Practical Round-Optimal Blind Signatures in the Standard Model

Georg Fuchsbauer[1,†], Christian Hanser[2,‡], and Daniel Slamanig[2,‡]

[1] Institute of Science and Technology Austria
georg.fuchsbauer@ist.ac.at
[2] IAIK, Graz University of Technology, Austria
{christian.hanser|daniel.slamanig}@iaik.tugraz.at

Abstract. Round-optimal blind signatures are notoriously hard to construct in the standard model, especially in the malicious-signer model, where blindness must hold under adversarially chosen keys. This is substantiated by several impossibility results. The only construction that can be termed theoretically efficient, by Garg and Gupta (Eurocrypt'14), requires complexity leveraging, inducing an exponential security loss.
We present a construction of practically efficient round-optimal blind signatures in the standard model. It is conceptually simple and builds on the recent structure-preserving signatures on equivalence classes (SPS-EQ) from Asiacrypt'14. While the traditional notion of blindness follows from standard assumptions, we prove blindness under adversarially chosen keys under an interactive variant of DDH. However, we neither require non-uniform assumptions nor complexity leveraging.
We then show how to extend our construction to partially blind signatures and to blind signatures on message vectors, which yield a construction of one-show anonymous credentials à la "anonymous credentials light" (CCS'13) in the standard model.
Furthermore, we give the first SPS-EQ construction under non-interactive assumptions and show how SPS-EQ schemes imply conventional structure-preserving signatures, which allows us to apply optimality results for the latter to SPS-EQ.

Keywords: (Partially) Blind Signatures, Standard Model, SPS-EQ, One-Show Anonymous Credentials

1 Introduction

The concept of blind signatures [22] dates back to the beginning of the 1980s. A blind signature scheme is an interactive protocol where a user (or obtainer) requests a signature on a message which the signer (or issuer) must not learn. In particular, the signer must not be able to link a signature to the execution of the issuing protocol in which it was produced (*blindness*). Furthermore, it should even for adaptive adversaries be infeasible to produce a valid blind signature

† Supported by the European Research Council, ERC Starting Grant (259668-PSPC).
‡ Supported by EU FP7 through project FutureID (GA No. 318424).

without the signing key (*unforgeability*). Blind signatures have proven to be an important building block for cryptographic protocols, most prominently for e-cash, e-voting and one-show anonymous credentials. In more than 30 years of research, many different (> 50) blind signature schemes have been proposed. The spectrum ranges from RSA-based (e.g., [22,19]) over DL-based (e.g., [41,2]) and pairing-based (e.g., [14,12]) to lattice-based (e.g., [44]) constructions, as well as constructions from general assumptions (e.g., [36,35,25]).

Blind signatures and their round complexity. Two distinguishing features of blind signatures are whether they assume a common reference string (CRS) set up by a trusted party to which everyone has access; and the number of rounds in the signing protocol. Schemes which require only one round of interaction (two moves) are called *round-optimal* [25]. Besides improving efficiency, round optimality also directly yields concurrent security (which otherwise has to be dealt with explicitly; e.g., [37,35]). There are very efficient round-optimal schemes [23,14,11] under interactive assumptions (chosen target one more RSA inversion and chosen target CDH, respectively) in the random oracle model (ROM), as well as under the interactive LRSW [39] assumption in the CRS model [32]. All these schemes are in the honest-key model, where blindness only holds against signers whose keys are generated by the experiment.

Fischlin [25] proposed a generic framework for constructing round-optimal blind signatures in the CRS model with blindness under malicious keys: the signer signs a commitment to the message and the blind signature is a non-interactive zero-knowledge (NIZK) proof of a signed commitment which opens to the message. Using structure-preserving signatures (SPS) [3] and the Groth-Sahai (GS) proof system [33] instead of general NIZKs, this framework was efficiently instantiated in [3]. In [12,13], Blazy et al. gave alternative approaches to compact round-optimal blind signatures in the CRS model which avoid including a GS proof in the final blind signature. Another round-optimal solution with comparable computational costs was proposed by Seo and Cheon [46] building on work by Meiklejohn et al. [40].

Removing the CRS. Known impossibility results indicate that the design of round-optimal blind signatures in the standard model has some limitations. Lindell [38] showed that concurrently secure (and consequently also round-optimal) blind signatures are impossible in the standard model when using simulation-based security notions. This can however be bypassed via game-based security notions, as shown by Hazay et al. [35] for non-round-optimal constructions.

