Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions

Benoît Libert[1], Thomas Peters[2], and Moti Yung[3]

[1] Ecole Normale Supérieure de Lyon (France)
[2] Ecole Normale Supérieure, CNRS, INRIA (France)
[3] Google Inc. and Columbia University (USA)

Abstract. Group signatures are a central cryptographic primitive which allows users to sign messages while hiding their identity within a crowd of group members. In the standard model (without the random oracle idealization), the most efficient constructions rely on the Groth-Sahai proof systems (Eurocrypt'08). The structure-preserving signatures of Abe *et al.* (Asiacrypt'12) make it possible to design group signatures based on well-established, constant-size number theoretic assumptions (a.k.a. "simple assumptions") like the Symmetric eXternal Diffie-Hellman or Decision Linear assumptions. While much more efficient than group signatures built on general assumptions, these constructions incur a significant overhead w.r.t. constructions secure in the idealized random oracle model. Indeed, the best known solution based on simple assumptions requires 2.8 kB per signature for currently recommended parameters. Reducing this size and presenting techniques for shorter signatures are thus natural questions. In this paper, our first contribution is to significantly reduce this overhead. Namely, we obtain the first fully anonymous group signatures based on simple assumptions with signatures shorter than 2 kB at the 128-bit security level. In dynamic (resp. static) groups, our signature length drops to 1.8 kB (resp. 1 kB). This improvement is enabled by two technical tools. As a result of independent interest, we first construct a new structure-preserving signature based on simple assumptions which shortens the best previous scheme by 25%. Our second tool is a method for attaining anonymity in the strongest sense using a new CCA2-secure encryption scheme which is also a Groth-Sahai commitment.

Keywords. Group signatures, standard model, simple assumptions, efficiency, structure-preserving cryptography, QA-NIZK arguments.

1 Introduction

As introduced by Chaum and van Heyst [29] in 1991, group signatures allow members of a group administered by some authority to anonymously sign messages on behalf of the group. In order to prevent abuses, an opening authority has the power to uncover a signer's identity if the need arises.

The usual approach for building a group signature consists in having the

signer encrypt his group membership credential under the public key of the opening authority while appending a non-interactive zero-knowledge (NIZK) proof, which is associated with the message, claiming that things were done correctly. Until 2006, efficient instantiations of this primitive were only available under the random oracle idealization [14], which is limited to only provide heuristic arguments in terms of security [24]. This state of affairs changed in the last decade, with the emergence of solutions [20,21,37,38] enabled by breakthrough results in the design of relatively efficient non-interactive witness indistinguishable (NIWI) proofs [39]. While drastically more efficient than solutions based on general NIZK proofs [12,15], the constructions of [20,21,37,38] still incur a substantial overhead when compared with their random-oracle-based counterparts [10,32,18]. Moreover, their most efficient variants [21,38] tend to rely on parametrized assumptions – often referred to as "q-type" assumptions – where the number of input elements is determined by a parameter q which, in turn, depends on the number of users in the system or the number of adversarial queries (or both). Since the assumption becomes stronger as q increases, a different assumption is needed for every adversary (based on its number of queries) and every maximal number of users in the group. Not only does it limit the scalability of realizations, it also restricts the level of confidence in their security.

In this paper, we consider the problem of devising as short as possible group signatures based on simple assumptions. By "simple assumption", we mean a well-established assumption, like the Decision Diffie-Hellman assumption, which is simultaneously non-interactive and described using a constant number of elements, regardless of the number of users in the system or the number of adversarial queries. We remark that even in the random oracle model, this problem turns out to be highly non-trivial as non-simple assumptions (like the Strong RSA [10,45] or Strong Diffie-Hellman [18,32]) are frequently relied on. In the standard model, our main contribution is designing the first group signatures based on simple assumptions and whose size is less than 2 kB for the currently recommended 128-bit security level. In static groups, our most efficient scheme features signatures slightly longer than 1 kB. So far, the best standard-model group signature based on simple assumptions was obtained from the structure-preserving signatures (SPS) of Abe *et al* [1,2] and required 2.875 kB per signature. Along the way and as a result of independent interest, we also build a new structure-preserving signature (SPS) with the shortest length among those based on simple assumptions. Concretely, the best previous SPS based on similar assumptions [1,2] is shortened by 25%.

Related Work. Group signatures have a long history. Still, efficient and provably coalition-resistant constructions (in the random oracle model) remained elusive until the work of Ateniese, Camenisch, Joye and Tsudik [10] in 2000. At that time, however, there was no proper formalization of the security properties that can be naturally expected from group signatures. This gap was filled in 2003 by Bellare, Micciancio and Warinschi [12] (BMW) who captured all the requirements of group signatures in three properties. In (a variant of) this model, Boneh, Boyen and Shacham [18] obtained very short signatures using the ran-

dom oracle methodology [14].

The BMW model assumes static groups where the set of members is frozen after the setup phase beyond which no new member can be added. The setting of dynamic groups was explored later on by Bellare-Shi-Zhang [15] and, independently, by Kiayias and Yung [45]. In these models [15,45], short signature lengths were obtained in [32]. A construction based on interactive assumptions in the standard model was also put forth by Ateniese *et al.* [9]. Using standard assumptions, Boyen and Waters gave a different solution [20] based on the Groth-Ostrovsky-Sahai NIZK proof system [36]. They subsequently managed to obtain $O(1)$-size signatures at the expense of appealing to a q-type assumption [21] . Their constructions [20,21] were both analyzed in (a relaxation of) the BMW model [12] where the adversary is not granted access to a signature opening oracle. In dynamic groups [15], Groth [37] obtained constant-size signatures in the standard model but, due to huge hidden constants, his result was mostly a proof of concept. By making the most of Groth-Sahai NIWI proofs [39], he subsequently reduced signatures to 48 group elements [38] with the caveat of resting on relatively *ad hoc* q-type assumptions. For the time being, the best group signatures based on standard assumptions are enabled by the structure-preserving signatures of Abe, Chase, David, Kohlweiss, Nishimaki, and Ohkubo [1]. In asymmetric pairings $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ (where $\mathbb{G} \neq \hat{\mathbb{G}}$), anonymously signing messages requires at least 40 elements of $\mathbb{G}$ and 26 elements of $\hat{\mathbb{G}}$.

In 2010, Abe *et al.* [8,3] advocated the use of *structure-preserving* cryptography as a general tool for building privacy-preserving protocols in a modular fashion. In short, structure-preserving signatures (SPS) are signature schemes that smoothly interact with Groth-Sahai proofs [39] as messages, signatures public keys all live in the source groups $(\mathbb{G}, \hat{\mathbb{G}})$ of a bilinear map $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$. SPS schemes were initially introduced by Groth [37] and further studied in [26,33]. In the last three years, a large body of work was devoted to the feasibility and efficiency of structure-preserving signatures [37,26,33,8,3,4,23,28,40,1,2]. In Type III pairings (i.e., where $\mathbb{G} \neq \hat{\mathbb{G}}$ and no isomorphism is computable from $\hat{\mathbb{G}}$ to $\mathbb{G}$ or backwards), Abe *et al.* [4] showed that any SPS scheme must contain at least 3 group elements per signature. For a natural class of reductions, the security of optimally short signatures was also shown [5] *unprovable* under any non-interactive assumption. These impossibility results were recently found [7] not to carry over to Type II pairings (i.e., where $\mathbb{G} \neq \hat{\mathbb{G}}$ and an efficiently computable isomorphism $\psi : \hat{\mathbb{G}} \to \mathbb{G}$ is available).

To the best of our knowledge, the minimal length of structure-preserving signatures based on simple assumptions remains an unsettled open question. We believe it to be of primary importance considering the versatility of structure-preserving cryptography in the design of privacy-related protocols, including group signatures [8], group encryption [26] or adaptive oblivious transfer [35].

Our Results. The first contribution of this paper is to describe a new structure-preserving signature based on the standard Symmetric eXternal Diffie-Hellman (SXDH) assumption and an asymmetric variant of the Decision Linear assumption with only 10 group elements (more precisely, 9 elements of $\mathbb{G}$ and one

element of $\hat{\mathbb{G}}$) per signature. So far, the best instantiation of [1,2] required 7 elements of $\mathbb{G}$ and 4 elements of $\hat{\mathbb{G}}$. Since the representation of $\hat{\mathbb{G}}$ elements is at least twice as long as that of $\mathbb{G}$ elements, our scheme thus saves 26% in terms of signature length. Armed with our new SPS and other tools, we then construct dynamic group signatures using only 32 elements of $\mathbb{G}$ and 14 elements of $\hat{\mathbb{G}}$ in each signature, where Abe *et al.* [1,2] need at least 40 elements of $\mathbb{G}$ and 26 elements of $\hat{\mathbb{G}}$. For typical parameters, our signatures are thus 37% shorter with a total length of only 1.8 kB at the 128-bit security level. In an independent work, Kiltz, Pan and Wee [48] managed to obtain even shorter structure-preserving signatures than ours under the SXDH assumption. If their construction is used in our dynamic group signature, it allows eliminating at least 4 more elements of $\mathbb{G}$ from signatures. In the static model of Bellare, Micciancio and Warinschi [12], we describe an even more efficient realization where the signature length decreases to almost 1 kB.

Our Techniques. Our structure-preserving signature can be seen as a non-trivial optimization of a modular design, suggested by Abe *et al* [1], which combines a weakly secure SPS scheme and a tagged one-time signature (TOTS). In a TOTS scheme, each signature contains a fresh tag and, without knowing the private key, it should be computationally infeasible to generate a signature on a new message for a previously used tag. The construction of [1] obtains a full-fledged SPS by combining a TOTS scheme with an SPS system that is only secure against extended random message attacks (XRMA). As defined in [1], XRMA security basically captures security against an adversary that only obtains signatures on random group elements *even knowing* some auxiliary information used to sample these elements (typically their discrete logarithms). While Abe *et al.* [1] make use of the discrete logs of signed messages in their proofs of XRMA security, their modular construction does not. Here, by explicitly using the discrete logarithms in the construction, we obtain significant efficiency improvements. Using Waters' dual system techniques [56], we construct an SXDH-based F-unforgeable signature scheme which, according to the terminology of Belenkiy *et al.* [11], is a signature scheme that remains verifiable and unforgeable even if the adversary only outputs an injective function of the forgery message. Our new SPS is the result of combining our F-unforgeable signature and the TOTS system of [2]. We stress that our scheme can no longer be seen as an instantiation of a generic construction. Still, at the natural expense of sacrificing modularity, it does provide shorter signatures.

