} \rho_{z,j} \pi_y \, z_j + \sum_{j \in [q]} \sum_{k \in [q]} \rho_{z,j} \psi_{y,k} \, \frac{1}{y_k} z_j \;. \tag{5}$$

Let us analyze the monomials contained in the z_j's. By (3) 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 (3) only occur on the RHS of (5).

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 (3)). 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 (1) has now the following, simplified representation:

$$\sum_{i \in [\ell]} \Big(\pi_{m^*,i} + \sum_{j \in [q]} \rho_{m^*,i,j} z_j + \sum_{j \in [q]} \psi_{m^*,i,j} \frac{1}{y_j} \Big) x_i = \sum_{j \in [q]} \sum_{k \in [q]} \rho_{z,j} \psi_{y,k} \, \frac{1}{y_k} z_j \tag{6}$$

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

Applying this to $C \coloneqq (\rho_{z,j})_{j\in[q]} \cdot (\psi_{y,k})_{k\in[q]}^\top$, which by (xiv) and (xv) 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 (xiv) and (xvi), Equation (1) 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, $z_j x_i$ and $\frac{1}{y_j} x_i$, for all $i \in [\ell], j \in [q]$, do not have common monomials, equating coefficients yields (with $\alpha \coloneqq \rho_{z,n}\psi_{y,n}$):

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

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 for an adversary to produce an existential forgery by "incident", 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. □

4.3 Proof of Theorem 3 (Class-Hiding)

Let us define $\mathsf{Game}_{\mathsf{real}}$ as the experiment in Definition 8 with b set to 0, that is, where the real-or-random oracle $\mathcal{O}^{RoR}$ returns randomizations of messages-signature pairs, and let $\mathsf{Game}_{\mathsf{random}}$ be the game where $\mathcal{O}^{RoR}$ returns fresh random pairs (i.e. when $b = 1$). More precisely, in $\mathsf{Game}_{\mathsf{real}}$ when $\mathcal{O}^{RoR}$ receives $(M_i)_{i\in[\ell]}$ from Q (that is, (M_i) was previously drawn by $\mathcal{O}^{RM}$) and a valid signature σ on it, it picks $\mu \xleftarrow{R} \mathbb{Z}_p^*$ and returns $\mathsf{ChgRep}_{\mathcal{R}}\big((M_i)_{i\in[\ell]}, \sigma, \mu, \mathsf{pk}\big)$. In $\mathsf{Game}_{\mathsf{random}}$, when queried on a message in Q, the $\mathcal{O}^{RoR}$ oracle

returns $(R_i)_{i\in[\ell]} \xleftarrow{R} (\mathbb{G}_1^*)^\ell$ together with $\sigma \leftarrow \mathsf{Sign}_{\mathcal{R}}((R_i)_{i\in[\ell]}, \mathsf{sk})$. In order to prove class-hiding, we must show that under the DDH assumption $\mathsf{Game}_{\mathsf{real}}$ and $\mathsf{Game}_{\mathsf{random}}$ are indistinguishable.

We first define a game $\mathsf{Game}'_{\mathsf{real}}$ in which the $\mathcal{O}^{RoR}$ oracle, on input $M \in Q$ and a valid signature on M, returns $(\mu M, \mathsf{Sign}_{\mathcal{R}}(\mu M, \mathsf{sk}))$, for $\mu \xleftarrow{R} \mathbb{Z}_p^*$, and show that $\mathsf{Game}'_{\mathsf{real}}$ is distributed equivalently to $\mathsf{Game}_{\mathsf{real}}$. Let $\mathsf{sk} = (x_i)_{i\in[\ell]}$, $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]}$ be the adversary's output in the first phase. If $\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = \mathtt{true}$ then

$$\hat{X}_i = x_i \hat{P} \quad \forall\, i \in [\ell] \ . \tag{7}$$

Let $\big((M_i)_{i\in[\ell]}, \sigma = (Z, Y, \hat{Y})\big)$ be the adversary's first valid input to $\mathcal{O}^{RoR}$. If $\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = \mathtt{true}$ then

$$\textstyle\prod_{i\in[\ell]} e(M_i, \hat{X}_i) = e(Z, \hat{Y}) \tag{8}$$

$$e(Y, \hat{P}) = e(P, \hat{Y}) \tag{9}$$

and $Y \neq 0_{\mathbb{G}_1}, \hat{Y} \neq 0_{\mathbb{G}_2}$. By this and (9) there exists some $\varphi \in \mathbb{Z}_p^*$ such that $Y = \varphi P$ and $\hat{Y} = \varphi \hat{P}$; we let $y \coloneqq \frac{1}{\varphi}$. By (7), the LHS of (8) equals $e(\sum_{i\in[\ell]} x_i M_i, \hat{P})$; moreover, the RHS equals $e(\frac{1}{y} Z, \hat{P})$. Thus, $Z = y \sum_{i\in[\ell]} x_i M_i$, and $\sigma = \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk};\, y)$.

