Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups

Masayuki Abe[1], Jens Groth[2⋆], Kristiyan Haralambiev[3], and Miyako Ohkubo[4]

[1] Information Sharing Platform Laboratories, NTT Corporation, Japan
abe.masyuki@lab.ntt.co.jp
[2] University College London, UK
j.groth@ucl.ac.uk
[3] Computer Science Department, New York University, US
kkh@cs.nyu.edu
[4] National Institute of Information and Communications Technology, Japan
m.ohkubo@nict.go.jp

Abstract. Structure-preserving signatures are signatures defined over bilinear groups that rely on generic group operations. In particular, the messages and signatures consist of group elements and the verification of signatures consists of evaluating pairing product equations. Due to their purist nature structure-preserving signatures blend well with other pairing-based protocols.
We show that structure-preserving signatures must consist of at least 3 group elements when the signer uses generic group operations. Usually, the generic group model is used to rule out classes of attacks by an adversary trying to break a cryptographic assumption. In contrast, here we use the generic group model to prove a lower bound on the complexity of digital signature schemes.
We also give constructions of structure-preserving signatures that consist of 3 group elements only. This improves significantly on previous structure-preserving signatures that used 7 group elements and matches our lower bound. Our structure-preserving signatures have additional nice properties such as strong existential unforgeability and can sign multiple group elements at once.

Keywords: Structure-Preservation, Digital Signatures, Generic Group Model.

1 Introduction

Digital signatures are fundamental cryptographic primitives used as building blocks in countless scenarios. Often, signatures are combined with zero-knowledge (ZK) proof systems, for example when constructing privacy-preserving cryptographic protocols. While suitable signature schemes for such cases have long been known, e.g., the schemes of Camenisch and Lysyanskaya [CL02,CL04], they were constructed with the intent to be used with interactive ZK proofs. The reason was the absence of an efficient non-interactive zero-knowledge (NIZK) proof system. Moreover, the only way to construct efficient NIZK proofs was using certain heuristics, e.g., random oracles, which transform interactive ZK proofs into NIZK proofs. In [GS08], Groth and Sahai presented

⋆ Supported by EPSRC grant number EP/G013829/1.

the first practical NIZK proof system for a non-trivial class of languages which does not resort to such heuristics. It is based on bilinear maps and is designed to be used on certain satisfiable systems of equations. The most interesting type of equation is the so-called "pairing-product equation" for which the proofs are also fully extractable, and therefore the proof system yields NIZK proofs of knowledge.

As pointed out in [AFG+10], many previous signatures scheme were not fully "compatible" with pairing-product equations. Even if the verification algorithm used pairing-product equations, the signatures and messages were not composed entirely of group elements and thus were not ideal counterparts for the pairing product equations of Groth-Sahai proofs. That is why [AFG+10] defined the notion of structure-preserving signatures which requires verification keys, messages, and signatures to be composed entirely of group elements and the verification equations to use pairing-product equations. Equipped with such signatures, one can easily design modular cryptographic protocols which rely on signatures and NIZK proofs and instantiate them efficiently. Of course some cryptographic protocols find other ingenious efficient solutions but these are specific to their tasks. In contrast, modular design makes constructions easier to build, less prone to errors, and provide a good alternative for efficiency comparisons. Moreover, modular constructions can be realized under different assumptions by choosing appropriate instantiations of the building blocks. Applications of structure-preserving signatures combined with Groth-Sahai proofs are numerous: group signatures, blind signatures, delegatable credentials, oblivious transfer, credential-based identification/key-exchange with hierarchical certification, etc.

Efficient structure-preserving signatures were presented in [AFG+10] and were applied to the construction of round-optimal blind signatures and fully-secure group signatures with concurrent join protocols. Although they were efficient, it was left as an open problem to find the optimal signature size and determine whether more efficient schemes can be constructed. These are the problems we consider in this work.

1.1 Our contribution

Results. We prove lower bounds on the complexity of structure-preserving signatures based on asymmetric bilinear groups. As far as we are aware, this is the first non-trivial lower bound for the complexity of practical signature schemes. We also construct a structure-preserving signature scheme that matches the lower bounds giving an optimal solution in terms of efficiency.

We demonstrate that a structure-preserving signature scheme must use at least two pairing product equations to verify a signature. Any structure-preserving signature scheme where the verification only uses one pairing product equation can be broken with a random message attack.

We also give a lower bound on the size of a signature. A structure-preserving signature with less than 3 group elements is vulnerable to a random message attack. The lower bound holds even when the message is a single group element.

Finally, we prove that the lower bounds are optimal by presenting a structure-preserving signature scheme where the verification of signatures uses only two verification equations and the signatures consist of only 3 group elements.

Our signature scheme has several nice properties. First, it is structure preserving. Second, it is strongly existentially unforgeable against adaptive chosen message attacks. Third, messages to be signed can consist of many group elements, which can be drawn from both of the base groups of the bilinear map.

The existential unforgeability of our signature scheme against adaptive chosen message attacks corresponds to an interactive cryptographic assumption, which we prove is true when the adversary only uses generic group operations. By adding a few extra group elements to the signatures (1 or 3 depending on whether the messages only contain elements in one base group or contains a mix of elements from both base groups) we can base security on a non-interactive cryptographic assumption.

Techniques. The lower bound on the number of pairing product equations needed in the verification process follows from a demonstration that any two signatures on two different random messages can be combined to yield signatures on different messages.

However, when there are two or more verification equations, the analysis of the number of group elements involved in a signature becomes intricate. We base our analysis on the signer being a generic algorithm. This differs from the standard use of the generic group model to rule out classes of attacks on cryptographic assumptions since the analysis is based on what the signing algorithm can do, not what some arbitrary unknown adversary can do. Arguably this is a more compelling way to use the generic group model since the analysis only fails for signature schemes where the designer invents a non-generic signing algorithm.

A generic signer must create signatures that are related to the messages in a specific way. Furthermore, the correctness of the signature scheme implies that signatures created this way must be valid signatures. With these two facts in mind, we analyze the pairing product equations in the verification and show that all pairing product equations must be linearly related if the signatures consist of 1 or 2 group elements. We conclude that they can be replaced by an equivalent single verification equation. But that would make the signature scheme vulnerable to a random message attack.

Our work on lower bounds on structure-preserving signatures gives insight into what a structure-preserving signature with more group elements should look like. The verification equations must be organized such that a generic signer can use the secret signing key to solve them for arbitrary messages. A random choice of 2 or more verification equations is unlikely to be solvable for a generic signing algorithm. With signature sizes of 3 or more group elements, however, it is possible to carefully select the verification equations such that they are solvable by a generic signer. We find such a set of verification equations that are solvable by a generic signer and at the same time resists generic attackers with access to an adaptive chosen message attack.

1.2 Related work

Lower bounds for cryptographic protocols have been studied extensively. For some tasks it is possible to give information-theoretic lower bounds; ciphertexts must, for instance, be longer than plaintexts to enable correct decryption. In the context of zero-knowledge proofs lower bounds on the round complexity [GO94] have been found by exploiting the tension between soundness and zero-knowledge. However, these lower

bounds do not readily apply to digital signatures where the hash-and-sign paradigm rules out strong information-theoretic bounds on the size and the protocols are non-interactive by definition. Gennaro, Gertner and Katz [GGK03] instead investigated the complexity of digital signatures that only make black-box calls to a one-way permutation and found asymptotic lower bounds on the number of black-box queries. In contrast, our lower bounds apply to practical pairing-based signature schemes.