In turn, our F-unforgeable signatures are obtained by taking advantage of the quasi-adaptive NIZK (QA-NIZK) arguments of linear subspace membership suggested by Jutla and Roy [43] and further studied in [51,44], where the CRS may depend on the language for which proofs have to be generated. In a nutshell, our starting point is a signature scheme suggested by Jutla and Roy (inspired by ideas due to Camenisch *et al.* [22]) where each signature is a CCA2-secure encryption of the private key (made verifiable via QA-NIZK proofs) and the message is included in the label [54]. We rely on the observation that QA-NIZK proofs for linear subspaces [43] (or their optimized variants [51,44]) make it pos-

sible to verify signatures even if the message is only available in the exponent.

In order to save the equivalent of 15 elements of the group $\mathbb{G}$ and make the group signature as short as possible, we also design a new CCA2-secure tag-based encryption (TBE) scheme [52,47] which incorporates a Groth-Sahai commitment. In fully anonymous group signatures, CCA2-anonymity is usually acquired by verifiably encrypting the signer's credential using a CCA2-secure cryptosystem while providing evidence that the plaintext coincides with a committed group element. Inspired by a lossy encryption scheme [13] suggested by Hemenway *et al.* [41], we depart from this approach and rather use a CCA2-secure encryption scheme which simultaneously plays the role of a Groth-Sahai commitment. That is, even when the Groth-Sahai CRS is a perfectly hiding CRS, we are able to extract committed group elements for any tag but a specific one, where the encryption scheme behaves like a perfectly hiding commitment and induces perfectly NIWI proofs. In order to make the validity of TBE ciphertexts publicly verifiable, we rely on the QA-NIZK proofs of Libert *et al.* [51] which are well-suited to the specific subspaces encountered[4] in this context. We believe this encryption scheme to be of interest in its own right since it allows shortening other group signatures based on Groth-Sahai proofs (e.g., [38]) in a similar way.

Our group signature in the static BMW model [12] does not build on structure-preserving signatures but rather follows the same design principle as the constructions of Boyen and Waters [20,21]. It is obtained by extending our F-unforgeable signature into a 2-level hierarchical signature [46] (or, equivalently, an identity-based signature [53]) where first-level messages are implicit in the exponent. In spirit and from an efficiency standpoint, our static group signature is thus similar to the second construction [21] of Boyen and Waters, with the benefit of providing full anonymity while relying on the sole SXDH assumption.

2 Background

2.1 Hardness Assumptions

We use bilinear maps $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ over groups of prime order p where $e(g, \hat{h}) \neq 1_{\mathbb{G}_T}$ if and only if $g \neq 1_{\mathbb{G}}$ and $\hat{h} \neq 1_{\hat{\mathbb{G}}}$. We rely on hardness assumptions that are non-interactive and described using a constant number of elements.

Definition 1. *The* **Decision Diffie-Hellman** *(DDH) problem in $\mathbb{G}$, is to distinguish the distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c), with $a, b, c \xleftarrow{R} \mathbb{Z}_p$. The DDH assumption is the intractability of the problem for any PPT distinguisher.*

In the following, we will rely on the Symmetric external Diffie-Hellman (SXDH) assumption which posits the hardness of DDH in $\mathbb{G}$ and $\hat{\mathbb{G}}$ in asymmetric pairing configurations. We also assume the hardness of the following problem, which generalizes the Decision Linear problem [18] to asymmetric pairings.

[4] Specifically, we have to prove membership of a $t \times n$ subspace of rank t described by a $2t \times n$ matrix and the security proofs of [50,51] still work in this case.

Definition 2 ([1]). *In bilinear groups* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ *of prime order* p*, the* **eXternal Decision Linear Problem** 2 *(XDLIN$_2$) is to distinguish the distribution*

$$D_1 = \{(g, g^a, g^b, g^{ac}, g^{bd}, \hat{g}, \hat{g}^a, \hat{g}^b, \hat{g}^{ac}, \hat{g}^{bd}, \hat{g}^{c+d}) \in \mathbb{G}^5 \times \hat{\mathbb{G}}^6 \mid a, b, c, d \xleftarrow{R} \mathbb{Z}_p\}$$
$$D_2 = \{(g, g^a, g^b, g^{ac}, g^{bd}, \hat{g}, \hat{g}^a, \hat{g}^b, \hat{g}^{ac}, \hat{g}^{bd}, \hat{g}^{z}) \in \mathbb{G}^5 \times \hat{\mathbb{G}}^6 \mid a, b, c, d, z \xleftarrow{R} \mathbb{Z}_p\}.$$

The XDLIN$_1$ assumption is defined analogously and posits the infeasibility of distinguishing g^{c+d} and g^z given $(g, g^a, g^b, g^{ac}, g^{bd}, \hat{g}, \hat{g}^a, \hat{g}^b, \hat{g}^{ac}, \hat{g}^{bd})$.

2.2 Linearly Homomorphic Structure-Preserving Signatures

Structure-preserving signatures [8,3] are signature schemes where messages and public keys all consist of elements of a group over which a bilinear map $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ is efficiently computable.

Libert *et al.* [50] considered structure-preserving signatures with linear homomorphic properties. This section recalls the one-time linearly homomorphic structure-preserving signature (LHSPS) of [50]. In the description below, we assume that all algorithms take as input the description of common public parameters cp consisting of asymmetric bilinear groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$ of prime order $p > 2^\lambda$, where λ is the security parameter.

In [50], Libert *et al.* suggested the following construction which can be proved secure under the SXDH assumption.

Keygen(cp, n): Given common public parameters $\mathsf{cp} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$ and the dimension $n \in \mathbb{N}$ of the subspace to be signed. Then, choose $\hat{g}_z, \hat{g}_r \xleftarrow{R} \hat{\mathbb{G}}$. For $i = 1$ to n, pick $\chi_i, \gamma_i \xleftarrow{R} \mathbb{Z}_p$ and compute $\hat{g}_i = \hat{g}_z^{\chi_i} \hat{g}_r^{\gamma_i}$. The private key is $\mathsf{sk} = \{(\chi_i, \gamma_i)\}_{i=1}^n$ while the public key is $\mathsf{pk} = \big(\hat{g}_z,\ \hat{g}_r,\ \{\hat{g}_i\}_{i=1}^n\big) \in \hat{\mathbb{G}}^{n+2}$.

Sign($\mathsf{sk}, (M_1, \ldots, M_n)$): In order to sign a vector $(M_1, \ldots, M_n) \in \mathbb{G}^n$ using $\mathsf{sk} = \{(\chi_i, \gamma_i)\}_{i=1}^n$, output $\sigma = (z, r) = \big(\prod_{i=1}^n M_i^{-\chi_i}, \prod_{i=1}^n M_i^{-\gamma_i}\big)$.

SignDerive($\mathsf{pk}, \{(\omega_i, \sigma^{(i)})\}_{i=1}^\ell$): given pk as well as ℓ tuples $(\omega_i, \sigma^{(i)})$, parse $\sigma^{(i)}$ as $\sigma^{(i)} = \big(z_i, r_i\big)$ for $i = 1$ to ℓ. Return $\sigma = (z, r) = \big(\prod_{i=1}^\ell z_i^{\omega_i}, \prod_{i=1}^\ell r_i^{\omega_i}\big)$.

Verify($\mathsf{pk}, \sigma, (M_1, \ldots, M_n)$): Given a signature $\sigma = (z, r) \in \mathbb{G}^2$ and a vector $(M_1, \ldots, M_n)$, return 1 if and only if $(M_1, \ldots, M_n) \neq (1_\mathbb{G}, \ldots, 1_\mathbb{G})$ and (z, r) satisfy $1_{\mathbb{G}_T} = e(z, \hat{g}_z) \cdot e(r, \hat{g}_r) \cdot \prod_{i=1}^n e(M_i, \hat{g}_i)$.

In [51], (a variant of) this scheme was used to construct constant-size QA-NIZK arguments [43] showing that a vector $\boldsymbol{v} \in \mathbb{G}^n$ belongs to a linear subspace subspace of rank t spanned by a matrix $\boldsymbol{\rho} \in \mathbb{G}^{t \times n}$. Under the SXDH assumption, each argument is comprised of two elements of $\mathbb{G}$, independently of t or n.

3 An F-Unforgeable Signature

As a technical tool, our constructions rely on a signature scheme which we prove F-unforgeable under the SXDH assumption. As defined by Belenkiy *et al.* [11], F-unforgeability refers to the inability of the adversary to output a valid signature

for a non-trivial message M without outputting the message itself. Instead, the adversary is only required to output $F(M)$, for an injective but not necessarily efficiently invertible function F.

The scheme extends ideas used in signature schemes suggested in [22,43], where each signature is a CCA2-secure encryption —using the message to be signed as a label— of the private key accompanied with a QA-NIZK proof that the encrypted value is the private key. In their most efficient variant, Jutla and Roy observed [43, Section 5] that it suffices to encrypt private keys g^{ω} with a projective hash value $(v^M \cdot w)^r$ [31] so as to obtain signatures of the form $(\sigma_1, \sigma_3, \sigma_3) = (g^{\omega} \cdot (v^M \cdot w)^r, g^r, h^r)$, which is reminiscent of selectively secure Boneh-Boyen signatures [16].

