

TYPE 2 STRUCTURE-PRESERVING SIGNATURE SCHEMES REVISITED

SANJIT CHATTERJEE AND ALFRED MENEZES

ABSTRACT. At CRYPTO 2014, Abe et al. presented generic-signer structure-preserving signature schemes using Type 2 pairings. According to the authors, the proposed constructions are optimal with only two group elements in each signature and just one verification equation. The schemes beat the known lower bounds in the Type 3 setting and thereby establish that the Type 2 setting permits construction of cryptographic schemes with unique properties not achievable in Type 3.

In this paper we undertake a concrete analysis of the Abe et al. claims. By properly accounting for the actual structure of the underlying groups and subgroup membership testing of group elements in signatures, we show that the schemes are not as efficient as claimed. We present natural Type 3 analogues of the Type 2 schemes, and show that the Type 3 schemes are superior to their Type 2 counterparts in every aspect. We also formally establish that in the concrete mathematical structure of asymmetric pairing, *all* Type 2 structure-preserving signature schemes can be converted to the Type 3 setting without any penalty in security or efficiency, and show that the converse is false. Furthermore, we prove that the Type 2 setting does not allow one to circumvent the known lower bound result for the Type 3 setting. Our analysis puts the optimality claims for Type 2 structure-preserving signature in a concrete perspective and indicates an incompleteness in the definition of a generic bilinear group in the Type 2 setting.

1. INTRODUCTION

The terms ‘Type 2’ and ‘Type 3’ pairings were introduced by Galbraith, Paterson and Smart [16]. A bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ defined over prime-order groups is called Type 2 or Type 3 depending on whether or not an efficiently computable isomorphism from \mathbb{G}_2 to \mathbb{G}_1 is known. Their aptly titled paper “Pairings for cryptographers” begins with the observation that many research papers treat pairings as a “black box” and then develop schemes that “may not be realizable in practice, or may not be as efficient as the authors assume”. A similar concern constitutes the central focus of the current work.

The term ‘structure-preserving signature’ (SPS) was coined in 2010 by Abe et al. [1] but such constructions existed even before (see, e.g., Groth [18]). These pairing-based signature schemes have the property that verification keys, messages, and signatures are all group elements. Moreover, signatures are verified by testing the equality of products of pairings of group elements; each such equality is called a product-of-pairings equation (PPE).

Unlike a standard digital signature, the *raison d’être* for an SPS is not as a stand-alone scheme, but rather in the modular design of cryptographic protocols. They have been used in numerous cryptographic protocols (see [4] for a list). One of the primary reasons for the popularity of SPS schemes in protocol design is that they are fully compatible with

the well-known Groth-Sahai (GS) constructions of pairing-based non-interactive witness-indistinguishable (NIWI) and non-interactive zero-knowledge (NIZK) proof systems [19].

In typical applications of structure-preserving signature schemes when used in conjunction with, say, GS proofs, a party has a signed message and wishes to convince a second party (the verifier) that it possesses the (valid) signed message without revealing the message or the signature.¹ Groth-Sahai NIWI and NIZK proofs allow a party (the prover) to convince a second party (the verifier) that it possesses a solution to a collection of PPEs. The complexity of verifying a GS proof is heavily dependent on the number of group elements in the signature and the number of PPEs in signature verification (see [11, §3.4]).

It is important to keep the above perspective in mind when investigating optimal constructions of structure-preserving signatures. In other words, having an optimal construction in terms of signature size (number of group elements) and verification complexity (number of PPEs and pairings) is useful for a protocol designer who cares for the *concrete* efficiency of a protocol designed on top of a structure-preserving signature. In contrast, if (at all) a structure-preserving signature finds application as a stand-alone primitive, then the high cost of pairing-based verifications can be easily mitigated by batching [10, 15]. As can be expected, we have witnessed significant research to design structure-preserving signature schemes with the smallest possible number of group elements in a signature and with the smallest possible number of PPEs in signature verification (and recently, with the smallest possible number of pairings [9]).

Previous work. At CRYPTO 2011, Abe et al. [2] presented a strongly secure SPS using Type 3 pairings. Verification has two PPEs, which was proven to be optimal in the sense that any Type 3 structure-preserving signature scheme with verification having a single PPE was shown to succumb to a random message attack. Moreover, signatures are comprised of three group elements, which was also shown to be optimal. In their lower bound results Abe et al. [2] used the notion of a ‘generic signer’. A generic signer has access only to generic group operations and the same notion was used in later works including [4, 9] to prove lower bound results.

At TCC 2014, Abe et al. [3] extended the aforementioned optimality results to the Type 1 setting, thereby unifying the Type 1 and 3 settings. They also proposed a selectively randomizable SPS which is optimal in terms of signature size and verification complexity in both Type 1 and 3 settings.

At CRYPTO 2014, Abe et al. [4] continued their investigation of structure-preserving signature schemes in the Type 2 setting. They presented a strongly unforgeable structure-preserving signature scheme and a randomizable structure-preserving signature scheme using Type 2 pairings. Both schemes are claimed to have signatures that are comprised of only two group elements, have only one PPE in signature verification, and were proven secure in the generic group model for Type 2 pairings. The authors conclude that their schemes enjoy the smallest signature (in terms of number of group elements) and fastest signature verification. Furthermore, they claimed that their constructions in Type 2 are optimal in terms of signature size, number of verification equations and verification key (see Table 1

¹We use the example of GS because many applications of structure-preserving signature schemes are in conjunction with such non-interactive proof systems. However, structure-preserving signatures are combined with other primitives too – see the work of Hanser and Slamanig [20].

of [4]). In light of the aforementioned lower bounds on the number of group elements in signatures and the number of PPEs in signature verification for Type 3 structure-preserving signature schemes, they conclude that the Type 2 schemes have no analogues in the Type 3 setting. According to the authors [4]: “This is significant from a high level pairing-based cryptography perspective, as it provides a concrete example of a property that can be obtained in the Type 2 setting but not in the other settings.” This is contrary to the arguments presented in [13] that any cryptographic protocol that employs Type 2 pairings has a natural counterpart in the Type 3 setting that does not suffer any loss in functionality, security or efficiency.

In a follow-up work, Barthe et al. [9] establish lower bounds on the number of pairings in the Type 2 setting. Using an automated tool they devise structure-preserving signatures that are ‘strongly-optimal’ – having one verification equation and minimum number of pairings in the Type 2 setting.

Concrete differences between Type 2 and Type 3 pairings. Abe et al. [4] use the notion of ‘generic algorithms’ in their results that establish the claimed superiority of Type 2 setting for SPS. A bilinear group generator \mathcal{G} is abstractly defined which takes input a security parameter and returns the descriptions of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ along with an efficiently-computable isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$. In their abstraction all the relevant operations over $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ such as subgroup membership, computing group operations, and evaluating the maps ψ and e are treated as “black-box”. Such an abstraction is useful *provided* it is able to capture all the essential properties of the concrete mathematical structure over which a Type 2 pairing is defined.

Type 2 and Type 3 pairings are concretely defined over certain elliptic curve groups [16]. As first pointed out in [16] and elaborated further in [13], each setting is constrained by the underlying mathematical structure. For example, no efficient method is known for hashing onto \mathbb{G}_2 in Type 2, whereas the isomorphism ψ , even though it exists in a mathematical sense, is not known to be efficiently computable in the Type 3 setting. Similarly, the structure of \mathbb{G}_2 in the Type 2 setting requires the evaluation of two pairings in subgroup membership tests for \mathbb{G}_2 . All these are deemed to be *necessary* assumptions in the asymmetric pairing setting that a protocol designer needs to keep in mind if s/he is concerned with concrete instantiation of protocols in the real world.

Our contributions. To critically evaluate the claimed advantages of Type 2 structure-preserving signature schemes, we deconstruct the Abe et al. proposals [4] in terms of the underlying concrete group structures. We show that the analysis of the Type 2 generic-signer structure-preserving signature schemes in [4] neglected to account for the concrete group structure and subgroup membership testing of group elements in a signature, leading to erroneous conclusions. Incorporating these subgroup membership tests into the signature verification increases the number of group elements in signatures and also increases the number of PPEs in signature verification. Next we examine whether the pairing-based subgroup membership tests can be discounted as verification equations when the signature scheme is composed with the Groth-Sahai proof system. Recall that such a modular composition is the primary motivation for structure-preserving signatures. Our analysis establishes that not all these pairing-based verifications can be dispensed with when the signature scheme is composed with such a proof system.

Furthermore, since GS proofs in the Type 2 setting are more costly than in the Type 3 setting, the Type 2 schemes are not as efficient as claimed in [4] in the stand-alone setting and significantly slower when composed with GS proofs. In support of this claim, two examples of Groth-Sahai NIWI proofs for verifying that the prover possesses a solution (X, Y) to the equation $e(A, X) \cdot e(B, Y) = t$ where e is a Type 2 or a Type 3 pairing are given in Appendix A. We present natural Type 3 analogues of the Type 2 schemes, and show that the Type 3 schemes are superior to their Type 2 counterparts in all aspects.

Continuing the process of deconstruction, we formally show that *all* Type 2 generic-signer structure-preserving signature schemes can be converted to Type 3 without any penalty in security and efficiency, but not all Type 3 schemes have a secure Type 2 counterpart. Further, we exhibit the impossibility of having a single pairing-based verification equation in the Type 2 setting even when messages are drawn from \mathbb{G}_2 and thereby put the lower bound results of [4] in the correct perspective. Our results demonstrate that any Type 2 structure-preserving signature scheme is merely an inefficient implementation of a corresponding Type 3 scheme. The claim of superiority of the Type 2 setting over Type 3 stems from an incomplete abstraction of the Type 2 setting in [4].

Organization. The remainder of the paper is organized as follows. In §2 we summarize the salient differences between Type 2 and Type 3 pairings derived from elliptic curves having even embedding degrees. In §3 we explain why, contrary to the claims, the strongly unforgeable structure-preserving signature scheme in [4] actually has signatures comprising of three group elements and has two PPEs in signature verification. We present a natural analogue of the scheme in the Type 3 setting, and show that it is more efficient than the Type 2 scheme. In §4, we present our Type 3 analogue of the Type 2 randomizable structure-preserving signature scheme in [4], and show that the Type 3 scheme is more efficient. In §5, we present our conversion framework for generic-signer structure-preserving signature schemes from the Type 2 setting to the Type 3 setting, the separation between Types 2 and 3, and the impossibility of having a single pairing-based verification equation in the Type 2 setting. We draw our conclusions in §6. Two instances of Groth-Sahai NIWI proofs in the Type 2 and Type 3 settings are given in Appendix A. The definitions of structure-preserving signatures and their security are reproduced in Appendix B.