The generic group model [Nec94,Sho97] is widely used in pairing-based cryptography to rule out generic attacks on cryptographic assumptions. However, there has been little work on using the generic group model to prove lower bounds on the efficiency of cryptographic protocols except for Bangerter, Camenisch and Krenn [BCK10] that gave lower bounds on the knowledge error in certain Sigma-protocols and Ostrovsky and Skeith [OS08] that gave lower bounds on single-server private information retrieval protocols based on homomorphic encryption. The generic group model has not been used to give lower bounds for the complexity of signature schemes.

The first structure-preserving signatures were presented by Groth [Gro06] who used them to build group signatures. Groth's signature scheme is based on the decision linear assumption but consists of thousands of group elements and is therefore not practical.

Green and Hohenberger [GH08] presented a structure-preserving signature scheme that provides security against random-message attacks, which they used to build a universally composable adaptive oblivious transfer protocol.

Cathalo, Libert and Yung [CLY09] constructed a partially structure-preserving signature scheme which signs only a single group element and used it for the construction of a group-encryption scheme.

Fuchsbauer [Fuc09] presented a structure-preserving signature scheme for signing messages that are Diffie-Hellman pairs. Fuchsbauer's scheme is automorphic, i.e., the public verification keys belong to the message space. Automorphic signatures have several applications including blind signatures, group signatures, anonymous proxy signatures and anonymous delegatable credentials [Fuc09,FV10,Fuc11].

Abe, Haralambiev and Ohkubo [AHO10] presented several constructions of structure-preserving signatures and found applications to blind signatures and group signatures. A merged version of [Fuc09,AHO10,Gro09] first coined the term structure-preserving signatures. The most efficient structure-preserving signature scheme from [AFG$^+$10] can sign multiple group elements belonging to one of the base groups with signatures that consist of 7 group elements and use two pairing product equations in the verification. In comparison, we present a scheme that can sign messages that contain group elements from both base groups and only uses 3 group elements in the signatures.

2 Preliminaries

2.1 Bilinear groups

Throughout the paper we let $\mathcal{G}$ be a bilinear group generator that on security parameter k returns $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H) \leftarrow \mathcal{G}(1^k)$ with the following properties:

- $\mathbb{G}, \mathbb{H}, \mathbb{T}$ are groups of prime order p.

– $e : \mathbb{G} \times \mathbb{H} \to \mathbb{T}$ is a bilinear map such that $\forall U \in \mathbb{G}, \forall V \in \mathbb{H}, \forall a, b \in \mathbb{Z} : e(U^a, V^b) = e(U, V)^{ab}$.
– G generates $\mathbb{G}$, H generates $\mathbb{H}$ and $e(G, H)$ generates $\mathbb{T}$.
– There are efficient algorithms for computing group operations, evaluating the bilinear map, comparing group elements and deciding membership of the groups.

There are many ways to set up bilinear groups. We will work in what Galbraith, Paterson and Smart [GPS08] call type III groups, where there are no efficiently computable isomorphisms $\mathbb{G} \to \mathbb{H}$ or $\mathbb{H} \to \mathbb{G}$. We focus on type III groups here because they have the most efficient instantiations and therefore the highest relevance for cryptographic purposes.

In a group $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$ generated by $\mathcal{G}$ we refer to deciding group membership, computing group operations in $\mathbb{G}, \mathbb{H}$ or $\mathbb{T}$, comparing group elements and evaluating the bilinear map as the generic group operations. In the signature schemes we construct we only use generic group operations.

As a matter of notation, we will mostly use capital letters A, G, M, R, S, U for group elements in $\mathbb{G}$ and capital letters B, H, N, T, V, W for group elements in $\mathbb{H}$ and capital letter Z for group elements in $\mathbb{T}$. We will use small letters $r, s, t, \ldots$ for discrete logarithms of group elements with respect to base G or base H. We use Greek letters $\alpha, \beta, \ldots$ for hidden field elements in $\mathbb{Z}_p$ chosen by algorithms as part of their operation.

2.2 Secure signature schemes

A digital signature scheme over groups generated by a bilinear group generator $\mathcal{G}$ is a triple of efficient algorithms $(\mathcal{K}, \mathcal{S}, \mathcal{V})$. The key generation algorithm $\mathcal{K}$ takes a description of the bilinear group as input and returns a public verification key VK and a secret signing key SK. The signing algorithm $\mathcal{S}$ takes a signing key SK and a message M in the message space $\mathcal{M}$ defined by GK and VK as input and returns a signature Σ. The verification algorithm $\mathcal{V}$ takes the verification key VK, a message M and the signature Σ and returns either 1 (accept) or 0 (reject).

Definition 1 (Correctness). *We say the signature scheme $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ over bilinear group generator $\mathcal{G}$ is (perfectly) correct if for all security parameters $k \in \mathbb{N}$*

$$\Pr[GK \leftarrow \mathcal{G}(1^k); (VK, SK) \leftarrow \mathcal{K}(GK); M \leftarrow \mathcal{M}; \Sigma \leftarrow \mathcal{S}_{SK}(M) : \mathcal{V}_{VK}(M, \Sigma) = 1] = 1.$$

A signature scheme is said to be existentially unforgeable if it is hard to forge a signature on a new message that has not been signed before. The adversary may see signatures on other messages before making the forgery. We distinguish between a random message attack, where the adversary gets pairs of random messages and corresponding signatures, and an adaptive chosen message attack where the adversary can choose arbitrary messages and receive signatures on them. Our signatures will be secure against adaptive chosen message attack, but our lower bounds on the complexity of signature schemes will hold even for the weaker random message attacks. We now formally define existential unforgeability against an adaptive chosen message attacks.

Definition 2 (EUF-CMA). *A signature scheme $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ over bilinear group generator $\mathcal{G}$ is existentially unforgeable against adaptive chosen message attacks if for all*

non-uniform polynomial time $\mathcal{A}$

$$\Pr[GK \leftarrow \mathcal{G}(1^k); (VK, SK) \leftarrow \mathcal{K}(GK); (M, \Sigma) \leftarrow \mathcal{A}^{\mathcal{S}_{SK}(\cdot)}(VK) : M \notin Q \ \wedge \ \mathcal{V}_{VK}(M, \Sigma) = 1] = \mathrm{negl}(k),$$

where Q *is the set of queries made by* $\mathcal{A}$ *to the signing oracle.*

Sometimes it is also useful to prevent the adversary from issuing a new signature for a message that has already been signed. A signature scheme is strongly existentially unforgeable if it is hard to find a signature on a message that has not been signed before and also hard to find a new signature for a message that has already been signed.