As in [56,34], the security proof proceeds with a sequence of games to gradually reach a game where the signing oracle never uses the private key, in which case it becomes easier to prove security. In the final game, signatures always encrypt a random value while QA-NIZK proofs are simulated. When transitioning from one hybrid game to the next one, the crucial step is to argue that, even if the signing oracle produces fewer and fewer signatures using the private key, the adversary's forgery will still encrypt the private key. This is achieved via an information theoretic argument borrowed from hash proof systems [30,31].

In order to obtain an F-unforgeable signature which is verifiable given only $F(M)$, our key observation is that QA-NIZK proofs make it possible to verify signatures even if M appears only implicitly in a tuple $(g^{s \cdot M}, g^s, h^{s \cdot M}, h^s) \in \mathbb{G}^4$.

Keygen(cp) : Given common public parameters $\mathsf{cp} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$ consisting of asymmetric bilinear groups of prime order $p > 2^{\lambda}$, do the following.

1. Choose $\omega, a \xleftarrow{R} \mathbb{Z}_p$, $g, v, w \xleftarrow{R} \mathbb{G}$, $\hat{g} \xleftarrow{R} \hat{\mathbb{G}}$ and set $h = g^a$, $\Omega = h^{\omega}$.
2. Define a matrix $\mathbf{M} = (M_{j,i})_{j,i}$ given by

$$\mathbf{M} = \left(\begin{array}{c|c|c|c|c|c} g & 1 & 1 & 1 & 1 & h \\ \hline v & g & 1 & h & 1 & 1 \\ \hline w & 1 & g & 1 & h & 1 \end{array}\right) \in \mathbb{G}^{3 \times 6}. \tag{1}$$

3. Generate a key pair $(\mathsf{sk}_{hsps}, \mathsf{pk}_{hsps})$ for the one-time linearly homomorphic signature of Section 2.2 in order to sign vectors of dimension $n = 6$. Let $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i)\}_{i=1}^6$ be the private key, of which the corresponding public key is $\mathsf{pk}_{hsps} = \big(\hat{g}_z,\ \hat{g}_r,\ \{\hat{g}_i\}_{i=1}^6\big)$.
4. Using $\mathsf{sk}_{hsps} = \{\chi_i, \gamma_i\}_{i=1}^6$, generate one-time homomorphic signatures $\{(z_j, r_j)\}_{j=1}^3$ on the rows $\boldsymbol{M}_j = (M_{j,1}, \ldots, M_{j,6}) \in \mathbb{G}^6$ of $\mathbf{M}$. These are obtained as $(z_j, r_j) = \Big(\prod_{i=1}^6 M_{j,i}^{-\chi_i},\ \prod_{i=1}^6 M_{j,i}^{-\gamma_i}\Big)$, for each $j \in \{1,2,3\}$ and, as part of the common reference string for the QA-NIZK proof system of [51], they will be included in the public key.

The private key is $\mathsf{sk} := \omega$ and the public key is defined as

$$\mathsf{pk} = \Big((\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T),\ p,\ g,\ h,\ \hat{g},\ (v, w),\ \Omega = h^{\omega},\ \mathsf{pk}_{hsps},\ \{(z_j, r_j)\}_{j=1}^3\Big).$$

Sign(sk, M) : given $\mathsf{sk} = \omega$ and a message $M \in \mathbb{Z}_p$, choose $s \xleftarrow{R} \mathbb{Z}_p$ to compute

$$\sigma_1 = g^{\omega} \cdot (v^M \cdot w)^s, \qquad \sigma_2 = g^{s \cdot M}, \qquad \sigma_3 = g^s$$
$$\sigma_4 = h^{s \cdot M} \qquad \sigma_5 = h^s$$

Then, generate a QA-NIZK proof that the vector $(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \Omega) \in \mathbb{G}^6$ is in the row space of $\mathbf{M}$. This QA-NIZK proof $(z, r) \in \mathbb{G}^2$ is obtained as

$$z = z_1^{\omega} \cdot (z_2^M \cdot z_3)^s, \qquad r = r_1^{\omega} \cdot (r_2^M \cdot r_3)^s. \tag{2}$$

Return the signature $\sigma = \big(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, z, r\big)$.

Verify(pk, σ, M) : parse σ as above and return 1 if and only if it holds that

$$e(\tilde{z}, \hat{g}_z) \cdot e(\tilde{r}, \hat{g}_r) = e(\sigma_1, \hat{g}_1)^{-1} \cdot e(\sigma_3, \hat{g}_3 \cdot {\hat{g}_2}^M)^{-1} \cdot e(\sigma_5, \hat{g}_5 \cdot {\hat{g}_4}^M)^{-1} \cdot e(\Omega, \hat{g}_6)^{-1}$$

and $(\sigma_2, \sigma_4) = (\sigma_3^M, \sigma_5^M)$.

Note that a signature can be verified given only $F(M) = \hat{g}^M$ by testing the equalities $e(\sigma_2, \hat{g}) = e(\sigma_3, F(M))$, $e(\sigma_4, \hat{g}) = e(\sigma_5, F(M))$ and

$$\begin{aligned} &e(z, \hat{g_z}) \cdot e(r, \hat{g_r}) \\ &= e(\sigma_1, \hat{g_1})^{-1} \cdot e(\sigma_2, \hat{g_2})^{-1} \cdot e(\sigma_3, \hat{g_3})^{-1} \cdot e(\sigma_4, \hat{g_4})^{-1} \cdot e(\sigma_5, \hat{g_5})^{-1} \cdot e(\Omega, \hat{g_6})^{-1}. \end{aligned}$$

In order to keep the description as simple as possible, the above description uses the QA-NIZK argument system of [51], which is based on linearly homomorphic signatures. However, the security proof goes through if we use the more efficient SXDH-based QA-NIZK argument of Jutla and Roy [44], as explained in the full version of the paper. The pair (z, r) can thus be replaced by a single $\mathbb{G}$-element.

Under the SXDH assumption, the scheme can be proved to be F-unforgeable for the injective function $F(M) = \hat{g}^M$. The proof of this result is implied by the security result of Section 4 where we describe a generalization of the scheme that will be used to build a group signature in the BMW model.

4 A Two-Level SXDH-based Hierarchical Signature

This section extends our F-unforgeable signature into a 2-level hierarchical signature with partially hidden messages. In a 2-level hierarchical signature [46] (a.k.a. identity-based signature), a signature on a message ID (called "identity") can be used as a delegated key for signing messages of the form (ID, M) for any M. In order to construct group signatures, Boyen and Waters [21] used hierarchical signatures that can be verified even when identities (i.e., first-level messages) are not explicitly given to the verifier, but only appear implicitly in the exponent. The syntax and security definition are given in [20,21].

In their most efficient construction [21], Boyen and Waters used a non-standard q-type assumption. This section gives a very efficient solution based on the standard SXDH assumption. It is obtained from our signature of Section

3 by having a signature $(g^{\omega} \cdot (v^{\mathsf{ID}} \cdot w)^s, g^s, h^s)$ on a given identity ID serve as a private key for this identity modulo the introduction of a delegation component t^s akin to those of the Boneh-Boyen-Goh hierarchical IBE [17]. For the security proof to go through, we need to make sure that pairs $(g^{s \cdot M}, g^s)$, $(h^{s \cdot M}, h^s)$ hide the same message M, which is not immediately verifiable in the SXDH setting. To enforce this condition, we thus include $\hat{g}^M$ in each signature.

Setup(cp) : Given public parameters $\mathsf{cp} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$, do the following.

1. Choose $\omega, a \xleftarrow{R} \mathbb{Z}_p$, $g, t, v, w \xleftarrow{R} \mathbb{G}$, $\hat{g} \xleftarrow{R} \hat{\mathbb{G}}$ and set $h = g^a$, $\Omega = h^{\omega}$.
2. Define a matrix $\mathbf{M} = (M_{j,i})_{j,i}$ given by

$$\mathbf{M} = \left(\begin{array}{c|c|c|c|c|c|c|c} g & 1 & 1 & 1 & 1 & 1 & 1 & h \\ \hline v & g & 1 & h & 1 & 1 & 1 & 1 \\ \hline w & 1 & g & 1 & h & 1 & 1 & 1 \\ \hline t & 1 & 1 & 1 & 1 & g & h & 1 \end{array}\right) \in \mathbb{G}^{4 \times 8}. \quad (3)$$

3. Generate a key pair $(\mathsf{sk}_{hsps}, \mathsf{pk}_{hsps})$ for the one-time linearly homomorphic signature of Section 2.2 in order to sign vectors of dimension $n = 8$. Let $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i)\}_{i=1}^8$ be the private key, of which the corresponding public key is $\mathsf{pk}_{hsps} = \big(\hat{g}_z,\ \hat{g}_r,\ \{\hat{g}_i\}_{i=1}^8\big)$.
4. Using $\mathsf{sk}_{hsps} = \{\chi_i, \gamma_i\}_{i=1}^8$, generate one-time homomorphic signatures $\{(z_j, r_j)\}_{j=1}^4$ on the rows $\boldsymbol{M}_j = (M_{j,1}, \ldots, M_{j,8}) \in \mathbb{G}^8$ of $\mathbf{M}$. These are obtained as $(z_j, r_j) = \Big(\prod_{i=1}^8 M_{j,i}^{-\chi_i},\ \prod_{i=1}^8 M_{j,i}^{-\gamma_i}\Big)$ each for $j \in \{1, \ldots, 4\}$ and, as part of the common reference string for the QA-NIZK proof system of [51], they will be included in the public key.