2. ASYMMETRIC BILINEAR PAIRINGS

Let \mathbb{F}_q be a finite field of characteristic $p \geq 5$, and let E be an ordinary elliptic curve defined over \mathbb{F}_q . Let n be a prime divisor of $\#E(\mathbb{F}_q)$ satisfying $\gcd(n, q) = 1$, and let k (the embedding degree) be the smallest positive integer such that $n \mid q^k - 1$. We will henceforth assume that k is even, since then some important speedups in pairing computations are applicable [7]. Some prominent families of elliptic curves with even embedding degree include the MNT [23], BN [8], KSS [22], and BLS [6] curves.

Since $k > 1$, we have $E[n] \subseteq E(\mathbb{F}_{q^k})$ where $E[n]$ denotes the n -torsion group of E . Let $G \in E(\mathbb{F}_q)[n]$ be an \mathbb{F}_q -rational point of order n , and define $\mathbb{G}_1 = \langle G \rangle$. Let \mathbb{G}_T denote the order- n subgroup of the multiplicative subgroup of \mathbb{F}_{q^k} .

2.1. Type 3 pairings. Following [16], we denote by D the CM discriminant of E and set $e = \gcd(k, 6)$ if $D = -3$, $e = \gcd(k, 4)$ if $D = -4$, $e = 2$ if $D < -4$, and $d = k/e$. For

example, BN curves have $k = 12$, $e = 6$ and $d = 2$, whereas MNT curves have $k = 6$, $e = 2$ and $d = 3$. Now, E has a unique degree- e twist \tilde{E} defined over \mathbb{F}_{q^d} such that $n \mid \#\tilde{E}(\mathbb{F}_{q^d})$ [21]. Let $\tilde{I} \in \tilde{E}(\mathbb{F}_{q^d})$ be a point of order n , and let $\tilde{\mathbb{G}}_3 = \langle \tilde{I} \rangle$. Then there is a monomorphism $\phi : \tilde{\mathbb{G}}_3 \rightarrow E(\mathbb{F}_{q^k})$ such that $I = \phi(\tilde{I}) \notin \mathbb{G}_1$. The group $\mathbb{G}_3 = \langle I \rangle$ is the Trace-0 subgroup of $E[n]$, so named because it consists of all points $P \in E[n]$ for which $\text{Tr}(P) = \sum_{i=0}^{k-1} \pi^i(P) = \infty$, where π denotes the q -th power Frobenius. The monomorphism ϕ can be defined so that $\phi : \tilde{\mathbb{G}}_3 \rightarrow \mathbb{G}_3$ can be efficiently computed in both directions; therefore we can identify $\tilde{\mathbb{G}}_3$ and \mathbb{G}_3 , and consequently the elements of \mathbb{G}_3 can be viewed as having coordinates in \mathbb{F}_{q^d} (instead of in the larger field \mathbb{F}_{q^k}).

Non-degenerate bilinear pairings $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \rightarrow \mathbb{G}_T$ are said to be of Type 3 because no efficiently-computable isomorphisms from \mathbb{G}_1 to \mathbb{G}_3 or from \mathbb{G}_3 to \mathbb{G}_1 are known [16]. There are several Type 3 pairings, of which the most efficient is Vercauteren's optimal pairing [24].

2.2. Type 2 pairings. Let $H \in E[n]$ with $H \notin \mathbb{G}_1$ and $H \notin \mathbb{G}_3$. Then $\mathbb{G}_2 = \langle H \rangle$ is an order- n subgroup of $E(\mathbb{F}_{q^k})$ with $\mathbb{G}_2 \neq \mathbb{G}_1$ and $\mathbb{G}_2 \neq \mathbb{G}_3$. Non-degenerate bilinear pairings $e_2 : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ are said to be of Type 2 because the map Tr is an efficiently-computable isomorphism from \mathbb{G}_2 to \mathbb{G}_1 ; note, however, that no efficiently-computable isomorphism from \mathbb{G}_1 to \mathbb{G}_2 is known. These pairings have the property that hashing onto \mathbb{G}_2 is infeasible (other than by multiplying H by a randomly selected integer).

The computation of e_2 is efficiently reduced to the task of computing Type 3 pairing e_3 [16]. Thus, the costs of computing e_2 and e_3 are approximately equal. To see this, define the maps $\psi : E[n] \rightarrow \mathbb{G}_1$, $Q \mapsto \frac{1}{k} \text{Tr}(Q)$ and $\rho : E[n] \rightarrow \mathbb{G}_3$, $Q \mapsto Q - \psi(Q)$. Recall that e_2 and e_3 are restrictions of the (reduced) Tate pairing $\hat{e} : E[n] \times E[n] \rightarrow \mathbb{G}_T$. Hence, for all $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, we have

$$(1) \quad e_2(P, Q) = \hat{e}(P, \psi(Q)) \cdot \hat{e}(P, \rho(Q)) = \hat{e}(P, \rho(Q)) = e_3(P, \rho(Q)).$$

Remark 1. Note that the Type 2 setting is equipped with not only the map $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ but also the map $\rho : \mathbb{G}_2 \rightarrow \mathbb{G}_3$. The abstract definition of the Type 2 setting, e.g., in [4], does not capture the latter. However, as we show in the following sections, the map ρ plays a crucial role for a comparative study of the protocols in the Type 2 and Type 3 settings.

2.3. Comparing the performance of Type 2 and Type 3 pairings. Since points in \mathbb{G}_2 have coordinates in \mathbb{F}_{q^k} whereas points in \mathbb{G}_3 have coordinates in the proper subfield \mathbb{F}_{q^d} , it would appear that the ratio of the bitlengths of points in \mathbb{G}_2 and \mathbb{G}_3 is k/d . Similarly, the ratio of the costs of addition in \mathbb{G}_2 and \mathbb{G}_3 can be expected to be k^2/d^2 bit operations (using naive methods for extension field arithmetic). These ratios are given in Table 3 of [16]. However, as observed in [12], points in \mathbb{G}_2 have a shorter representation which we describe next. We emphasize that this representation can be used for *all* order- n subgroups \mathbb{G}_2 of $E[n]$ different from \mathbb{G}_1 and \mathbb{G}_3 .

Let H be an arbitrary point from $E[n] \setminus (\mathbb{G}_1 \cup \mathbb{G}_3)$, and set $\mathbb{G}_2 = \langle H \rangle$. Define $G = \frac{1}{k} \text{Tr}(H)$ so that the map ψ restricted to \mathbb{G}_2 is an efficiently-computable isomorphism from \mathbb{G}_2 to \mathbb{G}_1 with $\psi(H) = G$. Finally, set $I = H - G$. Then $I \in \mathbb{G}_3$ and the map ρ restricted to \mathbb{G}_2 is an efficiently-computable isomorphism from \mathbb{G}_2 to \mathbb{G}_3 with $\rho(H) = I$.

Now, given a point $Q \in E[n]$, one can efficiently determine the unique points $Q_1 \in \mathbb{G}_1$ and $Q_2 \in \mathbb{G}_3$ such that $Q = Q_1 + Q_2$; namely, $Q_1 = \psi(Q)$ and $Q_2 = \rho(Q) = Q - Q_1$.

Writing $D(Q) = (\psi(Q), \rho(Q))$ and letting $\mathbb{H}_2 \subseteq \mathbb{G}_1 \times \mathbb{G}_3$ denote the range of D applied to \mathbb{G}_2 , we have an efficiently-computable isomorphism $D : \mathbb{G}_2 \rightarrow \mathbb{H}_2$ whose inverse is also efficiently computable. Hence, without loss of generality, points $Q \in \mathbb{G}_2$ can be represented by a pair of points (Q_1, Q_2) with $Q_1 \in \mathbb{G}_1$ and $Q_2 \in \mathbb{G}_3$. Note that arithmetic in \mathbb{G}_2 with this representation is component-wise. Thus the ratio of the bitlengths of points in \mathbb{G}_2 and \mathbb{G}_3 is in fact $(d+1)/d$, whereas the ratio of the costs of addition in \mathbb{G}_2 and \mathbb{G}_3 is $(d^2+1)/d^2$. We also have the following simple condition for determining membership of a point $Q \in E[n]$ in \mathbb{G}_2 .

Lemma 1. *Let $Q \in E[n]$, and let $Q_1 = \psi(Q)$ and $Q_2 = \rho(Q)$. Then $Q \in \mathbb{G}_2$ if and only if $\log_G Q_1 = \log_I Q_2$.*

Proof. Suppose that $Q \in \mathbb{G}_2$, so $Q = \ell H$ for some $\ell \in [0, n-1]$. Then $Q = \ell(G+I) = \ell G + \ell I$. Thus $Q_1 = \ell G$ and $Q_2 = \ell I$, whence $\log_G Q_1 = \log_I Q_2$. The converse is similar. \square

Table 2 of [12] lists the costs of performing basic operations in \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_3 for a particular BN curve. The table confirms the expectation that basic operations in \mathbb{G}_2 are only marginally more expensive than the operations in \mathbb{G}_3 . One notable exception is that testing membership in \mathbb{G}_2 is several times more expensive than testing membership in \mathbb{G}_1 and \mathbb{G}_3 . To see this, let us consider the case of BN curves E defined over \mathbb{F}_q where q and $n = \#E(\mathbb{F}_q)$ are prime; recall that these curves have embedding degree $k = 12$ and $d = 2$. Testing membership of a point Q in \mathbb{G}_1 is very efficient, and simply entails verifying that Q has coordinates in \mathbb{F}_q and satisfies the equation that defines the curve, i.e., $Q \in E(\mathbb{F}_q)$. Testing membership of a point Q in \mathbb{G}_3 involves a fast check that $\phi^{-1}(Q)$ is in $\tilde{E}(\mathbb{F}_{q^2})$, followed by an exponentiation to verify that $nQ = \infty$. Testing membership in \mathbb{G}_2 is more costly since the known methods require two pairing computations. If the shorter representation (as elements of $\mathbb{G}_1 \times \mathbb{G}_3$) is used for \mathbb{G}_2 then, by Lemma 1, membership of (Q_1, Q_2) in \mathbb{G}_2 can be determined by first checking that $Q_1 \in \mathbb{G}_1$ and $Q_2 \in \mathbb{G}_3$, and then verifying that $e_3(Q_1, I) = e_3(G, Q_2)$ [14]. If the longer representation (as elements of $E(\mathbb{F}_{q^{12}})$) is used for \mathbb{G}_2 , then membership of Q in \mathbb{G}_2 can be determined by first checking that $Q \in E(\mathbb{F}_{q^{12}})$ and $nQ = \infty$, and then verifying that $e_2(\psi(Q), H) = e_2(G, Q)$.