Definition 3 (sEUF-CMA). *A signature scheme* $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ *over bilinear group generator* $\mathcal{G}$ *is strongly existentially unforgeable against adaptive chosen message attacks if for all non-uniform polynomial time* $\mathcal{A}$

$$\Pr[GK \leftarrow \mathcal{G}(1^k); (VK, SK) \leftarrow \mathcal{K}(GK); (M, \Sigma) \leftarrow \mathcal{A}^{\mathcal{S}_{SK}(\cdot)}(VK) : (M, \Sigma) \notin Q \ \wedge \ \mathcal{V}_{VK}(M, \Sigma) = 1] = \mathrm{negl}(k),$$

where Q *is the set of message-signature pairs from* $\mathcal{A}$*'s queries to the signing oracle.*

2.3 Structure-preserving signature schemes

In this paper, we study structure-preserving signature schemes [AFG+10]. In a structure preserving signature scheme the verification key, the messages and the signatures consist only of group elements and the verification algorithm evaluates the signature by deciding group membership of elements in the signature and by evaluating pairing product equations, which are equations of the form

$$\prod_i \prod_j e(A_i, B_j)^{a_{ij}} = Z,$$

where $A_1, A_2, \ldots \in \mathbb{G}, B_1, B_2, \ldots \in \mathbb{H}, Z \in \mathbb{T}$ are group elements appearing in GK, VK, M or Σ and $a_{11}, a_{12}, \ldots \in \mathbb{Z}$ are constants. Structure-preserving signatures are extremely versatile because they mix well with other pairing-based protocols. Groth-Sahai proofs [GS08] are for instance designed with pairing product equations in mind and can therefore easily be applied to structure-preserving signatures.

Definition 4 (Structure-preserving signatures). *A signature scheme* $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ *over bilinear group generator* $\mathcal{G}$ *is said to be structure preserving if*

- $\mathcal{G}$ *generates a bilinear group* $GK = (p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$*,*
- *the verification key consists of* GK *and group elements in* $\mathbb{G}$ *and* $\mathbb{H}$*,*
- *the messages consist of group elements in* $\mathbb{G}$ *and* $\mathbb{H}$*,*
- *the signatures consist of group elements in* $\mathbb{G}$ *and* $\mathbb{H}$*, and*
- *the verification algorithm evaluates membership in* $\mathbb{G}$ *and* $\mathbb{H}$ *and pairing product equations with* $Z = 1$*.*

Our signatures are structure-preserving as defined above. When proving our lower bounds, we will relax the definition of structure-preserving signatures to allow arbitrary target group elements $Z \in \mathbb{T}$ to be included in the verification key and to appear in the verification equations. This strengthens our results, getting lower bounds in a relaxed model of structure-preserving signatures and constructing signatures in a strict model of structure-preserving signatures.

Generic signer. Abe et al. [AFG+10] did not explicitly require the signing algorithm to only use generic group operations when they defined structure-preserving signatures. However, it would be a natural addition to the definition of structure-preserving signatures because otherwise the cryptographic designer would have to invent some non-generic operations to be used in the signature scheme and that would be a surprising result in itself. All our signature schemes have a generic signer; as do all earlier structure-preserving signatures in the literature.

3 Lower bounds on structure-preserving signatures

In this section, we will prove lower bounds on the complexity of structure-preserving signatures. We summarize our lower bounds in the following main theorem, which follows from Theorems 2, 3 and 4.

Theorem 1. *All generic-signer structure-preserving signature schemes that are existentially unforgeable against random message attacks must use at least two verification equations and have signatures consisting of at least three group elements drawn from both $\mathbb{G}$ and $\mathbb{H}$. This holds even when the messages are single group elements and even if we allow the verification key to contain elements of $\mathbb{T}$.*

3.1 Impossibility of one verification equation

Theorem 2. *There is no structure-preserving signature with a single verification equation that is existentially unforgeable against random message attacks.*

Proof. Consider a structure preserving signature scheme for messages $M \in \mathbb{G}$ with the verification key containing group elements $U_1, U_2, \ldots \in \mathbb{G}, V_1, V_2, \ldots \in \mathbb{H}, Z \in \mathbb{T}$. Signatures are of the form $(S_1, S_2, \ldots, T_1, T_2, \ldots)$ with $S_i \in \mathbb{G}$ and $T_j \in \mathbb{H}$ and are verified by the following verification equation

$$\prod_i \prod_j e(S_i, T_j)^{a_{ij}} \cdot \prod_i \prod_j e(S_i, V_j)^{b_{ij}} \cdot \prod_j e(M, T_j)^{c_j} \cdot \prod_j e(M, V_j)^{d_j} \cdot \prod_i \prod_j e(U_i, T_j)^{e_{ij}} = Z.$$

Please note there is no need for terms of the form $e(U_i, V_j)$ because without loss of generality they can be incorporated into $Z \in \mathbb{T}$.

Suppose we get a signature $(S_1, \ldots, T_1, \ldots)$ on a random message $M \in \mathbb{G}$. Isolating T_ℓ and M in the verification, define for every ℓ

$$A_\ell = \prod_i S_i^{a_{i\ell}} \cdot \prod_i U_i^{e_{i\ell}} \qquad B_\ell = \prod_{j \neq \ell} T_j^{c_j} \cdot \prod_j V_j^{d_j}.$$

Suppose there is an ℓ for which $A_\ell \neq M^{-c_\ell}$. We can rewrite the verification equation

$$e(M,T_\ell)^{c_\ell} e(A_\ell,T_\ell) e(M,B_\ell) \cdot \prod_i \prod_{j\neq\ell} e(S_i,T_j)^{a_{ij}} \cdot \prod_i \prod_j e(S_i,V_j)^{b_{ij}} \cdot \prod_i \prod_{j\neq\ell} e(U_i,T_j)^{e_{ij}} = Z.$$

If $c_\ell = 0$ then setting $T'_\ell = T_\ell B_\ell^{-1}$ while keeping the rest of the signature intact gives us a forged signature on $M' = MA_\ell$, where $A_\ell \neq M^{-c_\ell} = M^0 = 1$. If $c_\ell \neq 0$ then setting $T'_\ell = T_\ell^{-1} B_\ell^{-\frac{2}{c_\ell}}$ while keeping the rest of the signature intact gives us a forged signature on $M' = M^{-1} A_\ell^{-\frac{2}{c_\ell}} \neq M$, where the inequality follows from $A_\ell \neq M^{-c_\ell}$. To avoid forged signatures must therefore, with overwhelming probability, have $A_\ell = M^{-c_\ell}$ for all ℓ.

If there is overwhelming probability that $A_\ell M^{c_\ell} = 1$ for all ℓ, then each T_ℓ is cancelled out in the verification. We can therefore without loss of generality ignore $T_1, T_2, \ldots$ and look at the case where signatures are of the form $(S_1, S_2, \ldots)$ with $S_i \in \mathbb{G}$ and the verification equation is of the form

$$\prod_i \prod_j e(S_i,V_j)^{b_{ij}} \cdot \prod_j e(M,V_j)^{d_j} = Z.$$

Obtaining two signatures $(S_1, S_2, \ldots)$ and $(S'_1, S'_2, \ldots)$ on two random messages M and M' gives us a signature $(S_1^2/S'_1, S_2^2/S'_2, \ldots)$ on M^2/M'. With overwhelming probability $M^2/M' \notin \{M, M'\}$ and we have a forgery. □

3.2 Impossibility of unilateral signatures

Let us call a signature unilateral if it only contains group elements in $\mathbb{G}$ or only contains group elements in $\mathbb{H}$. In other words, a unilateral signature is either of the form $(S_1, S_2, \ldots)$ with $S_i \in \mathbb{G}$ or of the form $(T_1, T_2, \ldots)$ with $T_i \in \mathbb{H}$.

Theorem 3. *There is no unilateral generic-signer structure-preserving signature scheme that is existentially unforgeable against random message attacks.*

Proof. Let us without loss of generality look at a signature scheme for single group element messages $M \in \mathbb{G}$. The verification key contains group elements $U_1, U_2, \ldots \in \mathbb{G}, V_1, V_2, \ldots \in \mathbb{H}, Z_1, Z_2, \ldots \in \mathbb{T}$.