The master secret key is $\mathsf{msk} := \omega$ and the master public key is defined as

$$\mathsf{mpk} = \Big((\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T),\ p,\ g,\ h,\ \hat{g},\ (t, v, w),\ \Omega = h^{\omega},\ \mathsf{pk}_{hsps},\ \{(z_j, r_j)\}_{j=1}^4\Big).$$

Extract$(\mathsf{msk}, \mathsf{ID})$: given $\mathsf{msk} = \omega$ and $\mathsf{ID} \in \mathbb{Z}_p$, choose $s \xleftarrow{R} \mathbb{Z}_p$ to compute

$$K_1 = g^{\omega} \cdot (v^{\mathsf{ID}} \cdot w)^s, \qquad K_2 = g^{s \cdot \mathsf{ID}}, \qquad K_3 = g^s$$
$$K_4 = h^{s \cdot \mathsf{ID}} \qquad K_5 = h^s \qquad K_6 = t^s$$

as well as $\hat{K}_7 = \hat{g}^{\mathsf{ID}}$. Looking ahead, K_6 will serve as a delegation component in the generation of level 2 signatures. Then, generate a QA-NIZK proof that the vector $(K_1, K_2, K_3, K_4, K_5, 1, 1, \Omega) \in \mathbb{G}^8$ is in the row space of the first 3 rows of $\mathbf{M}$. This QA-NIZK proof $(z, r) \in \mathbb{G}^2$ is obtained as

$$z = z_1^{\omega} \cdot (z_2^{\mathsf{ID}} \cdot z_3)^s, \qquad r = r_1^{\omega} \cdot (r_2^{\mathsf{ID}} \cdot r_3)^s. \quad (4)$$

Then, generate a QA-NIZK proof (z_d, r_d) that the delegation component K_6 is well-formed. This proof consists of $(z_d, r_d) = (z_4^s, r_4^s)$. The private key is

$$K_{\mathsf{ID}} = \big(K_1, K_2, K_3, K_4, K_5, K_6, \hat{K}_7, z, r, z_d, r_d\big). \quad (5)$$

Sign$(\mathsf{mpk}, K_{\mathsf{ID}}, M)$: to sign $M \in \mathbb{Z}_p$, parse K_{ID} as in (5) and do the following.

1. Choose $s' \xleftarrow{R} \mathbb{Z}_p$ and compute

$$\sigma_1 = K_1 \cdot K_6^M \cdot (v^{\mathsf{ID}} \cdot t^M \cdot w)^{s'} = g^{\omega} \cdot (v^{\mathsf{ID}} \cdot t^M \cdot w)^{\tilde{s}},$$

where $\tilde{s} = s + s'$, as well as

$$\sigma_2 = K_2 \cdot g^{s' \cdot \mathsf{ID}} = g^{\tilde{s} \cdot \mathsf{ID}}, \qquad \sigma_3 = K_3 \cdot g^{s'} = g^{\tilde{s}}, \qquad \hat{\sigma_6} = \hat{K_7} = \hat{g}^{\mathsf{ID}}$$
$$\sigma_4 = K_4 \cdot h^{s' \cdot \mathsf{ID}} = h^{\tilde{s} \cdot \mathsf{ID}}, \qquad \sigma_5 = K_5 \cdot h^{s'} = h^{\tilde{s}}.$$

2. Using (z, r) and (z_d, r_d), generate a QA-NIZK proof $(\tilde{z}, \tilde{r}) \in \mathbb{G}^2$ that the vector $(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_3^M, \sigma_5^M, \Omega) \in \mathbb{G}^8$ is in the row space of $\mathbf{M}$. Namely, compute $\tilde{z} = z \cdot z_d^M \cdot (z_2^{\mathsf{ID}} \cdot z_4^M \cdot z_3)^{s'}$ and $\tilde{r} = r \cdot r_d^M \cdot (r_2^{\mathsf{ID}} \cdot r_4^M \cdot r_3)^{s'}$.

Return the signature $\sigma = \left(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \tilde{z}, \tilde{r}, \hat{\sigma_6}\right) \in \mathbb{G}^7 \times \hat{\mathbb{G}}$.

Verify$(\mathsf{mpk}, \sigma, M)$: parse σ as above and return 1 if and only if it holds that

$$e(\tilde{z}, \hat{g_z}) \cdot e(\tilde{r}, \hat{g_r}) = e(\sigma_1, \hat{g_1})^{-1} \cdot e(\sigma_2, \hat{g_2})^{-1} \cdot e(\sigma_3, \hat{g_3} \cdot \hat{g_6}^M)^{-1} \cdot e(\sigma_4, \hat{g_4})^{-1} \cdot e(\sigma_5, \hat{g_5} \cdot \hat{g_7}^M)^{-1} \cdot e(\Omega, \hat{g_8})^{-1}$$

as well as $e(\sigma_2, \hat{g}) = e(\sigma_3, \hat{\sigma_6})$ and $e(\sigma_4, \hat{g}) = e(\sigma_5, \hat{\sigma_6})$.

As in Section 3, the technique of [44] can be used to shorten the signature by one element of $\mathbb{G}$ as it allows replacing $(\tilde{z}, \tilde{r})$ by one element of $\mathbb{G}$.

We prove that, under the sole SXDH assumption, the scheme is secure in the sense of the natural security definition used by Boyen and Waters [20,21]. In short, this definition requires that the adversary be unable to forge a valid signature for a pair $(\mathsf{ID}^\star, M^\star)$ such that no private key query was made for $\mathsf{ID}^\star$ and no signing query was made for the pair $(\mathsf{ID}^\star, M^\star)$.

Theorem 1. *The above hierarchical signature is secure under chosen-message attacks if the SXDH assumption holds in* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$. (The proof is available the full version of the paper).

A simple reduction shows that the signature scheme of Section 3 is F-unforgeable so long as the above scheme is a secure 2-level hierarchical signature.

Theorem 2. *The signature scheme of Section 3 is F-unforgeable under chosen-message attacks for the function $F(M) = \hat{g}^M$ if the SXDH assumption holds in* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$. (The proof is available in the full version of the paper).

5 A Structure-Preserving Signature from the SXDH and $\mathbf{XDLIN_2}$ Assumptions

Our F-unforgeable signature of Section 3 can be combined with the tagged one-time signature of Abe *et al.* [2] (or, more precisely, an adaption of [2] to asymmetric pairings) so as to obtain a new structure-preserving signature based on

the SXDH and XDLIN_2 assumptions. Like [1], we obtain an SPS scheme based on simple assumptions with only 11 group elements per signature. However, only one of them has to be in $\hat{\mathbb{G}}$, instead of 4 in [1]. Considering that $\hat{\mathbb{G}}$ elements are at least twice as long to represent as those of $\mathbb{G}$, we thus shorten signatures by the equivalent of 3 elements of $\mathbb{G}$ (or 20%).

Our construction can be seen as an optimized instantiation of a general construction [1] that combines a tagged one-time signature and an SPS scheme which is only secure against extended random-message (XRMA) attacks. A tagged one-time signature (TOTS) is a signature scheme where each signature contains a single-use tag: namely, only one signature is generated w.r.t. each tag. The generic construction of [1] proceeds by certifying the tag of the TOTS scheme using an XRMA-secure SPS scheme. Specifically, our F-unforgeable signature assumes the role of the XRMA-secure signature and its shorter message space allows us to make the most of the optimal tag size of [2]. In [1], the proofs of XMRA security rely on the property that, when the reduction signs random groups elements of its choice, it is allowed to know their discrete logarithms. However, this property is only used in the security proof and not in the scheme itself. Here, we also use the discrete logarithm of the tag in the SPS construction itself, which allows our F-unforgeable signature to supersede the XRMA-secure signature. By exploiting the smaller message space of our F-unforgeable signature, we can leverage the optimal tag size of [2]. Unlike the SPS of [2], we do not need to expand the tag from one to three group elements before certifying it.

Keygen(cp, n) : given the length n of messages to be signed and common parameters cp specifying the description of bilinear groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$, do the following.

a. Generate a key pair $(\mathsf{sk}_{fsig}, \mathsf{pk}_{fsig}) \leftarrow \mathsf{Setup}(\mathsf{cp})$ for the F-unforgeable signature of Section 3. Namely,

1. Choose $\omega, a \xleftarrow{R} \mathbb{Z}_p$, $g \xleftarrow{R} \mathbb{G}$, $\hat{g} \xleftarrow{R} \hat{\mathbb{G}}$ and set $h = g^a$, $\Omega = h^\omega$. Then, choose $v, w \xleftarrow{R} \mathbb{G}$.
2. Define a matrix $\mathbf{M} = (M_{j,i})_{j,i}$ given by

$$\mathbf{M} = \left(\begin{array}{c|c|c|c|c|c} g & 1 & 1 & 1 & 1 & h \\ \hline v & g & 1 & h & 1 & 1 \\ \hline w & 1 & g & 1 & h & 1 \end{array}\right) \in \mathbb{G}^{3\times 6}. \qquad (6)$$

3. Generate a key pair $(\mathsf{sk}_{hsps}, \mathsf{pk}_{hsps})$ for the linearly homomorphic signature of Section 2.2 in order to sign vectors of dimension $n = 6$. Let $\mathsf{sk}_{hsps} = \{(\chi_{0,i}, \gamma_{0,i})\}_{i=1}^6$ be the private key, of which the corresponding public key is $\mathsf{pk}_{hsps} = \big(\hat{g}_z,\ \hat{g}_r,\ \{\hat{g}_i\}_{i=1}^6\big)$.
4. Using $\mathsf{sk}_{hsps} = \{\chi_{0,i}, \gamma_{0,i}\}_{i=1}^6$, generate one-time homomorphic signatures $\{(z_j, r_j)\}_{j=1}^3$ on the rows $\boldsymbol{M}_j = (M_{j,1}, \ldots, M_{j,6}) \in \mathbb{G}^6$ of $\mathbf{M}$. These are obtained as $(z_j, r_j) = \Big(\prod_{i=1}^6 M_{j,i}^{-\chi_{0,i}},\ \prod_{i=1}^6 M_{j,i}^{-\gamma_{0,i}}\Big)$, for $j \in \{1, 2, 3\}$ and, as part of the common reference string for the QA-NIZK proofs of [51], they will be included in the public key.