Fischlin and Schröder [27] showed that black-box reductions of blind-signature unforgeability to non-interactive assumptions in the standard model are impossible if the scheme has three moves or less, blindness holds statistically (or computationally if unforgeability and blindness are unrelated) and protocol transcripts allow to verify whether the user is able to derive a signature. Existing constructions [31,30] bypass these results by making non-black-box use of the underlying primitives (and preventing signature-derivation checks in [31]).

Garg et al. [31] proposed the first round-optimal generic construction in the standard model, which can only be considered as a theoretical feasibility result.

Using fully homomorphic encryption, the user encrypts the message sent to the signer, who evaluates the signing circuit on the ciphertext. To remove the CRS, they use two-round witness-indistinguishable proofs (ZAPs) to let the parties prove honest behavior; to preserve round-optimality, they include the first fixed round of the ZAP in the signer's public key.

Garg and Gupta [30] proposed the first efficient round-optimal blind signature constructions in the standard model. They build on Fischlin's framework using SPS. To remove a trusted setup, they use a two-CRS NIZK proof system based on GS proofs, include the CRSs in the public key while forcing the signer to honestly generate the CRS. Their construction, however, requires complexity leveraging (the reduction for unforgeability needs to solve a subexponential DL instance for every signing query) and is proven secure with respect to non-uniform adversaries. Consequently, communication complexity is in the order of hundreds of KB (even at a 80-bit security level) and the computational costs (not considered by the authors) seem to limit their practical application even more significantly.

Partially blind signatures. Partially blind signatures are an extension of blind signatures, which additionally allow to include common information in a signature. Many non-round-optimal partially blind signature schemes in the ROM are based on a technique by Abe and Okamoto [7]. The latter [42] proposed an efficient construction for non-round-optimal blind as well as partially blind signatures in the standard model. Round-optimal partially blind signatures in the CRS model can again be obtained from Fischlin's framework [25]. Round-optimal partially blind signatures in the CRS model are constructed in [13,40,46]. To date, there is—to the best of our knowledge—no round-optimal partially blind signature scheme that is secure in the standard model.

One-show anonymous credentials systems. Such systems allow a user to obtain a credential on several attributes from an issuer. The user can later selectively show attributes (or prove relations about attributes) to a verifier without revealing any information about undisclosed attributes. No party (including the issuer) can link the issuing of a credential to any of its showings, yet different showings of the same credential are linkable. An efficient implementation of one-show anonymous credentials is Microsoft's U-Prove [16].

Baldimtsi and Lysyanskaya [9] showed that the underlying signature scheme [15] cannot be proven secure using known techniques. To mitigate this problem, in [8] they presented a generic construction of one-show anonymous credentials in the vein of Brands' [15] approach from so-called blind signatures with attributes. They also present a scheme based on a non-round-optimal blind signature scheme by Abe [2] and prove their construction secure in the ROM.

Our Contribution

Blind signatures and anonymous credentials. Besides Fischlin's generic *commit-prove* paradigm [25], there are other classes of schemes. For instance, RSA and BLS blind signatures [23,14,11] follow a *randomize-derandomize* approach, which exploits the homomorphic property of the respective signature scheme.

Other approaches follow the *commit-rerandomize-transform* paradigm, where a signature on a commitment to a message can be transformed into a rerandomized (unlinkable) signature on the original message [12,32]. Our construction is based on a new concept, which one may call *commit-randomize-derandomize-open* approach. It does not use non-interactive proofs at all and is solely based on the recent concept of structure-preserving signature schemes on equivalence classes (SPS-EQ) [34] and commitments. As we also avoid a trusted setup of the commitment parameters, we do not require a CRS. We do however prove our scheme secure under interactive hardness assumptions.

In SPS-EQ the message space is partitioned into equivalence classes and given a signature on a message anyone can *adapt* the signature to a different representative of the same class. SPS-EQ requires that after signing a representative a signer cannot distinguish between an adapted signature for a new representative of the same class and a fresh signature on a completely random message.

In our blind-signature scheme the obtainer combines a commitment to the message with a normalization element yielding a representative of an equivalence class (*commit*). She chooses a random representative of the same class (*randomize*), on which the signer produces a signature. She then adapts the signature to the original representative containing the commitment (*derandomize*), which can be done without requiring the signing key. The blind signature is the rerandomized (unlinkable) signature for the original representative plus an opening for the commitment (*open*). Our contributions to blind signatures are the following:

- We propose a new approach to constructing blind signatures in the standard model based on SPS-EQ. It yields conceptually simple and compact constructions and does not rely on techniques such as complexity leveraging. Our blind signatures are practical in terms of key size, signature size, communication and computational effort (when implemented with known instantiations of SPS-EQ [29], a blind signature consists of 5 bilinear-group elements).
- We provide the first construction of round-optimal partially blind signatures in the standard model, which follow straightforwardly from our blind signatures and are almost as efficient.
- We generalize our blind signature scheme to message vectors, which yields one-show anonymous credentials à la "anonymous credentials light" [8]. We thus obtain one-show anonymous credentials secure in the standard model (whereas all previous ones have either no security proof or ones in the ROM).