We first look at the case, where signatures are of the form $(S_1, S_2, \ldots)$ with $S_i \in \mathbb{G}$ and fit a number of verification equations of the form

$$\prod_i \prod_j e(S_i,V_j)^{b_{qij}} \cdot \prod_j e(M,V_j)^{d_{qj}} = Z_q.$$

Given two signatures $(S_1, \ldots)$ and $(S'_1, \ldots)$ on random messages M and M' we see that $(S_1^2/S'_1, \ldots)$ is a signature on M^2/M'. There is negligible probability of $M^2/M' \in \{M, M'\}$ so this gives us an existential forgery.

Next, consider the case where signatures are of the form $(T_1, T_2, \ldots)$ with $T_j \in \mathbb{H}$ and satisfy verification equations of the form

$$\prod_j e(M,T_j)^{c_{qj}} \cdot \prod_j e(M,V_j)^{d_{qj}} \cdot \prod_i \prod_j e(U_i,T_j)^{e_{qij}} = Z_q.$$

A generic signer chooses $(T_1, \ldots)$ independently of M because they belong to different groups. Generating the signature independently of M combined with correctness of the signature scheme means that the resulting signature must be valid for all messages M so it is trivial to find a selective forgery after a one-time random message attack. $\square$

3.3 Impossibility of signatures with 2 group elements

Theorem 4. *No generic-signer structure-preserving signature scheme with signatures having two group elements is existentially unforgeable against random message attacks.*

Proof. Theorem 3 ruled out the existence of unilateral generic-signer structure-preserving signatures. The remaining question is therefore, whether we can have signatures of the form (S, T) with $S \in \mathbb{G}$ and $T \in \mathbb{H}$. Suppose without loss of generality that we have a generic-signer structure-preserving signature scheme for messages $M \in \mathbb{G}$. The public verification key contains $U_1, \ldots \in \mathbb{G}, V_1, \ldots \in \mathbb{H}, Z_1, \ldots \in \mathbb{T}$ and a signature (S, T) on M satisfies a number of verification equations of the form

$$e(S,T)^{a_q} \cdot \prod_j e(S,V_j)^{b_{qj}} \cdot e(M,T)^{c_q} \cdot \prod_j e(M,V_j)^{d_{qj}} \cdot \prod_i e(U_i,T)^{e_{qi}} = Z_q.$$

Without loss of generality we may assume that the signer knows the discrete logarithms of all the elements in the public verification key. Using generic group operations it can only construct $S = M^\alpha G^\beta$ and $T = H^\tau$, where α, β, τ may be correlated to each other and the public verification key but are independent of M. Taking discrete logarithms of the verification equations, we get equations of the form

$$(\alpha m + \beta)\tau a_q + (\alpha m + \beta) \sum_j v_j b_{qj} + m\tau c_q + m \sum_j v_j d_{qj} + \tau \sum_i u_i e_{qi} = z_q.$$

The correctness of the signature scheme means that these equations are satisfied for any choice of m. Defining $b_q = \sum_j v_j b_{qj}, d_q = \sum_j v_j d_{qj}, e_q = \sum_i u_i e_{qi}$ this means that the choice of α, β and τ must satisfy pairs of equations of the form

$$a_q\alpha\tau + b_q\alpha + c_q\tau + d_q = 0 \qquad a_q\beta\tau + b_q\beta + e_q\tau = z_q.$$

By taking suitable non-trivial linear combinations of two such pairs of equations, say equation q_1 and q_2, we can eliminate the $\alpha\tau$ and $\beta\tau$ terms to get a pair of equations of the form

$$b\alpha + c\tau + d = 0 \qquad b\beta + e\tau = z.$$

If $b = 0$ and $c \neq 0$ or $b = 0$ and $e \neq 0$ we get a fixed τ and $T = H^\tau$ is uniquely determined. This T can therefore without loss of generality be published as part of the verification key making the signature scheme unilateral. Theorem 3 therefore tells us that if $b = 0$ then $c = 0$ and $e = 0$. This implies $d = 0$ and $z = 0$ as well, and we conclude that the two verification equations q_1 and q_2 are linearly related and one of them can without loss of generality be eliminated from the signature scheme. From Theorem 2 we deduce that there must be at least two verification equations that are not linearly related giving a linear combination with $b \neq 0$.

If $b \neq 0$ we have

$$\alpha = -\frac{c}{b}\tau - \frac{d}{b} \qquad \beta = -\frac{e}{b}\tau + \frac{z}{b}.$$

Plugging them into the verification equations gives us equations of the form

$$-a_q\frac{c}{b}\tau^2+(c_q-a_q\frac{d}{b}-b_q\frac{c}{b})\tau = b_q\frac{d}{b}-d_q \qquad -a_q\frac{e}{b}\tau^2+(e_q+a_q\frac{z}{b}-b_q\frac{e}{b})\tau = -b_q\frac{z}{b}+z_q.$$

If one of the quadratic equations in τ is non-trivial then T can take at most two possible values T_0 or T_1. After obtaining signatures on three random messages, two of them would be using the same T. The adversary would thus have signatures (S, T) and (S', T) on messages M and M' and this would give a signature $(S^2/S', T)$ on M^2/M', which with overwhelming probability gives an existential forgery.

If all the quadratic equations are trivial there are two possibilities. The first possibility is that $a_1 = 0, a_2 = 0, \ldots$ but then

$$c_q = b_q\frac{c}{b} \qquad d_q = b_q\frac{d}{b} \qquad e_q = b_q\frac{e}{b} \qquad z_q = b_q\frac{z}{b}$$

and it can be seen that all the verification equations are linearly related and can be replaced with a single verification equation. Theorem 2 rules out this possibility. The other possibility is that $c = 0$ and $e = 0$. This gives us

$$c_q = a_q\frac{d}{b} \qquad d_q = b_q\frac{d}{b} \qquad e_q = -a_q\frac{z}{b} \qquad z_q = b_q\frac{z}{b} \qquad \alpha = -\frac{d}{b} \qquad \beta = \frac{z}{b}.$$

Plugging $S = M^\alpha G^\beta$ into the verification equations shows the verification equations completely ignore T. With all verification equations ignoring T we are back in the unilateral case that we ruled out in Theorem 3. □

4 Minimal structure-preserving signatures

We will now present a structure-preserving signature scheme that matches the lower bounds we found in Section 3. The signature scheme is strongly existentially unforgeable against adaptive chosen message attacks. We can simultaneously sign tuples of messages in $\mathbb{G}$ and tuples of messages in $\mathbb{H}$. A signature consists of three group elements and is verified using two verification equations.