Remark 2. Unlike \mathbb{G}_1 and \mathbb{G}_3 , the group \mathbb{G}_2 does not have any special structure, and all the $n-1$ order- n subgroups of $E[n]$ other than \mathbb{G}_1 and \mathbb{G}_3 are candidates for \mathbb{G}_2 . Subgroup membership testing in \mathbb{G}_2 is costly because given any arbitrary point Q , the task is to decide whether (i) $Q \in E[n]$ and then whether (ii) $\psi(Q)$ and $\rho(Q)$ have the same discrete log with respect to the generators G and I . Thus a pairing-based verification is assumed to be necessary for a subgroup membership test for \mathbb{G}_2 (unless one knows some other efficient method for testing equality of discrete logarithms in \mathbb{G}_1 and \mathbb{G}_2 , e.g., by solving the discrete logarithm problem in \mathbb{G}_1 or \mathbb{G}_2). As the primary focus of our work is a concrete comparative study of structure-preserving signatures in Types 2 and 3, in the remainder of the paper we perform our analysis based on this reasonable assumption. However, for the sake of completeness, in Remark 5 we comment on why none of the superiority claims [4] of Type 2 structure-preserving signatures over Type 3 will hold even in the hypothetical scenario where an efficient subgroup membership testing in \mathbb{G}_2 that does not require pairing computation is discovered.

2.4. A case for concrete treatment. Protocol designers usually assume the existence of a bilinear group generator which given a security parameter generates the relevant group descriptions and the bilinear map. This abstraction filters out the interconnection between Type 2 and 3 settings. For example, the existing generic definition of Type 2 pairings is oblivious to the fact that both Type 2 and 3 pairings can be defined over the same elliptic curve and are restrictions of the same function to different subgroups.

In contrast, comparative studies of Type 2 and Type 3 setting, as initiated in [16] or in follow-up works such as [13], are in the concrete security setting. In fact Galbraith et al. noted that the existence of a polynomial-time bilinear group generator assumed in the asymptotic treatment is not always automatic (see §2.1 of [16]), although it is not a problem in practice as one can efficiently generate a bilinear group description for any concrete security level of interest. For example, the BN family is optimized for the 128-bit security level and the notion of asymptotic security cannot be used in a meaningful way when the underlying pairing is derived from such family of curves.

In particular, when efficiency is being studied one cannot meaningfully distinguish between the Type 2 and Type 3 settings in the asymptotic sense. Clearly, it's the concrete efficiency (e.g., the number of group elements in a signature or the number of PPEs and pairings in verification) that Abe et al. [4] and Barthe et al. [9] are concerned with when they discuss the efficiency or optimality of their constructions of structure-preserving signature in the Type 2 setting.

Thus the focus here, as in [16, 13], is on concrete security (along with functionality and efficiency) in the Type 2 and 3 settings. The Type 2 and 3 pairings (i.e., e_2 and e_3) are defined as restrictions of the (reduced) Tate pairing. In the performance comparison above we used the example of BN curves as they yield the most efficient pairings at the 128-bit security level. However, we note that our observations are without loss of generality and apply equally well to asymmetric pairings derived from other prominent families of elliptic curves such as MNT, KS and BLS. Readers are referred to Galbraith et al. [16] for a more general comparative treatment of the Type 2 and 3 settings including a discussion on the high cost of group membership testing for \mathbb{G}_2 in the Type 2 setting.²

In §§3–5, we use multiplicative notation for elements of \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_3 .

3. STRONGLY UNFORGEABLE STRUCTURE-PRESERVING SIGNATURES

We present the Type 2 strongly unforgeable SPS from [4] and our Type 3 analogue of it. The Type 3 scheme was obtained by following the general recipe given in [13] for converting a protocol from the Type 2 to the Type 3 setting.

3.1. Type 2 strongly unforgeable SPS [4].

- (1) *Setup.* Let $e_2 : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ be a Type 2 pairing where \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T have order n ; G , H are fixed generators of \mathbb{G}_1 , \mathbb{G}_2 , respectively.

²Since this is how Type 2 and Type 3 pairings are currently defined, any concrete efficiency/security treatment must be based on that existing knowledge. No comparative study or claim of superiority of one setting over another will make sense based on hitherto undiscovered mathematical structure. If there is a completely new way to define Type 2 and Type 3 pairings in the future, then of course that will mandate a new concrete analysis of *all* asymmetric pairing-based protocols.

- (2) *Key generation.* The secret key is $v, w \in_R [1, n-1]$. The public key is (V, W) where $V = G^v$ and $W = G^w$.
- (3) *Signature generation.* To sign $M \in \mathbb{G}_2$, select $t \in_R [1, n-1]$ and compute $R = H^{t-w}$ and $S = M^{v/t} H^{1/t}$. The signature on M is (R, S) .
- (4) *Signature verification.* To verify a signed message $(M, (R, S))$, check that (a) $M, R, S \in \mathbb{G}_2$; and (b) $e_2(W\psi(R), S) = e_2(V, M) \cdot e_2(G, H)$.

In [4, Theorem 2], the Type 2 scheme is proven strongly secure³ against generic forgers. Signatures are comprised of two \mathbb{G}_2 elements. Signature verification requires three \mathbb{G}_2 membership tests and one PPE verification.

3.2. Type 3 strongly unforgeable SPS.

- (1) *Setup.* Let $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \rightarrow \mathbb{G}_T$ be a Type 3 pairing where $\mathbb{G}_1, \mathbb{G}_3$ and \mathbb{G}_T have order n ; G, I are fixed generators of $\mathbb{G}_1, \mathbb{G}_3$, respectively.
- (2) *Key generation.* The secret key is $v, w \in_R [1, n-1]$. The public key is (V, W) where $V = G^v$ and $W = G^w$.
- (3) *Signature generation.* To sign $M \in \mathbb{G}_3$, select $t \in_R [1, n-1]$ and compute $R_1 = G^{t-w}$, $R_2 = I^{t-w}$, and $S = M^{v/t} I^{1/t}$. The signature on M is (R_1, R_2, S) .
- (4) *Signature verification.* To verify a signed message $(M, (R_1, R_2, S))$, check that
 - (a) $R_1 \in \mathbb{G}_1$ and $M, R_2, S \in \mathbb{G}_3$;
 - (b) $e_3(R_1, I) = e_3(G, R_2)$; and
 - (c) $e_3(WR_1, S) = e_3(V, M) \cdot e_3(G, I)$.

It is easy to verify correctness of the Type 3 signature scheme. The security proof given in [4, Theorem 2] that the Type 2 scheme is strongly secure against generic forgers also applies (with minimal changes) to the Type 3 signature scheme. The reason that the proof carries over with minimal changes is that we follow the strategy of [13] in the conversion. The Type 3 scheme is obtained by first replacing all \mathbb{G}_2 elements by the corresponding \mathbb{H}_2 elements and then discarding the redundant \mathbb{G}_1 elements that are not used either in the construction or in security argument in the Type 2 setting.

Signatures for the Type 3 scheme are comprised of one \mathbb{G}_1 element and two \mathbb{G}_3 elements. Signature verification requires one \mathbb{G}_1 membership test, three \mathbb{G}_3 membership tests, and two PPE verifications.

We note that the verification step 4(b) of the Type 3 scheme cannot be omitted. Indeed, if this step is omitted then the scheme succumbs to the following key-only attack: $(1, (W^{-1}G, 1, I))$ is a valid forgery. Moreover, even if the message $M = 1$ is disallowed, the scheme succumbs to the following random message attack. The forger first obtains a signed message $(M, (R_1, R_2, S))$. It then computes $M' = MS^{-1}$ and $R'_1 = R_1V^{-1}$, thereby obtaining a valid forgery $(M', (R'_1, R_2, S))$. We note that this attack is anticipated by the proof of Theorem 2 in [2] which establishes that any Type 3 structure-preserving signature scheme with a single verification equation is existentially forgeable under random message attack.

³A signature scheme is said to be *secure* if it is existentially unforgeable under chosen-message attack. If, in addition, it is infeasible to find a new signature for a message that has already been signed, then the signature scheme is said to be *strongly secure*.

3.3. Comparisons.

3.3.1. *Signature size.* Signatures in the Type 2 scheme are comprised of two \mathbb{G}_2 elements or, equivalently, two \mathbb{G}_1 and two \mathbb{G}_3 elements. Thus, signatures in the Type 3 scheme are smaller than signatures in the Type 2 scheme.

3.3.2. *Signature generation cost.* In signature generation, computing $R = H^{t-w}$ for the Type 2 scheme has exactly the same cost as computing $R_1 = G^{t-w}$ and $R_2 = I^{t-w}$ for the Type 3 scheme. However, the computation of $S = M^{v/t}H^{1/t}$ in the Type 2 scheme is significantly slower than in the Type 3 scheme since the computation takes place in \mathbb{G}_2 in the former and in \mathbb{G}_3 in the latter. Thus, signature generation is slower in the Type 2 scheme than in the Type 3 scheme.

3.3.3. *Signature verification cost.* Signature verification in the Type 2 scheme is significantly slower than in the Type 3 scheme. This is because, as explained in §2.3, the subgroup membership tests $M, R, S \in \mathbb{G}_2$ required in the Type 2 scheme each requires the verification of a PPE, whereas the subgroup membership tests $R_1 \in \mathbb{G}_1$ and $M, R_2, S \in \mathbb{G}_3$ in the Type 3 scheme are relatively inexpensive. Thus, signature verification in the Type 2 scheme requires *four* PPE verifications, whereas only *two* are needed in the Type 3 scheme. Note that the high cost of PPE verifications can be mitigated by batching [10, 15].

The costly subgroup membership tests in step 4(a) of the Type 2 scheme cannot be omitted for two reasons. First, if these tests are omitted then the security proof given in [4] is no longer applicable since the proof makes the assumption that $M, R, S \in \mathbb{G}_2$. Second, and more importantly, there are attacks on the scheme if the membership tests are omitted. For example, given a valid signed message $(M, (R, S))$, one can easily⁴ select a second point $R' \in E[n]$ with $R' \neq R$ and $\psi(R') = \psi(R)$, thereby obtaining a second valid signed message $(M, (R', S))$. Similarly, given $(M, (R, S))$ one can obtain a second valid signed message $(M', (R, S))$ or $(M, (R, S'))$ if membership tests for M or S are omitted.

3.3.4. *Cost of signature verification with Groth-Sahai proofs.* SPS schemes were not designed to be used as stand-alone primitives, but rather in conjunction with non-interactive proof systems like Groth-Sahai as explained in §1. Suppose that Groth-Sahai proof verification always requires subgroup membership tests for the group elements in commitment and proof as described in Appendix A. Now the pertinent question is whether in Type 2 it is possible to give a proof for a single PPE as opposed to two PPEs in Type 3. This may give some advantage to the Type 2 scheme because the cost of a Groth-Sahai proof depends heavily on the number of PPEs in signature verification.

Consider the Type 2 signature scheme of Abe et al. when used in conjunction with a Groth-Sahai proof. The prover provides a commitment of $(M, (R, S))$ together with a proof that the committed values satisfy the following PPE:

$$(2) \quad e_2(W\psi(R), S) = e_2(V, M) \cdot e_2(G, H).$$

In this proof system, the group elements G, H, V and W are known to the verifier, whereas the variables are $M, R, S \in \mathbb{G}_2$. However, since Groth-Sahai proofs do not have a mechanism for incorporating the evaluation of $\psi(R)$, the variables in (2) are actually $M, \psi(R)$ and S .