b. Generate a key pair $(\mathsf{pk}_{pots}, \mathsf{sk}_{pots})$ for the partial one-time SPS of Abe *et al.* [1]. Namely, choose $w_z, w_r, \mu_z, \mu_u, w_t \xleftarrow{R} \mathbb{Z}_p$ and set

$$\begin{array}{lllll} \hat{G}_z = \hat{g}^{w_z}, & \hat{G}_r = \hat{g}^{w_r}, & \hat{G}_t = \hat{g}^{w_t}, & \hat{H}_z = \hat{g}^{\mu_z}, & \hat{H}_u = \hat{g}^{\mu_u} \\ G_z = g^{w_z}, & G_r = g^{w_r}, & G_t = g^{w_t}, & H_z = g^{\mu_z}, & H_u = g^{\mu_u} \end{array}$$

Then, for $i = 1$ to n, choose $\chi_i, \gamma_i, \delta_i \xleftarrow{R} \mathbb{Z}_p$ and compute $\hat{G}_i = \hat{G_z}^{\chi_i} \cdot \hat{G_r}^{\gamma_i}$ and $\hat{H}_i = \hat{G_z}^{\chi_i} \cdot \hat{G_r}^{\delta_i}$. Define $\mathsf{sk}_{pots} := \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^n$ and

$$\mathsf{pk}_{pots} := \big(G_z, G_r, G_t, H_z, H_u, \hat{G}_z, \hat{G}_r, \hat{G}_t, \hat{H}_z, \hat{H}_u, \{\hat{G}_i, \hat{H}_i\}_{i=1}^n\big).$$

The private key is $SK = (\omega, w_r, \mu_u, \mathsf{sk}_{pots})$ and the public key consists of

$$PK = \Big(g,\ h,\ \hat{g},\ (v, w),\ \Omega = h^{\omega},\ \mathsf{pk}_{pots},\ \mathsf{pk}_{hsps},\ \{(z_j, r_j)\}_{j=1}^3 \Big).$$

Sign$(SK, \boldsymbol{M})$: given $SK = (\omega, w_r, \mu_u, \mathsf{sk}_{pots})$ and $\boldsymbol{M} = (M_1, \ldots, M_n) \in \mathbb{G}^n$,

1. Choose $s, \tau \xleftarrow{R} \mathbb{Z}_p$ to compute

$$\begin{array}{lll} \sigma_1 = g^{\omega} \cdot (v^{\tau} \cdot w)^s, & \sigma_2 = g^{s \cdot \tau}, & \sigma_3 = g^s, \\ \sigma_4 = h^{s \cdot \tau} & \sigma_5 = h^s, & \tilde{\sigma_6} = \hat{g}^{\tau}. \end{array}$$

Then, generate a QA-NIZK proof that the vector $(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \Omega)$ is in the row space of $\mathbf{M}$. This proof $(z, r) \in \mathbb{G}^2$ is computed as

$$z = z_1^{\omega} \cdot (z_2^{\tau} \cdot z_3)^s, \qquad r = r_1^{\omega} \cdot (r_2^{\tau} \cdot r_3)^s. \tag{7}$$

2. Choose $\zeta \xleftarrow{R} \mathbb{Z}_p$ and compute $Z = g^{\zeta} \cdot \prod_{i=1}^n M_i^{-\chi_i}$ as well as

$$R = (G_t^{\tau} \cdot {G_z}^{-\zeta})^{1/w_r} \cdot \prod_{i=1}^n M_i^{-\gamma_i}, \qquad U = (H_z^{-\zeta})^{1/\mu_u} \cdot \prod_{i=1}^n M_i^{-\delta_i}$$

Return $\sigma = \big(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \tilde{\sigma_6}, z, r, Z, R, U\big) \in \mathbb{G}^5 \times \hat{\mathbb{G}} \times \mathbb{G}^5$.

Verify$(PK, \sigma, \boldsymbol{M})$: given $\boldsymbol{M} = (M_1, \ldots, M_n) \in \mathbb{G}^n$, parse σ as above. Return 1 if and only if $e(\sigma_2, \hat{g}) = e(\sigma_3, \tilde{\sigma_6})$ and $e(\sigma_4, \hat{g}) = e(\sigma_5, \tilde{\sigma_6})$ as well as

$$\begin{aligned} e(z, \hat{g_z}) \cdot e(r, \hat{g_r}) &= \prod_{i=1}^5 e(\sigma_i, \hat{g}_i)^{-1} \cdot e(\Omega, \hat{g_6})^{-1} \\ e(G_t, \tilde{\sigma_6}) &= e(Z, \hat{G_z}) \cdot e(R, \hat{G_r}) \cdot \prod_{i=1}^n e(M_i, \hat{G}_i) \\ 1_{\mathbb{G}_T} &= e(Z, \hat{H_z}) \cdot e(U, \hat{H_u}) \cdot \prod_{i=1}^n e(M_i, \hat{H}_i). \end{aligned} \tag{8}$$

Each signature requires 10 elements of $\mathbb{G}$ and one element of $\hat{\mathbb{G}}$. Using the optimized F-unforgeable signature based on the Jutla-Roy QA-NIZK proof [44], we can also save one more element of $\mathbb{G}$ and obtain signatures in $\mathbb{G}^9 \times \hat{\mathbb{G}}$, which shortens the signatures of Abe *et al.* [1] by 26%. In the full version of the paper, we give more detailed comparisons among all SPS based on non-interactive assumptions.

In the application to group signatures, it is desirable to minimize the number of signature components that need to appear in committed form. To this end, signatures must be randomizable in such a way that (σ_3, σ_5) can appear in the clear modulo a re-randomization of $s \in \mathbb{Z}_p$. To enable this randomization, it is necessary to augment signatures (similarly to [6]) with a randomization token $(g^\tau, h^\tau, v^\tau, z_2^\tau, r_2^\tau)$. We will prove that the scheme remains unforgeable even when the signing oracle also outputs these randomization tokens at each invocation.[5] We call this notion *extended existential unforgeability* (or EUF-CMA* for short).

When the re-randomization tokens are used, proving the knowledge of a signature on a committed message $\boldsymbol{M} \in \mathbb{G}^n$ requires $2n + 24$ elements of $\mathbb{G}$ and 12 elements of $\hat{\mathbb{G}}$. In comparison, the best previous solution of Abe *et al.* costs $2n + 26$ elements of $\mathbb{G}$ and 18 elements of $\hat{\mathbb{G}}$.

Theorem 3. *The scheme provides EUF-CMA* security if the SXDH and XDLIN$_2$ assumptions hold in* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$. (The proof is given in the full version of the paper).

In short, the proof of Theorem 3 considers two kinds of forgeries. In Type I forgeries, the adversary's forgery contains an element $\hat{\sigma_6}^\star$ that did not appear in any signature obtained by the forger during the game. In contrast, Type II forgeries are those for which $\hat{\sigma_6}^\star$ is recycled from a response of the signing oracle. It is easy to see that a Type I forger allows breaking the security of the F-unforgeable signature. As for Type II forgeries, they are shown to contradict the XDLIN$_2$ assumption via a careful adaptation of the proof given by Abe *et al.* for their TOTS scheme [2]. While the latter was originally presented in symmetric pairings, it goes through in Type 3 pairings modulo natural changes that consist in making sure that most handled elements of $\hat{\mathbb{G}}$ have a counterpart in $\mathbb{G}$. One difficulty is that, at each query, the reduction must properly simulate the randomization tokens $(v^\tau, g^\tau, h^\tau, z_2^\tau, r_2^\tau)$ as well as an instance of the F-unforgeable signature without knowing the discrete logarithm $\log_{\hat{g}}(\hat{\sigma_6}) = \hat{g}^\tau$ or that of its shadow $\log_g(\sigma_6) = g^\tau$ in $\mathbb{G}$. Fortunately, this issue can be addressed by letting the reduction know $\log_g(v)$ and $\log_g(w)$.

In an independent work [48], Kiltz, Pan and Wee obtained even shorter signatures, which live in $\mathbb{G}^6 \times \hat{\mathbb{G}}$ under the SXDH assumption. On the other hand, their security reduction is looser than ours as the gap between the adversary's advantage and the reduction's probability to break the underlying assumption is quadratic (instead of linear in our case) in the number of signing queries.

[5] Note, however, that the adversary is not required to produce any randomization token as part of its forgery.

6 A Publicly Verifiable Tag-Based Encryption Scheme

As a tool for constructing a CCA2-anonymous group signature, we describe a new tag-based encryption scheme [52,47] which is inspired by the lossy encryption scheme [13] of [41]. In our group signature, we will exploit the fact that the DDH-based lossy encryption scheme of Bellare *et al.* [13] can also be seen as a Groth-Sahai commitment.

Keygen(cp)**:** Given public parameters $\mathsf{cp} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$ specifying asymmetric bilinear groups of prime order $p > 2^\lambda$, conduct the following steps.

1. Choose $g, h \xleftarrow{R} \hat{\mathbb{G}}$. Choose $x, \alpha, \beta \xleftarrow{R} \mathbb{Z}_p$ and set $X_1 = g^x$, $X_2 = h^x$, $S = g^\alpha$, $T = g^\beta$, $W = h^\alpha$ and $V = h^\beta$.
2. Generate a key pair $(\mathsf{pk}'_{hsig}, \mathsf{sk}'_{hsig})$ for the homomorphic signature of Section 2.2 in order to sign vectors in $\mathbb{G}^3$. Let $\mathsf{pk}'_{hsig} = \big(\hat{G}_z, \hat{G}_r, \{\hat{G}_i\}_{i=1}^3\big)$ be the public key and let $\mathsf{sk}'_{hsig} = \{(\varphi_i, \vartheta_i)\}_{i=1}^3$ be the private key.
3. Use sk'_{hsig} to generate linearly homomorphic signatures $\{(Z_i, R_i)\}_{i=1}^4$ on the rows of the matrix

$$\mathbf{L} = \left(\begin{array}{c|c|c} g & 1 & T \\ \hline h & 1 & V \\ \hline 1 & g & S \\ \hline 1 & h & W \end{array}\right) \in \mathbb{G}^{4\times 3}$$

which form a subspace of rank 2. The key pair consists of $\mathsf{sk} = (x, \alpha, \beta)$ and $\mathsf{pk} := \Big(g, h, X_1, X_2, S, W, T, V, \mathsf{pk}'_{hsig}, \{(Z_i, R_i)\}_{i=1}^4\Big)$.