Let us first discuss the case of signing a pair of group elements $(M, N) \in \mathbb{G} \times \mathbb{H}$. Working over a bilinear group $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$ the verification key is of the form $(U, V, W, Z) \in \mathbb{G} \times \mathbb{H}^3$. A signature on a message $(M, N) \in \mathbb{G} \times \mathbb{H}$ is of the form $(R, S, T) \in \mathbb{G}^2 \times \mathbb{H}$ and is verified by two verification equations

$$e(R, V)e(S, H)e(M, W) = e(G, Z) \qquad e(R, T)e(U, N) = e(G, H).$$

It is instructive to look at the verification equations from a generic signer's perspective in light of the same type of equations we used to prove the lower bounds in

Section 3. Using $R = M^{\alpha}G^{\beta}, S = M^{\gamma}G^{\delta}$ and $T = N^{\epsilon}H^{\eta}$ we get after taking discrete logarithms of the verification equations

$$(\alpha m + \beta)v + (\gamma m + \delta) + mw = z \qquad (\alpha m + \beta)(\epsilon n + \eta) + un = 1.$$

The signer does not know the discrete logarithms of M and N so the verification equations should hold for all choices of m and n. The signer must therefore choose $\alpha, \beta, \gamma, \delta, \epsilon, \eta \in \mathbb{Z}_p$ such that the following equations are satisfied

$$v\alpha + \gamma + w = 0 \qquad \beta v + \delta = z \qquad \alpha\epsilon = 0 \qquad \alpha\eta = 0 \qquad \beta\epsilon + u = 0 \qquad \beta\eta = 1.$$

This gives six constraints on $\alpha, \beta, \gamma, \delta, \epsilon, \eta$. An arbitrary pair of equations could in contrast give eight constraints on the six variables and might not be solvable. Furthermore, if we pick $\alpha = 0$ we are left with only four constrains

$$\gamma = -w \qquad \beta v + \delta = z \qquad \beta\epsilon + u = 0 \qquad \beta\eta = 1$$

on the five variables $\beta, \gamma, \delta, \epsilon, \eta$. This makes it possible to have many different solutions to the equations and avoids R, S or T being constrained to a single fixed value, which would bring us into conflict with the lower bounds from Section 3.

We extend the signature scheme sketched above in a natural way to sign messages in $\mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$. The full signature scheme can be found in Figure 1.

Key generation $\mathcal{K}(GK)$**:** Parse GK as $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$.
Pick at random $u_1, \ldots, u_{k_N}, v, w_1, \ldots, w_{k_M}, z \leftarrow \mathbb{Z}_p^*$ and compute

$$U_i = G^{u_i} \qquad V = H^{v} \qquad W_i = H^{w_i} \qquad Z = H^{z}.$$

Return the verification key $VK = (GK, U_1, \ldots, U_{k_N}, V, W_1, \ldots, W_{k_M}, Z)$ and the signing key $SK = (VK, u_1, \ldots, u_{k_N}, v, w_1, \ldots, w_{k_M}, z)$.

Signing $\mathcal{S}_{SK}(M_1, \ldots, M_{k_M}, N_1, \ldots, N_{k_N})$**:**
Given $(M_1, \ldots, M_{k_M}, N_1, \ldots, N_{k_N}) \in \mathbb{G}^{k_M} \times \mathbb{H}^{k_M}$ pick $r \leftarrow \mathbb{Z}_p^*$ and compute

$$R = G^{r} \qquad S = G^{z-rv}\prod_i M_i^{-w_i} \qquad T = (H\prod_i N_i^{-u_i})^{\frac{1}{r}}.$$

Return the signature (R, S, T).

Verification $\mathcal{V}_{VK}((M_1, \ldots, M_{k_M}, N_1, \ldots, N_{k_N}), (R, S, T))$**:**
Accept if $M_1, \ldots, M_{k_M}, R, S \in \mathbb{G}$ and $N_1, \ldots, N_{k_N}, T \in \mathbb{H}$ and

$$e(R, V)e(S, H)\prod_i e(M_i, W_i) = e(G, Z) \quad \wedge \quad e(R, T)\prod_i e(U_i, N_i) = e(G, H).$$

Fig. 1. Structure-preserving signature scheme for messages in $\mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$.

Theorem 5. *The signature scheme $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ described in Figure 1 is a structure-preserving signature scheme over $\mathcal{G}$ that is strongly existentially unforgeable against adaptive chosen message attacks in the generic group model.*

Proof. The verification key, the messages and the signatures consist of group elements in $\mathbb{G}$ and $\mathbb{H}$ and the verification consists of verifying two pairing product equations, so it is a structure-preserving scheme. Correctness follows from verifying that

$$e(G^r, H^v)e(G^{z-vr}\prod_i M_i^{-w_i}, H)\prod_i e(M_i, H^{w_i}) = e(G, H^z)$$
$$e(G^r, (H\prod_i N_i^{-u_i})^{\frac{1}{r}})\prod_i e(G^{u_i}, N_i) = e(G, H).$$

Lemma 1 shows that the signature scheme is secure in the generic group model for $k_M = 1$ and $k_N = 2$. We will show that if the signature scheme is secure for $k_M = 1$ and $k_N = 2$, then the signature scheme is also secure when using arbitrary constants $k_M \geq 1$ and $k_N \geq 2$. In the following we write $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ and $(\mathcal{K}', \mathcal{S}', \mathcal{V}')$ to distinguish between the two settings. We will show that if there is an adversary $\mathcal{A}'$ that can break $(\mathcal{K}', \mathcal{S}', \mathcal{V}')$, then there is an adversary $\mathcal{A}$ that can break $(\mathcal{K}, \mathcal{S}, \mathcal{V})$.

The adversary $\mathcal{A}$ gets as input a verification key $VK = (GK, U_1, U_2, V, W_1, Z)$. It picks at random $\alpha_i, \beta_i \leftarrow \mathbb{Z}_p$ and $\gamma_i, \delta_i \leftarrow \mathbb{Z}_p$ and computes

$$U_1' = U_1^{\gamma_1}U_2^{\delta_1} \ \ldots \ U_{k_N}' = U_1^{\gamma_{k_N}}U_2^{\delta_{k_N}} \qquad W_1' = W_1^{\alpha_1}H^{\beta_1} \ \ldots \ W_{k_M}' = W_1^{\alpha_{k_M}}H^{\beta_{k_M}}.$$

It gives the verification key $VK' = (GK, U_1', \ldots, U_{k_N}', V, W_1', \ldots, W_{k_N}', Z)$ to $\mathcal{A}'$. Conditioned on the overwhelmingly likely event $U_i' \neq 1$ and $W_i' \neq 1$ this has the same distribution as a normal key produced by $(\mathcal{K}', \mathcal{S}', \mathcal{V}')$.

When $\mathcal{A}'$ asks for a signature on $(M_1', \ldots, M_{k_M}', N_1', \ldots, N_{k_N}') \in \mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$ the adversary $\mathcal{A}$ computes

$$M = \prod_i (M_i')^{\alpha_i} \qquad N_1 = \prod_i (N_i')^{\gamma_i} \qquad N_2 = \prod_i (N_i')^{\delta_i}.$$

It asks the signing oracle for a signature (R, S, T) on (M, N_1, N_2). It then computes $S' = S\prod_i (M_i')^{-\beta_i}$. It returns the signature (R, S', T) to $\mathcal{A}$. It is straightforward to verify that a valid signature is returned to $\mathcal{A}'$. Furthermore, we observe that the returned signature is uniformly random over all possible solutions to the two verification equations just like a normal signature would be. It is therefore a good simulation.