⁴Given $R \in \mathbb{G}_2$, one computes $R_1 = \psi(R)$ and selects arbitrary $R'_2 \in \mathbb{G}_3$ with $R'_2 \neq R \cdot R_1^{-1}$. Then $R' = R_1 \cdot R'_2$ satisfies $\psi(R') = R_1$ and $R' \neq R$.

In other words, a Groth-Sahai proof for (2) only convinces a verifier that the prover knows $R_1 \in \mathbb{G}_1$ and $M, S \in \mathbb{G}_2$ that satisfy the following PPE:

$$(3) \quad e_2(WR_1, S) = e_2(V, M) \cdot e_2(G, H).$$

In particular, the proof does *not* establish that the prover knows $R \in \mathbb{G}_2$ such that $R_1 = \psi(R)$. As we have shown above, unless the prover establishes that s/he knows $R \in \mathbb{G}_2$ which has the same discrete logarithm to the base $H \in \mathbb{G}_2$ as R_1 to the base $G \in \mathbb{G}_1$, the signature scheme is insecure, i.e., not (strongly) unforgeable. Thus, as per the Groth-Sahai proof system, the prover needs to convince the verifier that it possesses a solution (M, R_1, R, S) to the following collection of PPEs:

$$(4) \quad e_2(WR_1, S) = e_2(V, M) \cdot e_2(G, H)$$

$$(5) \quad e_2(R_1, H) = e_2(G, R).$$

When composed with Groth-Sahai proof systems, the verification now has *two* PPEs (note that batching does not work in this scenario). This is in contrast to the claim made in [4] that the Type 2 signature scheme of §3.1 has only *one* PPE. Moreover, in addition to R, S , the prover has to commit to R_1 in the Groth-Sahai proof. So when composed with Groth-Sahai, signatures are comprised of *three* group elements, i.e., $R_1 \in \mathbb{G}_1$ must be included in the signature along with $R, S \in \mathbb{G}_2$.

Recall that the Type 3 signature scheme in §3.2 also has two PPEs in verification and signatures that are comprised of three group elements. Thus, it might appear at first glance that signature verification for the Type 2 and Type 3 schemes costs roughly the same when used in conjunction with Groth-Sahai proofs. However, the Groth-Sahai proofs for the Type 2 setting are based on hardness of the decisional linear (DLIN) problem in \mathbb{G}_2 [17], whereas Groth-Sahai proofs for the Type 3 setting can be based on hardness of the decisional Diffie-Hellman (DDH) problem in \mathbb{G}_1 and \mathbb{G}_3 [19]. Now, DLIN-based Groth-Sahai proofs are significantly more costly than DDH-based Groth-Sahai proofs in terms of commitment size, proof size, and the total number of pairing computations in proof verification. For example, one can see that the DLIN-based proof of knowledge of a solution (X, Y) to the equation $e_2(A, X) \cdot e_2(B, Y) = t$ in Appendix A.1 is significantly more costly than the DDH-based proof of knowledge of a solution (X, Y) to the equation $e_3(A, X) \cdot e_3(B, Y) = t$ in Appendix A.2; see also the performance estimates given in §3.4 of [11]. Thus, the Type 2 structure-preserving signature scheme will be significantly slower than its Type 3 counterpart when combined with Groth-Sahai proofs.

3.3.5. Conclusions. The Type 3 strongly unforgeable structure-preserving signature scheme is superior to its Type 2 counterpart with respect to signature size, signature generation cost, and signature verification cost when the schemes are used as stand-alone signature schemes and when used in conjunction with Groth-Sahai proofs. Moreover, the schemes have similar security proofs against generic forgers. Thus, the Type 2 scheme offers no advantages over the Type 3 scheme.

4. RANDOMIZABLE STRUCTURE-PRESERVING SIGNATURES

We present the Type 2 randomizable structure-preserving signature scheme from [4] and our Type 3 analogue of it. The Type 3 scheme was obtained by following the general recipe given in [13] for converting a protocol from the Type 2 setting to the Type 3 setting.

4.1. Type 2 randomizable SPS [4].

- (1) *Setup.* Let $e_2 : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a Type 2 pairing where \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T have order n ; G, H are fixed generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively.
- (2) *Key generation.* The secret key is $v, w \in_R [1, n-1]$. The public key is (V, W) where $V = G^v$ and $W = G^w$.
- (3) *Signature generation.* To sign $M \in \mathbb{G}_2$, select $r \in_R [1, n-1]$ and compute $R = H^r$ and $S = M^v H^{r^2+w}$. The signature on M is (R, S) .
- (4) *Randomization.* To randomize $(M, (R, S))$, select $\alpha \in_R [1, n-1]$ and compute $R' = RH^\alpha$ and $S' = SR^{2\alpha} H^{\alpha^2}$. The randomized signature on M is (R', S') .
- (5) *Signature verification.* To verify a signed message $(M, (R, S))$, check that (a) $M, R, S \in \mathbb{G}_2$; and (b) $e_2(G, S) = e_2(V, M) \cdot e_2(\psi(R), R) \cdot e_2(W, H)$.

In [4, Theorem 1], the Type 2 scheme is proven secure against generic forgers. Signatures are comprised of two \mathbb{G}_2 elements. Signature verification requires three \mathbb{G}_2 membership tests and one PPE verification.

4.2. Type 3 randomizable SPS.

- (1) *Setup.* Let $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \rightarrow \mathbb{G}_T$ be a Type 3 pairing, where $\mathbb{G}_1, \mathbb{G}_3$ and \mathbb{G}_T have order n ; G, I are fixed generators of $\mathbb{G}_1, \mathbb{G}_3$, respectively.
- (2) *Key generation.* The secret key is $v, w \in_R [1, n-1]$. The public key is (V, W) where $V = G^v$ and $W = G^w$.
- (3) *Signature generation.* To sign $M \in \mathbb{G}_3$, select $r \in_R [1, n-1]$ and compute $R_1 = G^r$, $R_2 = I^r$ and $S = M^v I^{r^2+w}$. The signature on M is (R_1, R_2, S) .
- (4) *Randomization.* To randomize $(M, (R_1, R_2, S))$, select $\alpha \in_R [1, n-1]$ and compute $R'_1 = R_1 G^\alpha$, $R'_2 = R_2 I^\alpha$, and $S' = SR_2^{2\alpha} I^{\alpha^2}$. The randomized signature on M is (R'_1, R'_2, S') .
- (5) *Signature verification.* To verify a signed message $(M, (R_1, R_2, S))$, check that
 - (a) $R_1 \in \mathbb{G}_1$ and $M, R_2, S \in \mathbb{G}_3$;
 - (b) $e_3(R_1, I) = e_3(G, R_2)$; and
 - (c) $e_3(G, S) = e_3(V, M) \cdot e_3(R_1, R_2) \cdot e_3(W, I)$.

It is easy to verify correctness of the Type 3 scheme. Following the strategy outlined in §3.2, the security proof given in [4, Theorem 1] that the Type 2 scheme is secure against generic forgers can be modified (with minimal changes) for the Type 3 signature scheme.

Signatures for the Type 3 scheme are comprised of one \mathbb{G}_1 element and two \mathbb{G}_3 elements. Signature verification requires one \mathbb{G}_1 membership test, three \mathbb{G}_3 membership tests, and two PPE verifications.

We note that the verification equation in step 5(b) of the Type 3 scheme cannot be omitted. Indeed, if this step is omitted then the scheme succumbs to the following random message attack. The forger first obtains a signed message $(M, (R_1, R_2, S))$. It then computes

$M' = MR_2$ and $R'_1 = R_1V^{-1}$, thereby obtaining a valid forgery $(M', (R'_1, R_2, S))$. Indeed, this attack is anticipated by the proof of Theorem 2 of [2].

4.3. Comparisons. The subgroup membership tests performed in step 5(a) of the Type 2 randomizable structure-preserving signature scheme cannot be omitted. If they are, then an attacker can proceed as follows. Having obtained a valid message-signature pair $(M, (R, S))$, she computes $M' = MR$ and $R' = RV^{-1}$. Note that $\rho(R') = \rho(R)$. Then $(M', (R', S))$ is a valid signed message since the term $e_2(V, M) \cdot e_2(\psi(R), R)$ in step 5(b) of signature verification remains unchanged:

$$\begin{aligned} e_2(V, M') \cdot e_2(\psi(R'), R') &= e_2(V, MR) \cdot e_2(\psi(R) \cdot \psi(V^{-1}), R') \\ &= e_2(V, M) \cdot e_2(V, R) \cdot e_2(\psi(R), R') \cdot e_2(\psi(V), R')^{-1} \\ &= e_2(V, M) \cdot e_3(V, \rho(R)) \cdot e_3(\psi(R), \rho(R)) \cdot e_3(V, \rho(R))^{-1} \\ &= e_2(V, M) \cdot e_2(\psi(R), R). \end{aligned}$$

The comparisons made between the Type 2 and Type 3 strongly unforgeable structure-preserving signature schemes in §3.3 are also valid for the Type 2 and Type 3 randomizable structure-preserving signature schemes in §4.1 and §4.2. Namely, the Type 3 scheme has smaller signatures, faster signature generation, faster signature verification in stand-alone applications (since it requires the verification of two PPEs instead of four PPEs for the Type 2 scheme), and faster signature verification when used with Groth-Sahai proofs (since both schemes have two PPEs and three group elements in signatures, but the Type 3 proofs are DDH-based instead of DLIN-based).

As mentioned in [4], randomizable structure-preserving signature schemes are useful in building anonymization protocols because the signature component that is uniformly distributed and independent of the message can be revealed without leaking any information about the message or the original signature from which the randomized signature was derived. In the Type 2 randomizable signature scheme of §4.1, the signature component R can be made public. In that case, only the single PPE in step 5(b) of signature verification needs to be transformed when used in conjunction with Groth-Sahai proofs (and the PPE is of the form described in §A.1). Similarly, in the Type 3 randomizable signature scheme of §4.2, the signature components R_1 and R_2 can be made public. In that case, only the single PPE in step 5(c) of signature verification needs to be transformed when used in conjunction with Groth-Sahai proofs (and the PPE is of the form described in §A.2).

In both situations, i.e., whether the message-independent signature components are made public or not, the Type 3 scheme is superior in all respects to its Type 2 counterpart.

4.4. Strongly-optimal signatures. In a recent paper, Barthe et al. [9] investigated the optimal number of pairings for structure-preserving signature. The question is indeed well motivated as the Groth-Sahai proof complexity also depends on the number of pairings in each PPE. Barthe et al. work in the Type 2 setting as that supposedly allows a single PPE based verification and explicitly disregard the PPEs in group membership testing for \mathbb{G}_2 elements in the verification. This is justified by stating that such tests “may require an amortizable (aka offline) pairing computation in practical instantiation”. However, this is *not* a valid assumption, particularly when the main goal of [9] is to find a lower bound on the “concrete number of pairings” and optimal construction meeting that bound. As we have

already pointed out in the context of the Abe et al. constructions [4], one cannot in general ignore the pairing-based verification equations involved in \mathbb{G}_2 membership testing either in the stand-alone setting or in conjunction with Groth-Sahai proofs. It is also evident that these pairings cannot be treated as offline (and thereby, amortizable) since they involve message and/or signature elements.