Encrypt(pk, M, τ)**:** To encrypt $M \in \mathbb{G}$ under the tag τ, choose $\theta_1, \theta_2 \xleftarrow{R} \mathbb{Z}_p$ and compute the ciphertext $\boldsymbol{C} = (C_0, C_1, C_2, Z, R)$ as

$$\boldsymbol{C} = \big(M \cdot X_1^{\theta_1} \cdot X_2^{\theta_2},\ g^{\theta_1} \cdot h^{\theta_2},\ (S^\tau \cdot T)^{\theta_1} \cdot (W^\tau \cdot V)^{\theta_2},\\ (Z_3^\tau \cdot Z_1)^{\theta_1} \cdot (Z_4^\tau \cdot Z_2)^{\theta_2}, (R_3^\tau \cdot R_1)^{\theta_1} \cdot (R_4^\tau \cdot R_2)^{\theta_2}\big).$$

Here, (Z, R) serves as a proof that the vector (C_1, C_1^τ, C_2) is in the row space of $\mathbf{L}$ and satisfies

$$e(Z, \hat{G}_z) \cdot e(R, \hat{G}_r) = e(C_1, \hat{G}_1{}^\tau \cdot \hat{G}_2)^{-1} \cdot e(C_2, \hat{G}_2)^{-1} \tag{9}$$

Decrypt$(\mathsf{sk}, \boldsymbol{C}, \tau)$**:** Parse $\boldsymbol{C}$ as above. Return $\perp$ if (Z, R) does not satisfy (9). Otherwise, return $M = C_0/C_1^x$.

We observe that (C_0, C_1) form a Groth-Sahai commitment based on the DDH assumption in $\mathbb{G}$. If $\log_g(X_1) = \log_h(X_2)$, the commitment is extractable. Otherwise, it is perfectly hiding. We will use this CCA2-secure scheme as a commitment that is extractable on all tags, except one $\tau^\star$ where it behaves as a perfectly hiding commitment. The above system achieves this while only expanding the original Groth-Sahai commitment (C_0, C_1) by 3 elements of $\mathbb{G}$.

This scheme will save our group signatures from having to contain (beyond (C_0, C_1)) an additional CCA2-secure encryption and a NIZK proof that the plaintext coincides with the content of a Groth-Sahai commitment. The above technique allows saving the equivalent of 16 elements of $\mathbb{G}$. We thus believe this cryptosystem to be of interest in its own right since it can be used in a similar way to shorten other group signatures (e.g., [38]) based on Groth-Sahai proofs.

In the full paper, the scheme is proved secure in the sense of [47].

Theorem 4. *The above scheme is selective-tag weakly IND-CCA2-secure if the SXDH assumption holds.* (The proof is given in the full paper).

7 Short Group Signatures in the BMW Model

The TBE scheme of Section 6 allows us to achieve anonymity in the CCA2 sense by encrypting an encoding of the group member's identifier. In order to minimize the signature length, we let the TBE ciphertext live in $\mathbb{G}$ instead of $\hat{\mathbb{G}}$. To open signatures in constant time, however, the opening algorithm uses the extraction trapdoor of a Groth-Sahai commitment in $\hat{\mathbb{G}}^2$ rather than the private key sk_{tbe} of the TBE system. The latter key is only used in the proof of anonymity where the reduction uses a somewhat inefficient opening algorithm of complexity $O(N)$.

Keygen(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and the number of users N, choose asymmetric bilinear groups $\mathsf{cp} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p)$ of order $p > 2^\lambda$.

1. Generate a key pair $(\mathsf{msk}, \mathsf{mpk})$ for the two-level hierarchical signature of Section 4. Let
$$\mathsf{mpk} := \Big((\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T),\ p,\ g,\ h,\ \hat{g},\ (t, v, w),\ \Omega = h^\omega,\ \mathsf{pk}_{hsps},\ \{(z_j, r_j)\}_{j=1}^4\Big)$$
be the master public key and $\mathsf{msk} := \omega \in \mathbb{Z}_p$ be the master secret key.
2. Generate a key pair $(\mathsf{sk}_{tbe}, \mathsf{pk}_{tbe})$ for the tag-based encryption scheme of Section 6. Let $\mathsf{pk}_{tbe} = \Big(g, h, X_1, X_2, S, W, T, V, \mathsf{pk}'_{hsig}, \{(Z_i, R_i)\}_{i=1}^4\Big)$ be the public key and $\mathsf{sk}_{tbe} = (x, \alpha, \beta)$ be the underlying private key. For simplicity, the element g can be recycled from mpk.
3. Choose a vector $\hat{\boldsymbol{u_1}} = (\hat{u}_{11}, \hat{u}_{12}) \xleftarrow{R} \hat{\mathbb{G}}^2$ and set $\hat{\boldsymbol{u_2}} = \hat{\boldsymbol{u_1}}^\xi$, where $\xi \xleftarrow{R} \mathbb{Z}_p$. Also, define the vectors $\boldsymbol{u_1} = (g, X_1)$ and $\boldsymbol{u_2} = (h, X_2)$. These vectors will form Groth-Sahai CRSes $(\boldsymbol{u_1}, \boldsymbol{u_2})$ and $(\hat{\boldsymbol{u_1}}, \hat{\boldsymbol{u_2}})$ in the perfectly binding setting. Although sk_{tbe} serves as an extraction trapdoor for commitments generated on the CRS $(\boldsymbol{u_1}, \boldsymbol{u_2})$, the group manager will more efficiently use $\zeta = \log_{\hat{u}_{11}}(\hat{u}_{12})$ to open signatures.
4. Choose a chameleon hash function $\mathsf{CMH} = (\mathsf{CMKg}, \mathsf{CMhash}, \mathsf{CMswitch})$ with a key pair (hk, tk) and randomness space $\mathcal{R}_{hash}$.
5. For each group member i, choose an identifier $\mathsf{ID}_i \xleftarrow{R} \mathbb{Z}_p$ and use msk to compute $K_{\mathsf{ID}_i} = (K_1, K_2, K_3, K_4, K_5, K_6, \hat{K_7}, z, r, z_d, r_d)$, where
$$K_1 = g^\omega \cdot (v^{\mathsf{ID}_i} \cdot w)^s \cdot, \qquad K_2 = g^{s \cdot \mathsf{ID}_i}, \qquad K_3 = g^s$$
$$K_4 = h^{s \cdot \mathsf{ID}_i} \qquad K_5 = h^s \qquad K_6 = t^s$$
$$z = z_1^\omega \cdot (z_2^{\mathsf{ID}_i} \cdot z_3)^s \qquad r = r_1^\omega \cdot (r_2^{\mathsf{ID}_i} \cdot r_3)^s \qquad \hat{K_7} = \hat{g}^{\mathsf{ID}_i}$$

and $(z_d, r_d) = (z_4^s, r_4^s)$. For each $i \in \{1, \ldots, N\}$, the i-th group member's private key is $\mathsf{gsk}[i] = (\mathsf{ID}_i, K_{\mathsf{ID}_i})$.

The group manager's secret key is $\mathsf{gsk} := \big(\mathsf{msk}, \zeta = \log_{\hat{u}_{11}}(\hat{u}_{12})\big)$ while the group public key consists of

$$\mathsf{gpk} := \Big((\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T),\ \mathsf{mpk},\ \mathsf{pk}_{tbe},\ (\boldsymbol{u_1}, \boldsymbol{u_2}),\ (\hat{\boldsymbol{u_1}}, \hat{\boldsymbol{u_2}}),\ \mathsf{CMH},\ hk\Big).$$

Sign$(\mathsf{gpk}, \mathsf{gsk}[i], M)$**:** In order to sign a message $M \in \mathbb{Z}_p$ using the i-th group member's private key $\mathsf{gsk}[i] = (\mathsf{ID}_i, K_{\mathsf{ID}_i})$, conduct the following steps.

1. Using $K_{\mathsf{ID}_i} = (K_1, K_2, K_3, K_4, K_5, K_6, \hat{K_7}, z, r, z_d, r_d)$, derive a second-level hierarchical signature. Namely, choose $s' \xleftarrow{R} \mathbb{Z}_p$ and compute

$$\begin{aligned}
\sigma_1 &= K_1 \cdot K_6^M \cdot (v^{\mathsf{ID}_i} \cdot t^M \cdot w)^{s'} & \sigma_2 &= K_2 \cdot g^{s' \cdot \mathsf{ID}_i} = g^{\tilde{s} \cdot \mathsf{ID}_i} \\
&= g^{\omega} \cdot (v^{\mathsf{ID}_i} \cdot t^M \cdot w)^{\tilde{s}} & \sigma_3 &= K_3 \cdot g^{s'} = g^{\tilde{s}} \\
\sigma_4 &= K_4 \cdot h^{s' \cdot \mathsf{ID}_i} = h^{\tilde{s} \cdot \mathsf{ID}_i} & \sigma_5 &= K_5 \cdot h^{s'} = h^{\tilde{s}},
\end{aligned}$$

and $\hat{\sigma_6} = \hat{K_7}$, where $\tilde{s} = s + s'$, as well as

$$\begin{aligned}
\tilde{z} &= z \cdot z_d^M \cdot (z_2^{\mathsf{ID}_i} \cdot z_4^M \cdot z_3)^{s'} & \tilde{r} &= r \cdot r_d^M \cdot (r_2^{\mathsf{ID}_i} \cdot r_4^M \cdot r_3)^{s'} \\
&= z_1^{\omega} \cdot (z_2^{\mathsf{ID}_i} \cdot z_4^M \cdot z_3)^{\tilde{s}} & &= r_1^{\omega} \cdot (r_2^{\mathsf{ID}_i} \cdot r_4^M \cdot r_3)^{\tilde{s}}.
\end{aligned}$$