Suppose $\mathcal{A}'$ produces a signature (R', S', T') on some $(M_1', \ldots, M_{k_M}', N_1', \ldots, N_{k_N}')$ satisfying the two verification equations using the key VK'. $\mathcal{A}$ can translate that into a valid signature (R', S, T') on a message (M, N_1, N_2) using VK by computing

$$S = S'\prod_i (M_i')^{\beta_i} \qquad M = \prod_i (M_i')^{\alpha_i} \qquad N_1 = \prod_i (N_i')^{\gamma_i} \qquad N_2 = \prod_i (N_i')^{\delta}.$$

We now have a strong existential forgery unless (R', S, T') has been used before in some query q to sign a message $(M^{(q)}, N_1^{(q)}, N_2^{(q)}) = (M, N_1, N_2)$. That would give

$$\prod_i (M_i')^{\alpha_i} = \prod_i (M_i^{(q)'})^{\alpha_i} \qquad \prod_i (N_i')^{\gamma_i} = \prod_i (N_i^{(q)'})^{\gamma_i}.$$

Observe that α_i and γ_i are information-theoretically hidden to $\mathcal{A}'$ who only sees $W'_i = W_1^{\alpha_i} H^{\beta_i}$ and $U'_i = U_1^{\gamma_i} U_2^{\delta_i}$. Furthermore, no matter the values of α_i, γ_i the adversary gets uniformly random signatures as answer to the chosen message attacks, so these signatures do not reveal anything about the α_i's and the γ_i's either. The only way the adversary can have more than negligible chance of success is by choosing $M'_1 = M_1^{(q)'}, \ldots, M'_{k_M} = M_{k_M}^{(q)'}, N'_1 = N_1^{(q)'}, \ldots, N'_{k_N} = N_{k_N}^{(q)'}$. This means $\mathcal{A}'$ has repeated the message from query q and some calculation shows that it has also repeated the signature $(R^{(q)'}, S^{(q)'}, T^{(q)'})$. We conclude that $\mathcal{A}'$ has negligible chance of breaking the strong existential unforgeability against chosen message attacks on the signature scheme with $k_M \geq 1$ and $k_N \geq 2$.

The remaining case to consider is $k_M = 0$ or $k_N \in \{0, 1\}$. Here it is easy to get a secure signature scheme, because we can simply require that the signer always uses $M = 1$ or $N_1 = 1$ or $N_2 = 1$, which can be checked in the verification step. Furthermore, when we always have $M = 1$ or $N_1 = 1$ or $N_2 = 1$ then the corresponding W_1 or U_1 or U_2 is not needed in the verification key. □

Lemma 1. *The signature scheme $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ described in Figure 1 is strongly existentially unforgeable against adaptive chosen message attacks in the generic group model for messages $(M, N_1, N_2) \in \mathbb{G} \times \mathbb{H}^2$.*

Proof. Let us for ease of notation write W instead of W_1 and U, U' instead of U_1, U_2. We write $(M, N, N') \in \mathbb{G} \times \mathbb{H}^2$ for the messages we are signing. We consider an adversary that only uses generic group operations on the group elements it sees and is unaware of the random u, u', v, w, z used in the public key and is unaware of the randomness r_i used to form the signature in signing query number i. Seeing signatures (R_i, S_i, T_i) on queries (M_i, N_i, N'_i) the generic adversary is restricted to picking $\rho, \rho_u, \rho_{u'}, \rho_1, \rho'_1, \ldots, \sigma, \sigma_u, \sigma_{u'}, \sigma_1, \sigma'_1, \ldots, \tau, \tau_v, \tau_w, \tau_z, \tau_1, \ldots \in \mathbb{Z}_p$ and computing

$$R = G^{\rho} U^{\rho_u} (U')^{\rho_{u'}} \prod_i R_i^{\rho_i} S_i^{\rho'_i}\ ,\ S = G^{\sigma} U^{\sigma_u} (U')^{\sigma_{u'}} \prod_i R_i^{\sigma_i} S_i^{\sigma'_i}\ ,\ T = H^{\tau} V^{\tau_v} W^{\tau_w} Z^{\tau_z} \prod_i T_i^{\tau_i}.$$

The queries (M_i, N_i, N'_i) are computed as products of $G, U, U', R_1, S_1, \ldots, R_{i-1}, S_{i-1}$ and $H, V, W, Z, T_1, \ldots, T_{i-1}$ raised to exponents chosen by the adversary and the message (M, N, N') for which a forgery is obtained is computed similarly. Taking discrete logarithms we have

$$\begin{aligned}
m_i &= \text{linear combination of } 1, u, u', r_1, s_1, \ldots, r_{i-1}, s_{i-1} \\
m &= \text{linear combination of } 1, u, u', r_1, s_1, \ldots, r_q, s_q \\
r &= \rho + \rho_u u + \rho_{u'} u' + \sum_i \rho_i r_i + \sum_i \rho'_i (z - r_i v - m_i w) \\
s &= \sigma + \sigma_u u + \sigma_{u'} u' + \sum_i \sigma_i r_i + \sum_i \sigma'_i (z - r_i v - m_i w) \\
n_i, n'_i &= \text{linear combination of } 1, v, w, z, t_1, \ldots, t_{i-1} \\
n, n' &= \text{linear combination of } 1, v, w, z, t_1, \ldots, t_q \\
t &= \tau + \tau_v v + \tau_w w + \tau_z z + \sum_i \tau_i \frac{1 - u n_i - u' n'_i}{r_i}
\end{aligned}$$

We first consider elements formal polynomials in the variables $u, u', v, w, z, r_1, \ldots, r_q$ and show that the generic adversary cannot make an existential forgery when they are viewed as formal multi-variate polynomials. Later, we will then consider the risk of two different formal polynomials resulting in identical values when evaluated over concrete random choices of $u, u', v, w, z, r_1, \ldots, r_q \in \mathbb{Z}_p^*$.

Taking discrete logarithms of the first verification equation gives us $rv + s + mw = z$, which means

$$0 = \rho v + \rho_u uv + \rho_{u'} u'v + \sum_i \rho_i r_i v + \sum_i \rho'_i (vz - r_i v^2 - m_i vw)$$
$$+ \sigma + \sigma_u u + \sigma_{u'} u' + \sum_i \sigma_i r_i + \sum_i \sigma'_i (z - r_i v - m_i w) + mw - z.$$

Since $s_i = z - r_i v - m_i w$ we have that $m_1, \ldots, m_q$ and m are multi-variate polynomials in $u, u', v, w, z, r_1, \ldots, r_q$. Each m_i has degree at most i and m has degree at most $q+1$.

Looking at the coefficients for $1, u, u', r_i$ we see that $\sigma = 0, \sigma_u = 0, \sigma_{u'} = 0$ and $\sigma_i = 0$ giving us $s = \sum_i \sigma'_i (z - r_i v - m_i w)$. Looking at the coefficients for $v, uv, u'v, r_i v^2$ we get $\rho = 0, \rho_u = 0, \rho_{u'} = 0, \rho'_i = 0$ giving us $r = \sum_i \rho_i r_i$. The coefficients for $r_i v$ give us $\sigma'_i = \rho_i$ so $s = \sum_i \rho_i (z - r_i v - m_i v)$.

Switching to the second verification equation we have $rt + un + u'n' = 1$. Define $\pi = \prod_i r_i$ and $\pi_j = \prod_{i \neq j} r_i$ such that $\pi = \pi_j r_j$. Multiplying the equation on both sides with π we get $rt\pi + un\pi + u'n'\pi = \pi$ so

$$0 = \left(\sum_i \rho_i r_i \right) \left(\tau\pi + \tau_v v\pi + \tau_w w\pi + \tau_z z\pi + \sum_j \tau_j (\pi_j - un_j \pi_j - u'n'_j \pi_j) \right)$$
$$+ un\pi + u'n'\pi - \pi.$$

Observe, $n_1, n'_1, \ldots, n_q, n'_q, n, n'$ are polynomials in $u, u', v, w, z, r_1^{-1}, \ldots, r_q^{-1}$. Each r_i^{-1} has at most degree 1 and a closer inspection reveals that $n_1\pi_1, n'_1\pi_1, \ldots, n_q\pi_q, n'_q\pi_q$ and $n\pi, n'\pi$ are polynomials in $u, u', v, w, z, r_1, \ldots, r_q$ of degree at most $q+1$.