$\mathsf{ChgRep}_{\mathcal{R}}$, according to its definition, applied to $(M, \sigma, \mu, \mathsf{pk})$ returns $(\mu M, \sigma')$, where σ' is a signature on μM with randomness ψy (where ψ is chosen uniformly from $\mathbb{Z}_p^*$ by $\mathsf{ChgRep}_{\mathcal{R}}$). The output signature σ' is thus distributed equivalently to a freshly generated signature on μM; meaning that $\mathsf{Game}_{\mathsf{real}}$ and $\mathsf{Game}'_{\mathsf{real}}$ are distributed equivalently.

We next define a game Game_j, for all $j \in [\ell]$, where the $\mathcal{O}^{RoR}$ oracle, when queried on $(M_1, \ldots, M_\ell) \in Q$, chooses $\mu \xleftarrow{R} \mathbb{Z}_p^*$ and $R_{j+1}, \ldots, R_\ell \xleftarrow{R} \mathbb{G}_1^*$ and returns

$$\big(M' \coloneqq (\mu M_1, \ldots, \mu M_j, R_{j+1}, \ldots, R_\ell),\ \mathsf{Sign}_{\mathcal{R}}(M', \mathsf{sk})\big) \ .$$

Note that by definition $\mathsf{Game}_1 = \mathsf{Game}_{\mathsf{random}}$ and $\mathsf{Game}_\ell = \mathsf{Game}'_{\mathsf{real}}$ ($\approx \mathsf{Game}_{\mathsf{real}}$).

Thus, if there exists an adversary that distinguishes $\mathsf{Game}_{\mathsf{real}}$ from $\mathsf{Game}_{\mathsf{random}}$ with probability $\epsilon(\kappa)$ then there must exist an index $j \in [\ell]$ such that the adversary 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 from a distinguisher between Game_{j-1} and Game_j.

Given a DDH instance (P, aP, bP, cP), we simulate the following game for the adversary. For $k = 1, \ldots$, at the k-th call the $\mathcal{O}^{RM}$ oracle samples $m_{k,i} \xleftarrow{R} \mathbb{Z}_p^*$, for all $i \in [\ell]$, appends

$$\big(m_{k,1}P, \ldots, m_{k,j-1}P, m_{k,j}(aP), m_{k,j+1}P, \ldots, m_{k,\ell}P\big) \tag{10}$$

to Q and returns it. The $\mathcal{O}^{RoR}$ oracle, on input the k-th message in Q, samples $R_{j+1}, \ldots, R_\ell \xleftarrow{R} \mathbb{G}_1^*$ and returns

$$M' = \big(m_{k,1}(bP), \ldots, m_{k,j-1}(bP), m_{k,j}(cP), R_{j+1}, \ldots, R_\ell\big) \tag{11}$$

and $\sigma \leftarrow \mathsf{Sign}_{\mathcal{R}}(M', \mathsf{sk})$. If (P, aP, bP, cP) is a real DDH instance (i.e. $c = ab$) then the first j elements in (11) are b-multiples of the first j elements in (10), and we have thus simulated Game_j. If c is random then so is the j-th element in (11) and we have simulated Game_{j-1}. Any adversary distinguishing Game_{j-1} from Game_j thus breaks the DDH assumption. □

Acknowledgments

The work of the first author has been supported by the European Research Council, ERC Starting Grant (259668-PSPC). The work of the last two authors has been supported by the European Commission through project FP7-FutureID, grant agreement number 318424.

References

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-Preserving Signatures and Commitments to Group Elements. In *CRYPTO*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.

[BGdMM05] Lucas Ballard, Matthew Green, Breno de Medeiros, and Fabian Monrose. Correlation-Resistant Storage via Keyword-Searchable Encryption. IACR Cryptology ePrint Archive, 2005. `http://eprint.iacr.org/`.

[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.

[Fuc14] Georg Fuchsbauer. Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014. Cryptology ePrint Archive, Report 2014/892, 2014. `http://eprint.iacr.org/`.

[HS14] Christian Hanser and Daniel Slamanig. Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials. In *ASIACRYPT*, 2014. `http://eprint.iacr.org/2014/705`.