SPS-EQ. We give the first structure-preserving signatures on equivalence classes satisfying all security notions from [34] under non-interactive assumptions. (Unfortunately, the scheme does not have all the properties required for building blind signatures from it, for which we strengthen the notions from [34].)

Moreover, we show how any SPS-EQ scheme can be turned into a standard structure-preserving signature scheme. This transformation allows us to apply the optimality criteria by Abe et al. [4,5] to SPS-EQ. We conclude that the scheme from [29] is optimal in terms of signature size and verification complexity and that it cannot be proven unforgeable under non-interactive assumptions.

2 Preliminaries

A function $\epsilon\colon \mathbb{N} \to \mathbb{R}^+$ is *negligible* if $\forall\, c > 0\ \exists\, k_0\ \forall\, k > k_0 : \epsilon(k) < 1/k^c$. By $a \xleftarrow{R} S$ we denote that a is chosen uniformly at random from a set S. We write $\mathsf{A}(a_1, \ldots, a_n; r)$ to make the randomness r used by a probabilistic algorithm $\mathsf{A}(a_1, \ldots, a_n)$ explicit. If $\mathbb{G}$ is an (additive) group then $\mathbb{G}^*$ denotes $\mathbb{G} \setminus \{0_{\mathbb{G}}\}$.

Definition 1 (Bilinear map). Let $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$, generated by P and $\hat{P}$, resp., and $(\mathbb{G}_T, \cdot)$ be cyclic groups of prime order p. We call $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ a *bilinear map (pairing)* if it is efficiently computable and the following holds:

Bilinearity: $e(aP, b\hat{P}) = e(P, \hat{P})^{ab} = e(bP, a\hat{P}) \quad \forall\, a, b \in \mathbb{Z}_p$.
Non-degeneracy: $e(P, \hat{P}) \neq 1_{\mathbb{G}_T}$, i.e., $e(P, \hat{P})$ generates $\mathbb{G}_T$.

If $\mathbb{G}_1 = \mathbb{G}_2$, then e is *symmetric* (Type-1) and *asymmetric* (Type-2 or 3) otherwise. For Type-2 pairings there is an efficiently computable isomorphism $\Psi\colon \mathbb{G}_2 \to \mathbb{G}_1$; for Type-3 pairings no such isomorphism is known. Type-3 pairings are currently the optimal choice in terms of efficiency and security trade-off [21].

Definition 2 (Bilinear-group generator). A bilinear-group generator is a polynomial-time algorithm BGGen that takes a security parameter 1^κ and outputs a bilinear group $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$ consisting of groups $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle \hat{P} \rangle$ and $\mathbb{G}_T$ of prime order p with $\log_2 p = \kappa$ and a pairing $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In this work we assume that BGGen is a *deterministic* algorithm.[3]

Definition 3 (Decisional Diffie-Hellman assumption). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. The DDH assumption holds in $\mathbb{G}_i$ for BGGen if for all probabilistic polynomial-time (PPT) adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{matrix} b \xleftarrow{R} \{0,1\},\ \mathsf{BG} = \mathsf{BGGen}(1^\kappa),\ r, s, t \xleftarrow{R} \mathbb{Z}_p \\ b^* \leftarrow \mathcal{A}\big(\mathsf{BG}, rP_i, sP_i, ((1-b)\cdot t + b \cdot rs)P_i\big) \end{matrix} : b^* = b\right] - \frac{1}{2} \leq \epsilon(\kappa)\ .$$

Definition 4 ((Symmetric) external Diffie-Hellman assumption). The XDH and SXDH assumptions hold for BGGen if the DDH assumption holds in $\mathbb{G}_1$ and holds in both $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

The next assumption is a static computational assumption derived from the SXDH version of the q-Diffie-Hellman inversion assumption [21].