Looking at the coefficients for π we see that there must exist some ℓ such that $\rho_\ell \neq 0$ and $\tau_\ell \neq 0$. Looking at the coefficients for $r_\ell\pi, r_\ell v\pi, r_\ell w\pi, r_\ell z\pi$ we see that $\tau = 0, \tau_v = 0, \tau_w = 0, \tau_z = 0$. Looking at the coefficients for $r_\ell \pi_j$ we see that $\tau_j = 0$ for $j \neq \ell$. Looking at the coefficients for $r_i \pi_\ell$ we see that $\rho_i = 0$ for $i \neq \ell$. This means $r = \rho_\ell r_\ell$ and $t = \tau_\ell \frac{1 - un_\ell - u'n'_\ell}{r_\ell}$. We now have

$$\rho_\ell r_\ell \cdot \tau_\ell \frac{1 - un_\ell - u'n'_\ell}{r_\ell} \pi - un\pi - \pi = 0.$$

From the coefficient of π we deduce that $\tau_\ell = \frac{1}{\rho_\ell}$. The equation now reads

$$\pi - un_\ell \pi - u'n'_\ell \pi + un\pi + u'n'\pi - \pi = 0,$$

which implies $un_\ell\pi + u'n_{\ell'}\pi = un\pi + u'n'_\ell\pi$. Plugging in all the possible linear combinations of $1, v, w, z, \frac{1 - un_1 - u'n'_1}{r_1}, \ldots, \frac{1 - un_q - u'n'_q}{r_q}$ that can make n, n', n_ℓ, n'_ℓ in this equation, we get $n = n_\ell$ and $n' = n'_\ell$.

Going back to the first equation we now have $r = \rho_\ell r_\ell$ and therefore $s = \rho_\ell(z - r_\ell v - m_\ell v)$, which gives us the equality

$$\rho_\ell r_\ell v + \rho_\ell(z - r_\ell v - m_\ell v) + mv - z = 0.$$

Looking at the coefficient of z we conclude $\rho_\ell = 1$. That tells us $m = m_\ell$. The adversary has therefore reused $m = m_\ell$ and $n = n_\ell, n' = n'_\ell$ for some ℓ and not obtained an existential forgery. Furthermore, $r = r_\ell, s = s_\ell, t = t_\ell$ so the adversary cannot even find a new signature on the same message.

We have now seen that the adversary cannot make an existential forgery when viewing group elements as formal multi-variate polynomials. However, it may be the case that for concrete choices of variables, two formally different polynomials evaluate to the same value. In this case, we cannot simulate the generic group and it may be that the adversary can make an existential forgery. The verification equations can be evaluated using generic group operations, so without loss of generality we can assume the adversary knows it when it has made a successful forgery. Since the polynomials have degree $O(q)$ we get with a birthday paradox argument and the Schwartz-Zippel lemma that the probability of this type of error occurring in the generic group simulation is a negligible $O(\frac{q^3}{p})$ when the adversary makes $O(q)$ generic group operations. □

5 Other aspects of structure-preserving signatures

5.1 Strong one-time signatures based on standard assumptions

We present below a strong one-time signature scheme for messages from $\mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$ with signature size 5 group elements. If the message is one-sided, i.e., $(M_1, \ldots, M_{k_M}) \in \mathbb{G}^{k_M}$, there is a simpler signature with 2 group elements and a single verification equation $e(R, H)e(S, V)\prod_i e(M_i, V_i) = e(G, W)$ [AHO10]. These schemes complement the lower bounds in Section 3 where it was shown that structure-preserving signature schemes with a single verification equation or with unilateral signatures or with signatures with less than 3 group elements do not exist if the adversary gets access to signatures on *two* random messages.

Key generation $\mathcal{K}(GK)$**:** Parse GK as $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$.

Pick $w, u, u_1, \ldots, u_{k_N}, v, z, v_1, \ldots, v_{k_M} \leftarrow \mathbb{Z}_p^*$ at random and compute

$$W = H^w, U = G^u, U_1 = G^{u_1}, \ldots, U_{k_N} = G^{u_{k_N}}, \quad \text{and}$$
$$Z = H^z, \ V = H^v, V_1 = H^{v_1}, \ldots, V_{k_M} = H^{v_{k_M}}.$$

Return verification key $VK = (GK, U, U_1, \ldots, U_{k_N}, V, Z, V_1, \ldots, V_{k_M}, W)$ and signing key $SK = (VK, w, u, u_1, \ldots, u_{k_N}, v, z, v_1, \ldots, v_{k_M})$.

Signing $\mathcal{S}_{SK}(M_1, \ldots, M_{k_M}, N_1, \ldots, N_{k_N})$**:** Given $(M_1, \ldots, M_{k_M}, N_1, \ldots, N_{k_N}) \in \mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$ pick at random $s_1, s_2, t \leftarrow \mathbb{Z}_p^*$ and compute

$$T = G^t, \qquad S_2 = H^{s_2}, \qquad R_2 = H^t S_2^{-u} \prod_i N_i^{-u_i}$$
$$S_1 = G^{s_1}, \qquad R_1 = G^w S_1^{-v} T^{-z} \prod_i M_i^{-v_i}$$

Verification $\mathcal{V}_{VK}((M_1,\ldots,M_{k_M},N_1,\ldots,N_{k_N}),(R_1,S_1,T,R_2,S_2))$**:**
Accept if $M_1,\ldots,M_{k_M},R_1,S_1,T\in\mathbb{G}$ and $N_1,\ldots,N_{k_N},R_2,S_2\in\mathbb{H}$ and

$$e(R_1,H)e(S_1,V)e(T,Z)\prod_i e(M_i,V_i)=e(G,W)\quad\wedge$$
$$e(G,R_2)e(U,S_2)\prod_i e(U_i,N_i)=e(T,H)$$

Theorem 6 (Full paper). *The signature scheme is strongly existentially unforgeable against one-time chosen message attacks if the DDH assumption holds in* $\mathbb{G}$ *and* $\mathbb{H}$*.*

5.2 Non-interactive assumptions

The existential unforgeability of our signature scheme in Figure 1 against adaptive chosen message attacks corresponds to an interactive cryptographic assumption. It would be nice to base the security of the signature scheme on a non-interactive assumption but we do not know of any such security reduction.