Assuming that signature verification involves a single PPE, Barthe et al. [9] derive a lower bound of three pairings for CMA-secure construction and two pairings for RMA security in the generic Type 2 setting. They use an automated tool to obtain signature schemes matching these lower bounds which they term as “strongly optimal”. However, when their abstract construction is translated to the concrete Type 2 setting, then we see that the CMA-secure scheme actually requires *six* more additional pairings, none of which can be made offline. Incidentally, following the general recipe of [13], they also propose a Type 3 counterpart that requires a total of five pairings of which only three are online.

More interesting is the case of their RMA-secure construction in the Type 2 setting which is claimed to have only two online pairings, whereas in concrete terms six additional online pairings will be required. Now consider the scenario when this signature scheme is composed with Groth-Sahai proofs. Given a signature $(R, S) \in \mathbb{G}_2^2$ for $M \in \mathbb{G}_2$, their verification equation⁵ is of the form

$$e_2(\psi(S) \cdot W, H) = e(\psi(R) \cdot V, M).$$

As the scheme is randomizable, the message-independent random group element R in the signature can be revealed but not the signature element $S \in \mathbb{G}_2$. As we already pointed out in the context of the Abe et al. strongly-unforgeable signature, Groth-Sahai proofs do not have any mechanism for incorporating the evaluation of $\psi(S)$. Hence, the signature now has an additional component $\psi(S) \in \mathbb{G}_1$ and verification involves one additional PPE:

$$e_2(\psi(S), H) = e_2(G, S).$$

Clearly, the signature contains three group elements and verification involves four online pairings that need to be counted when the scheme is composed with a Groth-Sahai proof.

5. A CLOSER LOOK AT TYPE 2 SCHEMES

We first establish that *all* Type 2 generic-signer structure-preserving signature schemes can be transformed to the Type 3 setting without any penalty in security or efficiency.⁶ Next, we demonstrate the impossibility of having signature verification with a single pairing-product equation in the Type 2 setting when messages are drawn from \mathbb{G}_2 . Finally, we show a separation between the Type 2 and Type 3 settings by proposing a Type 3 signature scheme that has no secure Type 2 counterpart.

Based on the claimed optimality of their Type 2 schemes, Abe et al. [4] asserted that the Type 2 setting is different from Type 3 setting as it “permits the construction of cryptographic schemes with unique properties”. This, according to [4], settles the open question in [13] of whether all Type 2 schemes can be converted to the Type 3 setting with no efficiency

⁵We correct a typo in [9] where R is used in the equation.

⁶Our transformation uses the concrete (and only known) mathematical structure over which Type 2 and Type 3 pairings are defined. This concreteness does not cause the transformation to lose its generality since *any* Type 2 structure-preserving signature scheme can be converted using our framework.

loss. In contrast, the results of this section formally establish that *all* Type 2 generic-signer structure-preserving signature schemes are merely Type 3 schemes in disguise and cannot beat the established lower bound results even when messages are drawn from \mathbb{G}_2 .

5.1. Conversion from Type 2 to Type 3. Recall the definition of structure-preserving signatures (SPS) from [4, Definition 4]. Based on that definition, any generic-signer structure-preserving signature scheme with message space \mathbb{G}_2 can be described as follows. The conversion framework with message space \mathbb{G}_1 is analogous.

SPS-T2

- (1) *Setup.* Let $e_2 : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a Type 2 pairing where \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T have order n ; G, H are fixed generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively.
- (2) *Key generation.* The secret key contains elements $u_1, u_2, \dots, v_1, v_2, \dots \in_R [1, n-1]$. The public key contains elements $U_1, U_2, \dots \in \mathbb{G}_1, V_1, V_2, \dots \in \mathbb{G}_2$, where $U_i = G^{u_i}$ and $V_j = H^{v_j}$. Note that because the signer is generic, we can assume without loss of generality that the signer knows the discrete logarithm of the U_i and the V_j .
- (3) *Signature generation.* The message is $M \in \mathbb{G}_2$. However, unlike the public key, we cannot in general assume that the signer knows the discrete logarithm of $M = H^m$. The signing algorithm is restricted to generic group operations, so a generic signer can only construct signature elements of the form $S_i = \psi(M)^{\alpha_i} G^{\beta_i} \in \mathbb{G}_1$ and $T_j = M^{\gamma_j} H^{\delta_j}$ where $\alpha_i, \beta_i, \gamma_j, \delta_j \in [0, n-1]$ are independent of m . Finally, the algorithm outputs a signature containing elements $(S_1, S_2, \dots) \in \mathbb{G}_1$ and $(T_1, T_2, \dots) \in \mathbb{G}_2$.
- (4) *Signature verification.* Given message M and a corresponding signature of the form $(S_1, S_2, \dots, T_1, T_2, \dots)$, the verifier does the following:
 - (a) check that $S_1, S_2, \dots \in \mathbb{G}_1$;
 - (b) check that $M \in \mathbb{G}_2$ and $T_1, T_2, \dots \in \mathbb{G}_2$;
 - (c) verify a collection of equations of the following form:

$$\begin{aligned} & \prod_i \prod_j e_2(S_i, T_j)^{a_{qij}} \cdot \prod_i \prod_j e_2(S_i, V_j)^{b_{qij}} \cdot \prod_j e_2(\psi(M), T_j)^{c_{qj}} \\ & \cdot \prod_j e_2(\psi(M), V_j)^{d_{qj}} \cdot \prod_i e_2(S_i, M)^{e_{qi}} \cdot \prod_i e_2(U_i, M)^{f_{qi}} \\ & \cdot \prod_i \prod_j e_2(U_i, T_j)^{g_{qij}} \cdot e_2(\psi(M), M)^{h_q} = 1. \end{aligned}$$

Note: We use the augmented set $S = \{S_1, S_2, \dots\} \cup \{\psi(T_1), \psi(T_2), \dots\}$ in the above verification equation. However, there is no need to consider the elements $\psi(V_j)$ separately because they can, without loss of generality, be included in the public key. The constant exponents a_{qij}, b_{qij}, \dots from $[0, n-1]$ used in the verification equations are specified as part of the signature verification algorithm.

We now propose the following transformation to convert SPS-T2 from the Type 2 to the Type 3 setting. The transformation uses the efficiently-computable isomorphism $D : \mathbb{G}_2 \rightarrow \mathbb{H}_2$ given by $D(Q) = (\psi(Q), \rho(Q))$ where $\mathbb{H}_2 \subseteq \mathbb{G}_1 \times \mathbb{G}_3$ (see §2.3). Our strategy is very simple: apply D so that all \mathbb{G}_2 elements in SPS-T2 are replaced by their “shorter representation” as elements of \mathbb{H}_2 . This strategy, together with the observation that the

computation of a Type 2 pairing e_2 is efficiently reduced to the task of computing a Type 3 pairing e_3 (see equation (1)), immediately yields the following Type 3 structure-preserving signature scheme.

SPS-T3

- (1) *Setup.* Let $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \longrightarrow \mathbb{G}_T$ be a Type 3 pairing where \mathbb{G}_1 , \mathbb{G}_3 and \mathbb{G}_T have order n ; G, I are fixed generators of $\mathbb{G}_1, \mathbb{G}_3$, respectively.
- (2) *Key generation.* For each element $V_j = H^{v_j}$ in SPS-T2, compute $V_{j_1} = G^{v_j}$ and $V_{j_2} = I^{v_j}$. The secret key contains elements $u_1, u_2, \dots, v_1, v_2, \dots \in_R [1, n - 1]$. The public key contains elements $U_1, U_2, \dots \in \mathbb{G}_1$ (as in SPS-T2) and $(V_{1_1}, V_{1_2}), (V_{2_1}, V_{2_2}), \dots \in \mathbb{H}_2$.
- (3) *Signature generation.* The message $M = H^m$ in SPS-T2 can be written as $(M_1, M_2) = (G^m, I^m) \in \mathbb{H}_2$. Recall that using generic group operations, a generic signer in SPS-T2 can only construct $S_i = M_1^{\alpha_i} G^{\beta_i}$ and $T_j = M^{\gamma_j} H^{\delta_j}$ where $\alpha_i, \beta_i, \gamma_j, \delta_j$ are independent of m . Representing T_j as an element of \mathbb{H}_2 we have $T_j = (T_{j_1}, T_{j_2}) = (M_1^{\gamma_j} G^{\delta_j}, M_2^{\gamma_j} I^{\delta_j}) \in \mathbb{H}_2$. It is easy to see that a generic signer can compute the signature element $T_j \in \mathbb{G}_2$ if and only if she can compute $M_1^{\gamma_j} G^{\delta_j} \in \mathbb{G}_1$ and $M_2^{\gamma_j} I^{\delta_j} \in \mathbb{G}_3$. Using the above idea we can convert each signature element $T_j \in \mathbb{G}_2$ of SPS-T2 to $(T_{j_1}, T_{j_2}) \in \mathbb{H}_2$ and thereby obtain the corresponding signature elements in SPS-T3. Finally, the algorithm outputs a signature of the form $S_1, S_2, \dots \in \mathbb{G}_1$ and $(T_{1_1}, T_{1_2}), (T_{2_1}, T_{2_2}), \dots \in \mathbb{H}_2$.
- (4) *Signature verification.* Given a message (M_1, M_2) and corresponding signature $(S_1, S_2, \dots, (T_{1_1}, T_{1_2}), (T_{2_1}, T_{2_2}), \dots)$, the verifier does the following:
 - (a) check that $S_1, S_2, \dots \in \mathbb{G}_1$;
 - (b) check that $(M_1, M_2), (T_{1_1}, T_{1_2}), (T_{2_1}, T_{2_2}), \dots \in \mathbb{H}_2$;
 - (c) verify a set of equations of the following form:

$$\begin{aligned} & \prod_i \prod_j e_3(S_i, T_{j_2})^{a_{qij}} \cdot \prod_i \prod_j e_3(S_i, V_{j_2})^{b_{qij}} \cdot \prod_j e_3(M_1, T_{j_2})^{c_{qj}} \\ & \cdot \prod_j e_3(M_1, V_{j_2})^{d_{qj}} \cdot \prod_i e_3(S_i, M_2)^{e_{qi}} \cdot \prod_i e_3(U_i, M_2)^{f_{qi}} \\ & \cdot \prod_i \prod_j e_3(U_i, T_{j_2})^{g_{qij}} \cdot e_3(M_1, M_2)^{h_q} = 1. \end{aligned}$$

Note: We use the augmented set $S = \{S_1, S_2, \dots\} \cup \{T_{1_1}, T_{2_1}, \dots\}$ in the above verification equation. As already observed in the context of SPS-T2, there is no need to consider the public key elements V_{1_1}, V_{2_1}, \dots separately and the constants in the exponent are specified in the verification algorithm.