Definition 5 (Co-Diffie-Hellman inversion assumption). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. The co-DHI$_i^*$ assumption holds for BGGen if for every PPT adversary $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\mathsf{BG} = \mathsf{BGGen}(1^\kappa),\ a \xleftarrow{R} \mathbb{Z}_p^* : \tfrac{1}{a}P_i \leftarrow \mathcal{A}(\mathsf{BG}, aP_1, aP_2)\right] \leq \epsilon(\kappa)\ .$$

[3] This is e.g. the case for BN-curves [10]; the most common choice for Type-3 pairings.

co-DHI$_1^*$ is implied by a variant of the decision linear assumption in asymmetric groups stating that given $(\mathsf{BG}, (aP_j, bP_j)_{j\in[2]}, raP_2, sbP_2)$ for $a, b, r, s \xleftarrow{R} \mathbb{Z}_p^*$ it is hard to distinguish $T = (r+s)P_2$ from a random $\mathbb{G}_2$ element. (A co-DHI$_i^*$ solver could be used to compute $\frac{1}{a}P_1$ and $\frac{1}{b}P_1$, which enables to check whether $e(\frac{1}{a}P_1, raP_2)\, e(\frac{1}{b}P_1, sbP_2) = e(P_1, T)$.) This holds analogously for co-DHI$_2^*$.

Generalized Pedersen commitments. These are commitments to a vector of messages $\boldsymbol{m} = (m_i)_{i\in[n]} \in \mathbb{Z}_p^n$ that consist of one group element. They are perfectly hiding and computationally binding under the discrete-log assumption.

$\mathsf{Setup}_\mathsf{P}(1^\kappa, n)$**:** Choose a group $\mathbb{G}$ of prime order p with $\log_2 p = \kappa$ and $n+1$ distinct generators $(P_i)_{i\in[n]}, Q$ and output parameters $\mathsf{cpp} \leftarrow (\mathbb{G}, p, (P_i)_{i\in[n]}, Q)$ (which is an implicit input to the following algorithms).

$\mathsf{Commit}_\mathsf{P}(\boldsymbol{m}; r)$**:** On input a vector $\boldsymbol{m} \in \mathbb{Z}_p^n$ and randomness $r \in \mathbb{Z}_p$, output a commitment $C \leftarrow \sum_{i\in[n]} m_i P_i + rQ$ and an opening $O \leftarrow (\boldsymbol{m}, r)$.

$\mathsf{Open}_\mathsf{P}(C, O)$**:** On input $C \in \mathbb{G}$ and $O = (\boldsymbol{m}, r)$, if $C = \sum_{i\in[n]} m_i P_i + rQ$ then output $\boldsymbol{m} = (m_i)_{i\in[n]}$; else output $\perp$.

Remark 1. $\mathsf{Setup}_\mathsf{P}$ is typically run by a trusted party; it can however also be run by the receiver since commitments are perfectly hiding.

2.1 Structure-Preserving Signatures on Equivalence Classes

Structure-preserving signatures (SPS) [3,4,18,6] can sign elements of a bilinear group without requiring any prior encoding. In such a scheme public keys, messages and signatures consist of group elements only and the verification algorithm evaluates a signature by deciding group membership and evaluating pairing-product equations (PPEs).

The notion of SPS on equivalence classes (SPS-EQ) was introduced by Hanser and Slamanig [34]. Their initial instantiation turned out to only be secure against random-message attacks (cf. [28] and the updated full version of [34]), but together with Fuchsbauer [29] they subsequently presented a scheme that is unforgeable under chosen-message attack (EUF-CMA) in the generic group model.

The concept of SPS-EQ is as follows. Let p be a prime and $\ell > 1$; then $\mathbb{Z}_p^\ell$ is a vector space and we can define a projective equivalence relation on it, which propagates to $\mathbb{G}_i^\ell$ and partitions $\mathbb{G}_i^\ell$ into equivalence classes. Let $\sim_\mathcal{R}$ be this relation, i.e., for $M, N \in \mathbb{G}_i^\ell : M \sim_\mathcal{R} N \Leftrightarrow \exists\, s \in \mathbb{Z}_p^* : M = sN$. An SPS-EQ scheme signs an equivalence class $[M]_\mathcal{R}$ for $M \in (\mathbb{G}_i^*)^\ell$ by signing a representative M of $[M]_\mathcal{R}$. It then allows for switching to other representatives of $[M]_\mathcal{R}$ and updating the signature without access to the secret key. An important property of SPS-EQ is *class-hiding*, which roughly means that two message-signature pairs corresponding to the same class should be unlinkable.

Here, we discuss the abstract model and the security model of such a signature scheme, as introduced in [34].