By adding a few group elements to the signature it is possible to base the signature scheme on a non-interactive cryptographic assumption though. Consider the following variant of the signature scheme in Figure 1, where the signer picks $M_1\leftarrow\mathbb{G}$ and $N_1,N_2\leftarrow\mathbb{H}$ at random when making signatures. In other words, we can sign messages of the form $(M_2,\ldots,M_{k_M},N_3,\ldots,N_{k_N})\in\mathbb{G}^{k_M-1}\times\mathbb{H}^{k_N-2}$ and a signature consists of $(R,S,M_1,T,N_1,N_2)\in\mathbb{G}^3\times\mathbb{H}^3$, which is verified by the verification equations

$$e(R,V)e(S,H)\prod_i e(M_i,W_i)=e(G,Z)\ \text{ and }\ e(R,T)\prod_i e(U_i,N_i)=e(G,H).$$

The signature scheme is strongly existentially unforgeable against adaptive chosen message attacks if the following non-interactive assumption holds for $\mathcal{G}$, which essentially says the signature scheme $(\mathcal{K},\mathcal{S},\mathcal{V})$ from Figure 1 is strongly existentially unforgeable against *random* message attacks for message space $\mathbb{G}\times\mathbb{H}^2$.

Assumption 1 *Given a random bilinear group* $(p,\mathbb{G},\mathbb{H},\mathbb{T},e,G,H)\leftarrow\mathcal{G}(1^k)$ *and uniformly random group elements* $(U,\hat{U},V,W,Z)\in\mathbb{G}^2\times\mathbb{H}^3$ *and uniformly random* $(R_1,S_1,M_1,T_1,N_1,\hat{N}_1),\ldots,(R_q,S_q,M_q,T_q,N_q,\hat{N}_q)\in\mathbb{G}^3\times\mathbb{H}^3$ *such that*

$$e(R_j,V)e(S_j,H)e(M_j,W)=e(G,Z)\text{ and }e(R_j,T_j)e(U,N_j)e(\hat{U},\hat{N}_j)=e(G,H)$$

a non-uniform polynomial time adversary has negligible probability of finding a different tuple $(R,S,M,T,N,\hat{N})\in\mathbb{G}^3\times\mathbb{H}^3$ *satisfying the two pairing product equations.*

Lemma 1 implies that Assumption 1 holds in the generic group model. Actually, a careful analysis of the proof of Lemma 1 shows that a generic adversary using $O(q)$ group operations has probability $O(\frac{q^2}{p})$ of breaking Assumption 1.

Theorem 7 (Full paper). *If Assumption 1 holds, then the signature scheme* $(\mathcal{K},\mathcal{S},\mathcal{V})$ *in Figure 1 is strongly existentially unforgeable against adaptive chosen message attacks when the signer always chooses* $M_1\leftarrow\mathbb{G}$ *and* $N_1,N_2\leftarrow\mathbb{H}$ *at random.*

The signature scheme we just described has signatures consisting of 6 group elements. By setting $U_1 = 1, \ldots, U_{k_N} = 1$ and dropping N_1 and N_2 from a signature, the scheme can be used to sign messages of the form $(M_2, \ldots, M_{k_M}) \in \mathbb{G}^{k_M - 1}$ using only 4 group elements. This variant is secure under a related non-interactive assumption.

5.3 Rerandomizable signatures

The signature scheme in Figure 1 is strongly existentially unforgeable, so it is not possible even to forge a new signature on a message that has already been signed before. In some cases strong existential unforgeability is a useful feature, while in other cases standard existential unforgeability suffices. In this section, we present a rerandomizable signature scheme where a signature can be modified into a different signature for the same message. Rerandomizability may for instance be useful in settings where the signature has to be hidden. One might choose to hide the signature by encrypting it but if the signature is rerandomizable it may be possible to send part of the rerandomized signature in the clear. An additional advantage of the rerandomizable signature scheme we are about to present is that after rerandomization we may only need to hide elements in one of the groups $\mathbb{H}$. This makes it possible to use special purpose variants of Groth-Sahai proofs (they refer to it as the linear case) that are particularly efficient.

We do not know how to construct a rerandomizable signature scheme with 3 group elements that can simultaneously sign messages both in $\mathbb{G}$ and $\mathbb{H}$. But by setting $W_i = 1$ and $Z = 1$ in the signature scheme in Figure 1 we get an efficient rerandomizable signature scheme for messages containing group elements in $\mathbb{H}$. The full description of our rerandomizable signature scheme can be found below.

Key generator $\mathcal{K}(GK)$**:** Parse GK as $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, e, G, H)$.

Pick at random $u_1, \ldots, u_{k_N}, v \leftarrow \mathbb{Z}_p^*$ and compute

$$U_1 = G^{u_1} \quad \ldots \quad U_{k_N} = G^{u_{k_N}} \qquad V = H^v.$$

Return $VK = (GK, U_1, \ldots, U_{k_N}, V)$ and $SK = (VK, u_1, \ldots, u_{k_N}, v)$.

Signing $\mathcal{S}_{SK}(N_1, \ldots, N_{k_N})$**:** Given $(N_1, \ldots, N_{k_N}) \in \mathbb{H}^{k_N}$ pick $r \leftarrow \mathbb{Z}_p^*$ and set

$$R = G^r \qquad S = R^v \qquad T = (H \prod_i N_i^{-u_i})^{\frac{1}{r}}.$$

Rerandomization $R_{VK}(R, S, T)$:

Pick $r' \leftarrow \mathbb{Z}_p^*$ and return the rerandomized signature $(R', S', T') = (R^{r'}, S^{r'}, T^{\frac{1}{r'}})$.

Verification $\mathcal{V}_{VK}((N_1, \ldots, N_{k_N}), (R, S, T))$**:**

Accept if $R, S \in \mathbb{G}$ and $N_1, \ldots, N_{k_N}, T \in \mathbb{H}$ and

$$e(R, V) = e(S, H) \qquad \wedge \qquad e(R, T) \prod_i e(U_i, N_i) = e(G, H).$$

Theorem 8 (Full paper). *The signature scheme $(\mathcal{K}, \mathcal{S}, \mathcal{V})$ over $\mathcal{G}$ described above is a rerandomizable structure-preserving signature scheme that is existentially unforgeable against adaptive chosen message attacks in the generic group model.*

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 *Lecture Notes in Computer Science*, pages 209–236, 2010.

[AHO10] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010.

[BCK10] Endre Bangerter, Jan Camenisch, and Stephan Krenn. Efficiency limitations for Σ-protocols for group homomorphisms. In *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 553–571, 2010.

[CL02] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In *SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289, 2002.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72, 2004.

[CLY09] Julien Cathalo, Benoît Libert, and Moti Yung. Group encryption: Non-interactive realization in the standard model. In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 179–196, 2009.

[Fuc09] Georg Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009.

[Fuc11] Georg Fuchsbauer. Commuting signatures and verifiable encryption. In *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 224–245, 2011.

[FV10] Georg Fuchsbauer and Damien Vergnaud. Fair blind signatures without random oracles. In *AFRICACRYPT*, volume 6055 of *Lecture Notes in Computer Science*, pages 16–33, 2010.

[GGK03] Rosario Gennaro, Yael Gertner, and Jonathan Katz. Lower bounds on the efficiency of encryption and digital signature schemes. In *STOC*, pages 417–425, 2003.

[GH08] Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 179–197, 2008.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.

[GPS08] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

[Gro06] Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In *ASIACRYPT*, volume 4248 of *Lecture Notes in Computer Science*, pages 444–459, 2006.

[Gro09] Jens Groth. Homomorphic trapdoor commitments to group elements. Cryptology ePrint Archive, Report 2009/007, 2009.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432, 2008.

[Nec94] Vasilii I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mat. Zametki*, 55(2):91–101, 1994.

[OS08] Rafail Ostrovsky and William E. Skeith III. Communication complexity in algebraic two-party protocols. In *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 379–396, 2008.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266, 1997.