Correctness of SPS-T3 follows directly from the correctness of SPS-T2. Moreover, SPS-T3 maintains all the claimed benefits of SPS-T2. We now show that SPS-T3 is as secure as its original Type 2 counterpart SPS-T2. For concreteness, the security argument is sketched for existential unforgeability under chosen message attack (EUF-CMA), but it is easy to see that the argument extends to other standard notions of security such as EUF-RMA and strong unforgeability under chosen/random message attack.

Claim 2. *SPS-T2 is EUF-CMA-secure if and only if SPS-T3 is EUF-CMA-secure.*

Proof. In the framework of the conversion described above, we have consistently replaced all \mathbb{G}_2 elements in SPS-T2 by the corresponding \mathbb{H}_2 elements to derive the corresponding algorithms of SPS-T3. Recall that $D : \mathbb{G}_2 \rightarrow \mathbb{H}_2$ is an efficiently-computable isomorphism whose inverse is also efficiently computable. Hence, given an EUF-CMA adversary against SPS-T3, one can easily construct an EUF-CMA adversary against SPS-T2 and vice versa. \square

Remark 3. SPS-T3 does not have any efficiency gain (or loss) compared to SPS-T2. Further optimizations for SPS-T3 are usually possible by removing some redundant group elements after a careful scrutiny of the construction and its security argument as suggested in [13]. For example, the Type 3 schemes described in §3 and §4 are optimized versions of their Type 2 counterparts obtained by following the general recipe given above.

Remark 4. The subgroup membership tests described in step 4(b) of SPS-T2 and SPS-T3 involve pairing-based verification equations. We have observed in §3 and §4 that avoiding subgroup membership tests can lead to a random message attack in both the Type 2 and 3 settings. Apart from these pairing-based verifications of subgroup membership, signature verification will involve at least one more pairing product equation. See the proof of Theorem 3 for further details.

Remark 5. Consider the following hypothetical situation. Working within the mathematical structure of asymmetric pairings described in §2, someone in the future discovers an efficient method for membership testing in \mathbb{G}_2 that does not require a pairing computation. By Lemma 1, the pairing-based verifications in the Type 3 setting for testing whether $(Q_1, Q_2) \in \mathbb{H}_2$ (see step 4(b) in SPS-T3) will no longer be required. This simple observation together with Claim 2 immediately shows that if there exists, say, an EUF-CMA secure structure-preserving signature scheme in Type 2 with a single PPE-based verification, then there exists an EUF-CMA secure structure-preserving signature scheme in Type 3 with a single PPE-based verification. For example, if the membership testing in \mathbb{G}_2 in the verification step of the Type 2 randomizable SPS of [4] can be performed without pairing then the verification in step 5(b) of the Type 3 randomizable SPS of Section 4.2 can be replaced by a pairing-free check of $(R_1, R_2) \in \mathbb{H}_2$, leading to a single PPE-based verification in the Type 3 setting. Consequently, our hypothetical situation will refute the Abe et al. assertion [4] that, unlike the Type 2 setting, in the Type 3 setting no secure structure-preserving signature scheme can have a single PPE-based verification. Further, when read in conjunction with Claim 2 and Remark 3, it is easy to see that none of the superiority claims in [4] of a structure-preserving signature scheme in Type 2 over Type 3 will hold even in this hypothetical scenario.

5.2. Impossibility of single PPE in verification. In Theorem 2 of [2], Abe et al. showed that there is no Type 3 structure-preserving signature scheme with a single pairing-based verification equation that is existentially unforgeable under random message attack. The original argument was for messages in \mathbb{G}_1 , but can be easily extended when messages are from \mathbb{G}_3 . In Theorem 3 of [4], Abe et al. showed a similar impossibility result for Type 2 structure-preserving signature schemes with messages in \mathbb{G}_1 .

Assuming that the hypothetical scenario discussed in Remark 5 does not occur⁷, one can generalize the above results to show that the impossibility holds even when the messages are drawn from \mathbb{H}_2 . As a corollary, one concludes that there is no Type 2 SPS scheme with a single pairing-based verification equation that is existentially unforgeable under random message attack.

Theorem 3. *No structure-preserving signature scheme with a single pairing-product equation based signature verification is secure in the sense of existential unforgeability under random message attack.*

Proof. The case of messages in \mathbb{G}_1 in the Type 3 setting (resp. the Type 2 setting) is proved in [2, Theorem 2] (resp. [4, Theorem 3]). The case of messages in \mathbb{G}_3 in the Type 3 setting is analogous to the proof of Theorem 2 in [2]. The case of the Type 1 setting was settled in [3, Theorem 4].

We now show the same impossibility for messages in \mathbb{G}_2 . For ease of exposition, we will use the structure of SPS-T3, which we have already shown equivalent to SPS-T2, and the message space \mathbb{H}_2 (recall that \mathbb{H}_2 is isomorphic to \mathbb{G}_2 , and that an element of \mathbb{H}_2 is comprised of a pair in $\mathbb{G}_1 \times \mathbb{G}_3$ the components of which have the same discrete logarithm with respect to the fixed generators G and I). Our argument closely follows the proof of Theorem 2 from [2] but needs to take care of additional complications due to the structure of \mathbb{H}_2 .

Recall the signature verification for SPS-T3 where in step 4(c) we described the general form of a verification equation. Our claim is that having a *single* verification equation of the form 4(c) and omitting the subgroup membership test in step 4(b) lead to a random message attack. In other words, signature verification must involve more than one PPEs (some of which may be in the disguise of subgroup membership test for \mathbb{H}_2 i.e., \mathbb{G}_2). For simplicity, we assume that the signature contains two elements of \mathbb{H}_2 . Note that Abe et al. claim that two group elements is the optimal signature size in Type 2 – see Table 1 of [4]. However, it is easy to see that our result holds for the more general case.

Consider a structure-preserving signature scheme for messages in \mathbb{H}_2 with verification key containing group elements $U_1, U_2, \dots \in \mathbb{G}_1$, $V_1, V_2, \dots \in \mathbb{G}_3$, and $Z \in \mathbb{G}_T$.⁸ For simplicity, in the following we consider two U_i 's and two V_i 's in the verification key. A signature is of

⁷Note that Theorem 2 of [2] has to be interpreted modulo the (implicit) assumption that the hypothetical scenario discussed in Remark 5 does not occur. Otherwise, the Type 3 randomizable structure-preserving signature scheme in Section 4.2 with message space \mathbb{G}_3 and its dual discussed later in Section 5.3 with message space \mathbb{G}_1 will contradict the impossibility result of [2].

⁸Here, as in [2], we have relaxed the original definition of structure-preserving signatures to allow the public verification key to contain an arbitrary element Z from \mathbb{G}_T that appears in the verification equation. As already observed in [2], the relaxation strengthens the impossibility result.

the form $(S_1, T_1), (S_2, T_2) \in \mathbb{H}_2$ and is verified by the following PPE:

$$\begin{aligned} & e_3(S_1, T_1)^{a_{11}} \cdot e_3(S_1, T_2)^{a_{12}} \cdot e_3(S_2, T_1)^{a_{21}} \cdot e_3(S_2, T_2)^{a_{22}} \\ & \cdot e_3(S_1, V_1)^{b_{11}} \cdot e_3(S_1, V_2)^{b_{12}} \cdot e_3(S_2, V_1)^{b_{21}} \cdot e_3(S_2, V_2)^{b_{22}} \\ & \cdot e_3(M_1, T_1)^{c_{11}} \cdot e_3(M_1, T_2)^{c_{12}} \cdot e_3(M_1, V_1)^{d_{11}} \cdot e_3(M_1, V_2)^{d_{12}} \\ & \cdot e_3(S_1, M_2)^{c_{21}} \cdot e_3(S_2, M_2)^{c_{22}} \cdot e_3(U_1, M_2)^{d_{21}} \cdot e_3(U_2, M_2)^{d_{22}} \\ & \cdot e_3(U_1, T_1)^{e_{11}} \cdot e_3(U_1, T_2)^{e_{12}} \cdot e_3(U_2, T_1)^{e_{21}} \cdot e_3(U_2, T_2)^{e_{22}} \\ & \cdot e_3(M_1, M_2)^f = Z. \end{aligned}$$

Note that terms such as $e_3(U_i, V_j)$ can be incorporated in $Z \in \mathbb{G}_T$ without any loss of generality.

Given a signature $(S_1, T_1), (S_2, T_2) \in \mathbb{H}_2$ on a random message $(M_1, M_2) \in \mathbb{H}_2$, we isolate S_1, S_2 and M_2 in the verification equation to obtain:

$$\begin{aligned} A_1 &= T_1^{a_{11}} T_2^{a_{12}} V_1^{b_{11}} V_2^{b_{12}} & A_2 &= T_1^{a_{21}} T_2^{a_{22}} V_1^{b_{21}} V_2^{b_{22}} \\ B_1 &= M_1^f S_2^{c_{22}} U_1^{d_{21}} U_2^{d_{22}} & B_2 &= M_1^f S_1^{c_{21}} U_1^{d_{21}} U_2^{d_{22}}. \end{aligned}$$

Suppose that $A_1 \neq M_2^{-c_{21}}$. We first rewrite the verification equation as

$$e_3(S_1, M_2)^{c_{21}} \cdot e_3(S_1, A_1) \cdot e_3(B_1, M_2) \cdot \hat{Z} = Z.$$

Note that \hat{Z} does not contain the terms S_1 and M_2 . If $c_{21} = 0$, then we set $S'_1 = S_1 B_1^{-1}$ and $M'_2 = M_2 A_1$. For the message (M_1, M'_2) we have a forged signature $(S'_1, T_1), (S_2, T_2)$.⁹ If $c_{21} \neq 0$, then we set $S'_1 = S_1^{-1} B_1^{-2/c_{21}}$ and $M'_2 = M_2^{-1} A_1^{-2/c_{21}}$ and the corresponding forgery is $(S'_1, T_1), (S_2, T_2)$ for message (M_1, M'_2) .

A similar attack works when $A_2 \neq M_2^{-c_{22}}$.