2. Choose $\theta_1, \ldots, \theta_{12} \xleftarrow{R} \mathbb{Z}_p$ and compute Groth-Sahai commitments

$$\begin{aligned}
\boldsymbol{C}_{\sigma_1} &= (1, \sigma_1) \cdot \boldsymbol{u_1}^{\theta_1} \cdot \boldsymbol{u_2}^{\theta_2}, & \boldsymbol{C}_{\sigma_2} &= (1, \sigma_2) \cdot \boldsymbol{u_1}^{\theta_3} \cdot \boldsymbol{u_2}^{\theta_4}, \\
\boldsymbol{C}_{\sigma_4} &= (1, \sigma_4) \cdot \boldsymbol{u_1}^{\theta_5} \cdot \boldsymbol{u_2}^{\theta_6}, & \boldsymbol{C}_{\hat{\sigma_6}} &= (1, \hat{\sigma_6}) \cdot \hat{\boldsymbol{u_1}}^{\theta_7} \cdot \hat{\boldsymbol{u_2}}^{\theta_8}. \\
\boldsymbol{C}_{\tilde{z}} &= (1, \tilde{z}) \cdot \boldsymbol{u_1}^{\theta_9} \cdot \boldsymbol{u_2}^{\theta_{10}}, & \boldsymbol{C}_{\tilde{r}} &= (1, \tilde{r}) \cdot \boldsymbol{u_1}^{\theta_{11}} \cdot \boldsymbol{u_2}^{\theta_{12}}
\end{aligned}$$

Note that $\boldsymbol{C}_{\sigma_2}$ can be written as $(C_1, C_0) = (g^{\theta_3} \cdot h^{\theta_4}, \sigma_2 \cdot X_1^{\theta_3} \cdot X_2^{\theta_4})$.

3. Generate Groth-Sahai NIWI proofs $\boldsymbol{\pi}_1 \in \hat{\mathbb{G}}^2$, $\boldsymbol{\pi}_2 \in \mathbb{G}^2 \times \hat{\mathbb{G}}^2$ and $\boldsymbol{\pi}_3 \in \mathbb{G}^2 \times \hat{\mathbb{G}}^2$ that committed variables $(\tilde{z}, \tilde{r}, \sigma_1, \sigma_2, \sigma_4, \hat{\sigma_6})$ satisfy

$$\begin{aligned}
e(\boxed{\tilde{z}}, \hat{g_z}) \cdot e(\boxed{\tilde{r}}, \hat{g_r}) = e(\boxed{\sigma_1}, \hat{g_1})^{-1} \cdot e(\boxed{\sigma_2}, \hat{g_2})^{-1} \cdot e(\sigma_3, \hat{g_3} \cdot \hat{g_6}^M)^{-1} \\
\cdot e(\boxed{\sigma_4}, \hat{g_4})^{-1} \cdot e(\sigma_5, \hat{g_5} \cdot \hat{g_7}^M)^{-1} \cdot e(\Omega, \hat{g_8})^{-1}
\end{aligned} \tag{10}$$

and

$$e(\boxed{\sigma_2}, \hat{g}) = e(\sigma_3, \boxed{\hat{\sigma_6}}), \qquad e(\boxed{\sigma_4}, \hat{g}) = e(\sigma_5, \boxed{\hat{\sigma_6}}). \tag{11}$$

4. Choose $r_{hash} \xleftarrow{R} \mathcal{R}_{hash}$ and compute a chameleon hash value

$$\tau = \mathsf{CMhash}(hk, (\boldsymbol{C}_{\sigma_1}, \boldsymbol{C}_{\sigma_2}, \sigma_3, \boldsymbol{C}_{\sigma_4}, \sigma_5, \boldsymbol{C}_{\hat{\sigma_6}}, \boldsymbol{C}_{\tilde{z}}, \boldsymbol{C}_{\tilde{r}}, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \boldsymbol{\pi}_3), r_{hash}).$$

Then, using τ and $(\theta_3, \theta_4) \in \mathbb{Z}_p^2$, compute $C_2 = (S^\tau \cdot T)^{\theta_3} \cdot (W^\tau \cdot V)^{\theta_4}$. Using pk'_{hsig}, compute $(Z, R) = \big((Z_3^\tau \cdot Z_1)^{\theta_3} \cdot (Z_4^\tau \cdot Z_2)^{\theta_4}, (R_3^\tau \cdot R_1)^{\theta_3} \cdot (R_4^\tau \cdot R_2)^{\theta_4}\big)$ as a QA-NIZK argument that (C_1, C_1^τ, C_2) is in the row

space of $\mathbf{L}$. This allows turning $\boldsymbol{C}_{\sigma_2} = (C_1, C_0)$ into a TBE ciphertext $\tilde{\boldsymbol{C}}_{\sigma_2} = (C_0, C_1, C_2, Z, R)$ as

$$\tilde{\boldsymbol{C}}_{\sigma_2} = \big(\sigma_2 \cdot X_1^{\theta_3} \cdot X_2^{\theta_4},\ g^{\theta_3} \cdot h^{\theta_4},\ (S^{\tau} \cdot T)^{\theta_3} \cdot (W^{\tau} \cdot V)^{\theta_4},\\ (Z_3^{\tau} \cdot Z_1)^{\theta_3} \cdot (Z_4^{\tau} \cdot Z_2)^{\theta_4},\ (R_3^{\tau} \cdot R_1)^{\theta_3} \cdot (R_4^{\tau} \cdot R_2)^{\theta_4} \big) \in \mathbb{G}^5$$

for the tag τ. Note that $\tilde{\boldsymbol{C}}_{\sigma_2}$ contains the original commitment $\boldsymbol{C}_{\sigma_2}$.
Return $\sigma = \big(\boldsymbol{C}_{\sigma_1}, \tilde{\boldsymbol{C}}_{\sigma_2}, \sigma_3, \boldsymbol{C}_{\sigma_4}, \sigma_5, \boldsymbol{C}_{\hat{\sigma_6}}, \boldsymbol{C}_{\tilde{z}}, \boldsymbol{C}_{\tilde{r}}, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \boldsymbol{\pi}_3, r_{hash}\big)$.

Verify$(\mathsf{gpk}, M, \sigma)$**:** Parse σ as above. Return 1 if and only if: (i) The proofs $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \boldsymbol{\pi}_3$ verify; (ii) $\tilde{\boldsymbol{C}}_{\sigma_2}$ is a valid TBE ciphertext (i.e., (9) holds) for the tag $\tau = \mathsf{CMhash}(hk, (\boldsymbol{C}_{\sigma_1}, \boldsymbol{C}_{\sigma_2}, \sigma_3, \boldsymbol{C}_{\sigma_4}, \sigma_5, \boldsymbol{C}_{\hat{\sigma_6}}, \boldsymbol{C}_{\tilde{z}}, \boldsymbol{C}_{\tilde{r}}, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \boldsymbol{\pi}_3), r_{hash})$.

Open$(\mathsf{gpk}, \mathsf{gmsk}, M, \sigma)$**:** To open σ using $\mathsf{gmsk} = \big(\mathsf{msk}, \zeta\big)$, parse σ as above and return $\perp$ if it is not a valid signature w.r.t. gpk and M. Otherwise, use $\zeta = \log_{\hat{u}_{11}}(\hat{u}_{12})$ to decrypt the Elgamal ciphertext $\boldsymbol{C}_{\hat{\sigma_6}} \in \hat{\mathbb{G}}^2$. Then, check if the resulting plaintext is $\hat{g}^{\mathsf{ID}}$ for some group member's identifier ID. If so, output ID. Otherwise, return $\perp$.

The signature consists of 19 elements of $\mathbb{G}$, 8 elements of $\hat{\mathbb{G}}$ and one element of $\mathbb{Z}_p$. If each element of $\mathbb{G}$ (resp. $\hat{\mathbb{G}}$) has a 256-bit (resp. 512-bit) representation, the entire signature fits within 9216 bits (or 1.125 kB). By using the technique of Jutla and Roy [44] to shorten the hierarchical signature, it is possible to shorten the latter by one group element (as explained in Section 4), which saves two elements of $\mathbb{G}$ in the group signature without modifying the underlying assumption. In this case, the signature length reduces to 8704 bits (or 1.062 kB). Using the technique of Boyen, Mei and Waters [19], it is also possible to eliminate the randomness r_{hash} and replace the chameleon hash function by an ordinary collision-resistant hash function, as explained in the full version of the paper. By doing so, at the expense of a group public key made of $\Theta(\lambda)$ elements of $\hat{\mathbb{G}}$, we can further compress signatures down to 8448 bits (or 1.031 kB).

To give a concrete comparison with earlier constructions, an implementation of the Boyen-Waters group signature [21] in asymmetric prime order groups requires 8 elements of $\mathbb{G}$ and 8 elements of $\hat{\mathbb{G}}$ for a total of 6400 bits per signature. However, besides the SXDH assumption, the resulting scheme relies on the non-standard q-Hidden Strong Diffie-Hellman assumption [21] and only provides anonymity in the CPA sense.

Theorem 5. *The scheme provides full traceability under the SXDH assumption.*

The proof of Theorem 5 relies on the unforgeability of the two-level hierarchical signature of Section 4. By preparing extractable Groth-Sahai CRSes $(\boldsymbol{u_1}, \boldsymbol{u_2})$ and $(\boldsymbol{\hat{u}_1}, \boldsymbol{\hat{u}_2})$, the reduction can always turn a full traceability adversary (see [12] for a definition) into a forger for the hierarchical signature. The proof is straightforward and the details are omitted.