Suppose now that $A_1 M_2^{c_{21}} = 1$ and $A_2 M_2^{c_{22}} = 1$. So both S_1 and S_2 are cancelled from the verification equation and henceforth we will only consider the signature elements T_1, T_2 . Now, the verification equation will be of the form

$$\begin{aligned} & e_3(M_1, T_1)^{c_{11}} \cdot e_3(M_1, T_2)^{c_{12}} \cdot e_3(M_1, V_1)^{d_{11}} \cdot e_3(M_1, V_2)^{d_{12}} \\ & \cdot e_3(U_1, M_2)^{d_{21}} \cdot e_3(U_2, M_2)^{d_{22}} \\ & \cdot e_3(U_1, T_1)^{e_{11}} \cdot e_3(U_1, T_2)^{e_{12}} \cdot e_3(U_2, T_1)^{e_{21}} \cdot e_3(U_2, T_2)^{e_{22}} \\ & \cdot e_3(M_1, M_2)^f = Z. \end{aligned}$$

Proceeding as before, we isolate M_1 and M_2 to obtain

$$A_3 = T_1^{c_{11}} T_2^{c_{12}} V_1^{d_{11}} V_2^{d_{12}} \quad B_3 = U_1^{d_{21}} U_2^{d_{22}}.$$

Suppose $A_3 \neq M_2^{-f}$. The verification equation can be written as

$$e_3(M_1, M_2)^f \cdot e_3(M_1, A_3) \cdot e_3(B_3, M_2) \cdot Z' = Z.$$

Note that Z' does not contain the elements M_1 and M_2 . If $f = 0$, then setting $M'_1 = M_1 B_3^{-1}$ and $M'_2 = M_2 A_3$ yields the forgery (T_1, T_2) for (M'_1, M'_2) . If $f \neq 0$, then setting $M'_1 = M_1^{-1} B_3^{-2/f}$ and $M'_2 = M_2^{-1} A_3^{-2/f}$ yields the forgery (T_1, T_2) for (M'_1, M'_2) .

⁹The attack can be prevented by checking whether (M_1, M'_2) and (S'_1, T_1) are elements of \mathbb{H}_2 or not. However that requires *two* additional pairing-product equations in signature verification.

Suppose now that $A_3 M_2^f = 1$; so the message element M_1 is also cancelled from the verification equation. Thus the signature verification is reduced to the form:

$$e_3(U_1, M_2)^{d_{21}} \cdot e_3(U_2, M_2)^{d_{22}} \cdot e_3(U_1, T_1)^{e_{11}} \cdot e_3(U_1, T_2)^{e_{12}} \\ \cdot e_3(U_2, T_1)^{e_{21}} \cdot e_3(U_2, T_2)^{e_{22}} = Z.$$

Producing a forgery is now trivial. The adversary obtains signatures (T_1, T_2) and (T'_1, T'_2) on random messages (M_1, M_2) and (M'_1, M'_2) . From these the adversary forms a signature $(T_1^2/T'_1, T_2^2/T'_2)$ on a new message $(M_1^2/M'_1, M_2^2/M'_2)$. \square

5.3. Separation. We construct a Type 3 randomizable structure-preserving signature scheme that has no secure counterpart in the Type 2 setting. The Type 3 scheme is a “dual” of the scheme presented in §4.2 in the sense that the former has $V, W \in \mathbb{G}_1$ and $M, S \in \mathbb{G}_3$, whereas the latter has $V, W \in \mathbb{G}_3$ and $M, S \in \mathbb{G}_1$.

- (1) *Setup.* Let $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \rightarrow \mathbb{G}_T$ be a Type 3 pairing, where $\mathbb{G}_1, \mathbb{G}_3$ and \mathbb{G}_T have order n ; G, I are fixed generators of $\mathbb{G}_1, \mathbb{G}_3$, respectively.
- (2) *Key generation.* The secret key is $v, w \in_R [1, n-1]$. The public key is (V, W) where $V = I^v$ and $W = I^w$.
- (3) *Signature generation.* To sign $M \in \mathbb{G}_1$, select $r \in_R [1, n-1]$ and compute $R_1 = G^r$, $R_2 = I^r$ and $S = M^v G^{r^2+w}$. The signature on M is (R_1, R_2, S) .
- (4) *Randomization.* To randomize $(M, (R_1, R_2, S))$, select $\alpha \in_R [1, n-1]$ and compute $R'_1 = R_1 G^\alpha$, $R'_2 = R_2 I^\alpha$, and $S' = S R_1^{2\alpha} G^{\alpha^2}$. The randomized signature on M is (R'_1, R'_2, S') .
- (5) *Signature verification.* To verify a signed message $(M, (R_1, R_2, S))$, check that
 - (a) $M, R_1, S \in \mathbb{G}_1$ and $R_2 \in \mathbb{G}_3$;
 - (b) $e_3(R_1, I) = e_3(G, R_2)$; and
 - (c) $e_3(S, I) = e_3(M, V) \cdot e_3(R_1, R_2) \cdot e_3(G, W)$.

Because of the dual nature of the two schemes, the security proof against generic forgers for the Type 3 scheme indicated in §4.2 carries over to the Type 3 scheme described here when we swap the roles of the elements in \mathbb{G}_1 and \mathbb{G}_3 .

However, the above Type 3 scheme does not have a secure and natural counterpart in the Type 2 setting. The natural Type 2 variant has public key $V = H^v$, $W = H^w$, signatures on a message $M \in \mathbb{G}_1$ comprising of $R = H^r$ and $S = M^v G^{r^2+w}$, and verification that checks $M, S \in \mathbb{G}_1$, $R \in \mathbb{G}_2$ and $e_2(S, H) = e_2(M, V) \cdot e_2(\psi(R), R) \cdot e_2(G, W)$. Now, given the public key (V, W) an adversary can mount the following no-message attack. Select arbitrary $m, r \in [1, n-1]$ and compute a forged signature on $M = G^m$ as $R = H^r$ and $S = \psi(V)^m \psi(W) G^{r^2} = M^v G^{r^2+w}$. While the absence of an efficiently-computable isomorphism from \mathbb{G}_3 to \mathbb{G}_1 allows us to construct the secure Type 3 scheme described above, the availability of ψ in the Type 2 setting provides the adversary with the means to mount the no-message attack.

5.4. Type 2: A designer’s artifact? It is not the case that the Abe et al. [4] constructions and security arguments have any intrinsic weakness. However, their efficiency analysis as well as the optimality claims are incorrect. A similar observation holds for the optimality claims made in the follow-up work of Barthe et al. [9] and in various lower bound results

of [4, 9].¹⁰ The central problem in the analysis of protocols in the generic Type 2 model and associated lower bound claims stems from an incomplete abstraction of the underlying mathematical structure.

In prime-order asymmetric pairing groups, a protocol designer has the choice of using elements from \mathbb{G}_1 , \mathbb{G}_3 and $\mathbb{H}_2 \subseteq \mathbb{G}_1 \times \mathbb{G}_3$. However, the definition of a bilinear group generator in the generic Type 2 setting recognizes only \mathbb{G}_1 , \mathbb{G}_2 and the isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$. See, for example, the definition of a bilinear group generator \mathcal{G} in §2.1 of [4]. The definition does not take into account the fact that in concrete settings there may exist a group \mathbb{G}_3 and an efficiently-computable isomorphism $\rho : \mathbb{G}_2 \rightarrow \mathbb{G}_3$. This incompleteness in the abstract definition has a significant bearing on the concrete analysis of pairing-based cryptographic protocols as we demonstrate in this paper.¹¹

More generally, a protocol designer desiring to use the map ψ in a cryptographic protocol or the corresponding security argument unnecessarily restricts herself to \mathbb{G}_1 and \mathbb{G}_2 (i.e. \mathbb{H}_2). This design artifact introduces (costly) redundancy in the cryptographic scheme without any benefit in terms of functionality or security. This observation was first made in [13] based on a careful analysis of existing Type 2 schemes. However, [13] did not attempt a formal proof of the assertion that Type 2 pairings are “merely less efficient implementation of Type 3 pairings”. Motivated by the erroneous claim of superiority of Type 2 over Type 3 in [4], in this paper we formally settle the relation between Type 2 and Type 3 settings in the context of generic-signer structure-preserving signatures.

6. CONCLUDING REMARKS

We presented natural Type 3 analogues of the Type 2 strongly unforgeable and randomizable structure-preserving signature schemes that were proposed in [4]. By properly accounting for subgroup membership testing of group elements in signatures, we have shown that the Type 3 schemes are superior to their Type 2 counterparts when the signature schemes are used in a stand-alone setting, and when used in conjunction with Groth-Sahai proofs. Finally, we show that all generic-signer Type 2 schemes are merely Type 3 schemes in disguise and cannot beat the existing lower bound results. On the other hand, not all Type 3 schemes have a secure Type 2 counterpart. We conclude that the question posed in [13] of the existence of a cryptographic protocol which necessarily has to be restricted to Type 2 for implementation or security reasons is still open.

Acknowledgements. We thank Jens Groth and Francisco Rodríguez-Henríquez for their comments on an earlier draft of the paper. We also thank the Asiacrypt reviewers for their helpful feedback.

¹⁰For example, Theorem 4 of [4] proves a lower bound of two group elements in the verification key under the assumption of a single verification equation. The theorem as stated is void because there is *no* secure structure-preserving signature with a single verification equation.

¹¹Following the approach outlined here, we believe it is not difficult to devise a more comprehensive definition of generic bilinear group generator in the Type 2 setting. Such a definition should be able to better model the concrete properties of the Type 2 setting, such as infeasibility of hashing into \mathbb{G}_2 and the cost of subgroup membership testing in \mathbb{G}_2 . However, we do not undertake such an exercise or, for that matter, a better model of Type 2 structure-preserving signature, since we don’t see any concrete motivation for using the Type 2 setting in the first place.

APPENDIX A. GROTH-SAHAI PROOFS

In this section, we use additive notation for elements of \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_3 .

A.1. DLIN-based proofs. Let $A, B \in \mathbb{G}_1$ and $t \in \mathbb{G}_T$. We present a Groth-Sahai non-interactive witness-indistinguishable proof of knowledge of $X, Y \in \mathbb{G}_2$ such that $e_2(A, X) \cdot e_2(B, Y) = t$. The NIWI proof is derived from the general description in §4.2 of [17]. It can also be used with Type 3 pairings. Security is based on the decisional linear (DLIN) assumption.

- (1) *Setup.* Let $e_2 : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a Type 2 pairing.
- (2) *Common reference string.* Let H be a generator of \mathbb{G}_2 . Let $a, b, i, j \in_R [1, n-1]$, and define $U = aH$, $V = bH$, $I = iU$, $J = jV$, $K = (i + j)H$. The common reference string is (H, U, V, I, J, K) .
- (3) *Commitment.* Select $s_{11}, s_{12}, s_{13}, s_{21}, s_{22}, s_{23} \in_R [1, n-1]$ and compute $d_{11} = s_{11}U + s_{13}I$, $d_{12} = s_{12}V + s_{13}J$, $d_{13} = X + s_{11}H + s_{12}H + s_{13}K$, $d_{21} = s_{21}U + s_{23}I$, $d_{22} = s_{22}V + s_{23}J$ and $d_{23} = Y + s_{21}H + s_{22}H + s_{23}K$. The commitment is $d = (d_{11}, d_{12}, d_{13}, d_{21}, d_{22}, d_{23})$.
- (4) *Proof.* Compute $\theta_1 = s_{11}A + s_{21}B$, $\theta_2 = s_{12}A + s_{22}B$ and $\theta_3 = s_{13}A + s_{23}B$. The proof is $\theta = (\theta_1, \theta_2, \theta_3)$.
- (5) *Verification.* Check that $\theta_1, \theta_2, \theta_3 \in \mathbb{G}_1$, $d_{11}, d_{12}, d_{13}, d_{21}, d_{22}, d_{23} \in \mathbb{G}_2$, and

$$\begin{aligned} e_2(A, d_{11}) \cdot e_2(B, d_{21}) &= e_2(\theta_1, U) \cdot e_2(\theta_3, I) \\ e_2(A, d_{12}) \cdot e_2(B, d_{22}) &= e_2(\theta_2, V) \cdot e_2(\theta_3, J) \\ e_2(A, d_{13}) \cdot e_2(B, d_{23}) &= e_2(\theta_1, H) \cdot e_2(\theta_2, H) \cdot e_2(\theta_3, K) \cdot t. \end{aligned}$$

A.2. DDH-based proofs. Let $A, B \in \mathbb{G}_1$ and $t \in \mathbb{G}_T$. We present a Groth-Sahai non-interactive witness-indistinguishable proof of knowledge of $X, Y \in \mathbb{G}_3$ such that $e_3(A, X) \cdot e_3(B, Y) = t$. The NIWI proof is derived from the general description in §4.1 of [17]. Security is based on the decisional Diffie-Hellman (DDH) assumption in \mathbb{G}_3 . Since the decisional Diffie-Hellman problem is easy in \mathbb{G}_2 , the NIWI proof has no counterpart with Type 2 pairings.

- (1) *Setup.* Let $e_3 : \mathbb{G}_1 \times \mathbb{G}_3 \rightarrow \mathbb{G}_T$ be a Type 3 pairing.
- (2) *Common reference string.* Let I be a generator of \mathbb{G}_3 . Let $a, b \in_R [1, n-1]$, and define $U = aI$, $V = bI$, $J = bU$. The common reference string is (I, U, V, J) .
- (3) *Commitment.* Select $s_{11}, s_{12}, s_{21}, s_{22} \in_R [1, n-1]$ and compute $d_{11} = s_{11}I + s_{12}V$, $d_{12} = X + s_{11}U + s_{12}J$, $d_{21} = s_{21}I + s_{22}V$ and $d_{22} = Y + s_{21}U + s_{22}J$. The commitment is $d = (d_{11}, d_{12}, d_{21}, d_{22})$.
- (4) *Proof.* Compute $\theta_1 = s_{11}A + s_{21}B$ and $\theta_2 = s_{12}A + s_{22}B$. The proof is $\theta = (\theta_1, \theta_2)$.
- (5) *Verification.* Check that $\theta_1, \theta_2 \in \mathbb{G}_1$, $d_{11}, d_{12}, d_{21}, d_{22} \in \mathbb{G}_3$, and

$$\begin{aligned} e_3(A, d_{11}) \cdot e_3(B, d_{21}) &= e_3(\theta_1, I) \cdot e_3(\theta_2, V) \\ e_3(A, d_{12}) \cdot e_3(B, d_{22}) &= e_3(\theta_1, U) \cdot e_3(\theta_2, J) \cdot t. \end{aligned}$$

APPENDIX B. DEFINITIONS

Here we reproduce the definition of structure-preserving signature and its security from [4].

Recall that a signature scheme is defined as a set of four algorithms: $\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V}$. The setup algorithm \mathcal{P} takes input a security parameter and outputs public parameter PP . The key generation algorithm \mathcal{K} takes input PP and outputs signing and verification key pair (SK, VK) . The signing algorithm takes input SK and a message M from the appropriate message space \mathcal{M} and returns a signature σ . The verification algorithm takes input VK , and a message-signature pair (M, σ) and returns a bit indicating whether the signature is valid or not. The set of four algorithms $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ must satisfy the standard correctness requirement:

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

The formal definition of a structure-preserving signature scheme assumes the existence of a bilinear group generator which, given a security parameter, returns a bilinear group description of the appropriate type.

Definition 1. *A signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is called a Type 2 structure-preserving signature scheme if*

- PP includes a bilinear group description $(n, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H)$ generated by \mathcal{G} , elements from $\mathbb{G}_1, \mathbb{G}_2$ and constants in \mathbb{Z}_n .
- VK consists of PP and elements from \mathbb{G}_1 and \mathbb{G}_2 .
- messages consists of group elements from \mathbb{G}_1 and \mathbb{G}_2 .
- \mathcal{V} only needs to decide membership in \mathbb{G}_1 and \mathbb{G}_2 , use the map ψ and evaluate pairing product equations.

Existential unforgeability under chosen message attack (EUF-CMA) for a structure-preserving signature scheme is defined in the standard way.

A randomizable variant of structure-preserving signature is also discussed in [4]: given a verification key VK , and a message-signature pair (M, σ) , a randomization algorithm \mathcal{R} returns a *randomized* signature σ' .

Definition 2 (Randomizability). *A signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is called (perfectly) randomizable if there exists a randomization algorithm \mathcal{R} such that for all $k \in \mathbb{N}$ and for all interactive adversaries \mathcal{A} , we have*

$$\Pr[PP \leftarrow \mathcal{P}(1^k); (SK, VK) \leftarrow \mathcal{K}(PP); (M, \sigma) \leftarrow \mathcal{A}(SK); \\ \sigma_0 \leftarrow \mathcal{S}_{SK}(M); \sigma_1 \leftarrow \mathcal{R}_{VK}(M, \sigma); b \in_R \{0, 1\} \\ : \mathcal{V}_{VK}(M, \sigma) = 1 \wedge \mathcal{A}(\sigma_b) = b] \approx \frac{1}{2} + \epsilon.$$

(We correct a minor error in [4]: ϵ , which is a negligible function in k , was missing in the original definition [4].)

REFERENCES

- [1] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo, “Structure-preserving signatures and commitments to group elements”, *Advances in Cryptology – CRYPTO 2010*, LNCS 6223 (2010), 209–236.
- [2] M. Abe, J. Groth, K. Haralambiev and M. Ohkubo, “Optimal structure-preserving signatures in asymmetric bilinear groups”, *Advances in Cryptology – CRYPTO 2011*, LNCS 6841 (2011), 649–666.
- [3] M. Abe, J. Groth, M. Ohkubo and M. Tibouchi, “Unified, minimal and selectively randomizable structure-preserving signatures”, *Theory of Cryptography – TCC 2014*, LNCS 8349 (2014), 688–712.
- [4] M. Abe, J. Groth, M. Ohkubo and M. Tibouchi, “Structure-preserving signatures from Type II pairings”, *Advances in Cryptology – CRYPTO 2014*, LNCS 8616 (2014), 390–407.
- [5] M. Abe, J. Groth, M. Ohkubo and M. Tibouchi, “Structure-preserving signatures from Type II pairings”, full version of [4]. Available at <http://eprint.iacr.org/2014/312>.
- [6] P. Barreto, B. Lynn and M. Scott, “Constructing elliptic curves with prescribed embedding degrees”, *Security in Communication Networks – SCN 2002*, LNCS 2576 (2003), 257–267.
- [7] P. Barreto, B. Lynn and M. Scott, “Efficient implementation of pairing-based cryptosystems”, *Journal of Cryptology*, 17 (2004), 321–334.
- [8] P. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order”, *Selected Areas in Cryptography – SAC 2005*, LNCS 3897 (2006), 319–331.
- [9] G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt and M. Tibouchi, “Strongly-optimal structure preserving signatures from Type II pairings: Synthesis and lower bounds”, *Public-Key Cryptography – PKC 2015*, LNCS 9020 (2015), 355–376. Full version available at <http://eprint.iacr.org/>.
- [10] M. Bellare, J. Garay and T. Rabin, “Fast batch verification for modular exponentiation and digital signatures”, *Advances in Cryptology – EUROCRYPT ’98*, LNCS 1403 (1998), 236–250.
- [11] M. Chase, “Efficient non-interactive zero-knowledge proofs for privacy applications”, Ph.D. thesis, Brown University, 2008.
- [12] S. Chatterjee, D. Hankerson, E. Knapp and A. Menezes, “Comparing two pairing-based aggregate signature schemes”, *Designs, Codes and Cryptography*, 55 (2010), 141–167.
- [13] S. Chatterjee and A. Menezes, “On cryptographic protocols employing asymmetric pairings – The role of ψ revisited”, *Discrete Applied Mathematics*, 159 (2011), 1311–1322.
- [14] L. Chen, Z. Cheng and N. Smart, “Identity-based key agreement protocols from pairings”, *International Journal of Information Security*, 6 (2007), 213–241.
- [15] A. Ferrara, M. Green, S. Hohenberger and M. Pedersen, “Practical short signature batch verification”, *Topics in Cryptology – CT-RSA 2009*, LNCS 5473 (2009), 309–324.
- [16] S. Galbraith, K. Paterson and N. Smart, “Pairings for cryptographers”, *Discrete Applied Mathematics*, 156 (2008), 3113–3121.
- [17] E. Ghadafi, N. Smart and B. Warinschi, “Groth-Sahai proofs revisited”, *Public-Key Cryptography – PKC 2010*, LNCS 6056 (2010), 177–192.
- [18] J. Groth, “Simulation-sound NIZK proofs for a practical language and constant size group signatures”, *Advances in Cryptology – ASIACRYPT 2006*, LNCS 4284 (2006), 444–459.
- [19] J. Groth and A. Sahai, “Efficient noninteractive proof systems for bilinear groups”, *SIAM Journal on Computing* 41 (2012), 1193–1232.
- [20] C. Hanser and D. Slamanig, “Structure-preserving signatures on equivalence classes and their application to anonymous credentials”, *Advances in Cryptology – ASIACRYPT 2014*, LNCS 8873 (2014), 491–511.
- [21] F. Hess, N. Smart and F. Vercauteren, “The eta pairing revisited”, *IEEE Transactions on Information Theory*, 52 (2006), 4595–4602.
- [22] E. Kachisa, E. Schaefer and M. Scott, “Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field”, *Pairing-Based Cryptography – Pairing 2008*, LNCS 5209 (2008), 126–135.
- [23] A. Miyaji, M. Nakabayashi and S. Tanako, “New explicit condition of elliptic curve trace for FR-reduction”, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E84-A (2001), 1234–1243.

- [24] F. Vercauteren, “Optimal pairings”, *IEEE Transactions on Information Theory*, 56 (2010), 455–461.

DEPARTMENT OF COMPUTER SCIENCE AND AUTOMATION, INDIAN INSTITUTE OF SCIENCE
E-mail address: sanjit@csa.iisc.ernet.in

DEPARTMENT OF COMBINATORICS & OPTIMIZATION, UNIVERSITY OF WATERLOO
E-mail address: ajmeneze@uwaterloo.ca