Theorem 6. *The scheme provides full anonymity assuming that: (i) The SXDH assumption holds in* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$*; (ii)* CMhash *is a collision-resistant chameleon hash function.* (The proof is given in the full version of the paper).

In the full version of the paper, we extend the above system to obtain dynamic group signatures based on the SXDH and XDLIN_2 assumption. The signature length is only 1.8 kB, which gives us the shortest dynamic group signatures based on constant-size assumptions to date. The construction builds on our structure-preserving signature and the encryption scheme of Section 6 in a modular manner. Detailed efficiency comparisons are given in the full paper.

Acknowledgements

The first author's work was supported by the "Programme Avenir Lyon Saint-Etienne de l'Université de Lyon" in the framework of the programme "Investissements d'Avenir" (ANR-11-IDEX-0007). The second author was supported by the European Research Council (FP7/2007-2013 Grant Agreement no. 339563 CryptoCloud). Part of this work of the third author was done while visiting the Simons Institute for Theory of Computing, U.C. Berkeley.

References

1. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, M. Ohkubo. Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions. In *Asiacrypt'12*, *LNCS* 7658, pp. 4–24, 2012.
2. M. Abe, B. David, M. Kohlweiss, R. Nishimaki, M. Ohkubo. Tagged One-Time Signatures: Tight Security and Optimal Tag Size. In *PKC'13*, *LNCS* 7778, pp. 312–331, 2013.
3. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, M. Ohkubo. Structure-Preserving Signatures and Commitments to Group Elements. In *Crypto'10*, *LNCS* 6223, pp. 209–236, 2010.
4. M. Abe, J. Groth, K. Haralambiev, M. Ohkubo. Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. In *Crypto'11*, *LNCS* 6841, pp. 649–666, 2011.
5. M. Abe, J. Groth, M. Ohkubo. Separating Short Structure-Preserving Signatures from Non-interactive Assumptions In *Asiacrypt'11*, *LNCS* 7073, pp. 628–646, 2011.
6. M. Abe, J. Groth, M. Ohkubo, M. Tibouchi. Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures. In *TCC'14*, *LNCS* 8349, pp. 688–712, 2014.
7. M. Abe, J. Groth, M. Ohkubo, M. Tibouchi. Structure-Preserving Signatures in Type II Pairings. In *Crypto'14*, *LNCS* 8616, pp. 390–407, 2014.
8. M. Abe, K. Haralambiev, M. Ohkubo. Signing on Elements in Bilinear Groups for Modular Protocol Design. Cryptology ePrint Archive: Report 2010/133, 2010.
9. G. Ateniese, J. Camenisch, S. Hohenberger, B. de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive: Report 2005/385, 2005.
10. G. Ateniese, J. Camenisch, M. Joye, G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Crypto'00*, *LNCS* 1880, pp. 255–270, 2000.
11. M. Belenkiy, M. Chase, M. Kohlweiss, A. Lysyanskaya. P-signatures and Non-interactive Anonymous Credentials. In *TCC'08*, *LNCS* 4948, pp. 356–374, 2008.

12. M. Bellare, D. Micciancio, B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *Eurocrypt'03*, *LNCS* 2656, pp. 614–629, 2003.
13. M. Bellare, D. Hofheinz, S. Yilek. Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. In *Eurocrypt'09*, *LNCS* 5479, pp. 1–35, 2009.
14. M. Bellare, P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *1st ACM Conference on Computer and Communications Security*, pp. 62–73, ACM Press, 1993.
15. M. Bellare, H. Shi, C. Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA'05*, *LNCS* 3376, pp. 136–153, 2005.
16. D. Boneh, X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Eurocrypt'04*, *LNCS* 3027, pp. 223–238, 2004.
17. D. Boneh, X. Boyen, E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Eurocrypt'05*, *LNCS* 3494, pp. 440–456, 2005.
18. D. Boneh, X. Boyen, H. Shacham. Short Group Signatures. In *Crypto'04*, *LNCS* 3152, pp. 41–55. Springer, 2004.
19. X. Boyen, Q. Mei, B. Waters. Direct Chosen-Ciphertext Security from Identity-Based Techniques. In *ACM-CCS'05*, pp. 320–329, ACM Press, 2006.
20. X. Boyen, B. Waters. Compact Group Signatures Without Random Oracles. In *Eurocrypt'06*, *LNCS* 4004, pp. 427–444, Springer, 2006.
21. X. Boyen, B. Waters. Full-Domain Subgroup Hiding and Constant-Size Group Signatures. In *PKC'07*, *LNCS* 4450, pp. 1–15, 2007.
22. J. Camenisch, N. Chandran, and V. Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In *Eurocrypt '09*, LNCS 5479, pp. 351–368, Springer, 2009.
23. J. Camenisch, M. Dubovitskaya, K. Haralambiev. Efficient Structure-Preserving Signature Scheme from Standard Assumptions. In *SCN'12*, LNCS 7485, pp. 76–94, Springer, 2012.
24. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. *Journal of the ACM*, 51(4):557–594, 2004.
25. R. Canetti, S. Halevi, J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In *Eurocrypt'04*, *LNCS* 3027, pp. 207–222, 2004.
26. J. Cathalo, B. Libert, M. Yung. Group Encryption: Non-Interactive Realization in the Standard Model. In *Asiacrypt'09*, *LNCS* 5912, pp. 179–196, 2009.
27. M. Chase, M. Kohlweiss. A Domain Transformation for Structure-Preserving Signatures on Group Elements. Cryptology ePrint Archive: Report 2011/342, 2011.
28. M. Chase, M. Kohlweiss. A New Hash-and-Sign Approach and Structure-Preserving Signatures from DLIN. In *SCN'12*, *LNCS* 7485, pp. 131–148, 2012.
29. D. Chaum, E. van Heyst. Group Signatures. In *Eurocrypt'91*, *LNCS* 547, pp. 257–265, Springer, 1991.
30. R. Cramer, V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Crypto'98*, LNCS 1462, pp. 13–25, 1998.
31. R. Cramer, V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In *Eurocrypt'02*, *LNCS* 2332, pp. 45–64, 2002.
32. C. Delerablée, D. Pointcheval. Dynamic Fully Anonymous Short Group Signatures. In *Vietcrypt'06*, *LNCS* 4341, pp. 193–210, Springer, 2006.
33. G. Fuchsbauer. Automorphic Signatures in Bilinear Groups and an Application to Round-Optimal Blind Signatures. Cryptology ePrint Archive: Report 2009/320, 2009.

34. M. Gerbush, A. Lewko, A. O 'Neill, B. Waters. Dual form signatures: An approach for proving security from static assumptions. In *Asiacrypt '12*, LNCS 7658, pp. 25–42, Springer, 2012.
35. M. Green, S. Hohenberger. Universally Composable Adaptive Oblivious Transfer. In *Asiacrypt'06*, *LNCS* 5350, pp. 179–197. Springer, 2006.
36. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In *Eurocrypt'06*, *LNCS* 4004, pp. 339–358. Springer, 2006.
37. J. Groth. Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures. In *Asiacrypt'06*, *LNCS* 4284, pp. 444–459, Springer, 2006.
38. J. Groth. Fully anonymous group signatures without random oracles. In *Asiacrypt'07*, *LNCS* 4833, pp. 164–180. Springer, 2007.
39. J. Groth, A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *Eurocrypt'08*, LNCS 4965, pp. 415–432, 2008.
40. D. Hofheinz, T. Jager. Tightly Secure Signatures and Public-Key Encryption. In *Crypto'12*, *LNCS* 7417, pp. 590–607, 2012.
41. B. Hemenway, B. Libert, R. Ostrovsky, D. Vergnaud. Lossy Encryption: Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security. In *Asiacrypt'11*, LNCS 7073, pp. 70–88, 2011.
42. C. Jutla, A. Roy. Relatively-Sound NIZKs and Password-Based Key-Exchange. In *PKC'12*, *LNCS* 7293, pp. 485–503, 2012.
43. C. Jutla, A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In *Asiacrypt '13*, LNCS 8269, pp. 1–20, Springer, 2013.
44. C. Jutla, A. Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In *Crypto '14*, LNCS 8617, pp. 295–312, Springer, 2014.
45. A. Kiayias, M. Yung. Secure scalable group signature with dynamic joins and separable authorities. International Journal of Security and Networks (IJSN) Vol. 1, No. 1/2, pp. 24–45, 2006.
46. E. Kiltz, A. Mityagin, S. Panjwani, B. Raghavan. Append-Only Signatures. In *ICALP'05*, LNCS 3580, pp. 434–445, 2005.
47. E. Kiltz. Chosen-ciphertext security from tag-based encryption. In *TCC'06*, *LNCS* 3876, pp. 581–600, 2006.
48. E. Kiltz, J. Pan, H. Wee. Structure-Preserving Signatures from Standard Assumptions, Revisited. In *Crypto'15*, *LNCS* series, 2015.
49. H. Krawczyk and T. Rabin. Chameleon signatures. In *NDSS'00*, 2000.
50. B. Libert, T. Peters, M. Joye, M. Yung. Linearly homomorphic structure-preserving signatures and their applications. In *Crypto '13*, LNCS 8043, pp. 289–307, Springer, 2013.
51. B. Libert, T. Peters, M. Joye, M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In *Eurocrypt '14*, LNCS 8441, pp. 514–532, Springer, 2014.
52. P. MacKenzie, M. Reiter, K. Yang. Alternatives to Non-malleability: Definitions, Constructions, and Applications. In *TCC'04*, LNCS 2951, pp. 171–190, 2004.
53. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Crypto'84*, *LNCS* 196, pp. 47–53, 1984.
54. V. Shoup. A proposal for an ISO standard for public key encryption. Manuscript, December 20, 2001.
55. B. Waters. Efficient identity-based encryption without random oracles. In *Eurocrypt'05*, *LNCS* 3494, pp. 114–127. Springer, 2005.
56. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *Crypto '09*, LNCS 5677, pp. 619–636, Springer, 2009.