Definition 6 (Structure-preserving signatures on equivalence classes). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ on $(\mathbb{G}_i^*)^\ell$ (for $i \in \{1, 2\}$) consists of the following PPT algorithms:

$\mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, a bilinear-group generation algorithm, which on input a security parameter κ outputs an asymmetric bilinear group BG.

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$, on input BG and vector length $\ell > 1$, outputs a key pair $(\mathsf{sk}, \mathsf{pk})$.

$\mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$, given a representative $M \in (\mathbb{G}_i^*)^\ell$ and a secret key sk, outputs a signature σ for the equivalence class $[M]_{\mathcal{R}}$.

$\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$, on input a representative $M \in (\mathbb{G}_i^*)^\ell$ of class $[M]_{\mathcal{R}}$, a signature σ on M, a scalar μ and a public key pk, returns an updated message-signature pair (M', σ'), where $M' = \mu \cdot M$ is the new representative and σ' its updated signature.

$\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk})$ is deterministic and, on input a representative $M \in (\mathbb{G}_i^*)^\ell$, a signature σ and a public key pk, outputs 1 if σ is valid for M under pk and 0 otherwise.

$\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$ is a deterministic algorithm, which given a secret key sk and a public key pk outputs 1 if the keys are consistent and 0 otherwise.

An SPS-EQ scheme must satisfy *correctness*, *EUF-CMA security* and *class-hiding*.

Definition 7 (Correctness). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ on $(\mathbb{G}_i^*)^\ell$ is *correct* if for all $\kappa \in \mathbb{N}$, all $\ell > 1$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BGGen}_{\mathcal{R}}(1^\kappa), \ell)$, all messages $M \in (\mathbb{G}_i^*)^\ell$ and all $\mu \in \mathbb{Z}_p^*$: $\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1$,

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

In contrast to standard signatures, EUF-CMA security is defined with respect to equivalence classes, i.e., a forgery is a signature on a message from an equivalence class from which no message has been signed.

Definition 8 (EUF-CMA). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ is *existentially unforgeable under adaptively chosen-message attacks*, if for all PPT algorithms $\mathcal{A}$ with access to a signing oracle $\mathcal{O}$, there is a negligible function $\epsilon(\cdot)$ such that:

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

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

Class-hiding is defined in [34] and uses the following oracles and a list $\mathcal{Q}$ to keep track of queried messages M.

$\mathcal{O}^{RM}$: Pick a message $M \xleftarrow{R} (\mathbb{G}_i^*)^\ell$, append it to $\mathcal{Q}$ and return M.

$\mathcal{O}^{RoR}(M, \mathsf{sk}, \mathsf{pk}, b)$: Given message M, key pair $(\mathsf{sk}, \mathsf{pk})$ and bit b, return $\perp$ if $M \notin \mathcal{Q}$. On the first valid call, record M and $\sigma \leftarrow \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$; if later called on $M' \neq M$, return $\perp$. Pick $R \xleftarrow{R} (\mathbb{G}_i^*)^\ell$ and $\mu \xleftarrow{R} \mathbb{Z}_p^*$, set $(M_0, \sigma_0) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$ and $(M_1, \sigma_1) \leftarrow (R, \mathsf{Sign}_{\mathcal{R}}(R, \mathsf{sk}))$ and return (M_b, σ_b).

$\mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$: Generate a Type-3 bilinear group BG with order p of bitlength κ.

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$: On input BG and vector length $\ell > 1$, choose $(x_i)_{i\in[\ell]} \xleftarrow{R} (\mathbb{Z}_p^*)^\ell$, set $\mathsf{sk} \leftarrow (x_i)_{i\in[\ell]}$, $\mathsf{pk} \leftarrow (\hat{X}_i)_{i\in[\ell]} = (x_i\hat{P})_{i\in[\ell]}$ and output $(\mathsf{sk}, \mathsf{pk})$.

$\mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$: Given a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of class $[M]_{\mathcal{R}}$ and secret key $\mathsf{sk} = (x_i)_{i\in[\ell]}$, choose $y \xleftarrow{R} \mathbb{Z}_p^*$ and output $\sigma = (Z, Y, \hat{Y})$ with

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

$\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk})$: Given $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$, $\sigma = (Z, Y, \hat{Y}) \in \mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ and public key $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]}$, output 1 if the following hold and 0 otherwise:

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

$\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$: Given representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$, $\sigma = (Z, Y, \hat{Y})$, scalar $\mu \in \mathbb{Z}_p^*$ and pk, return $\perp$ if $\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = 0$. Otherwise pick $\psi \xleftarrow{R} \mathbb{Z}_p^*$ and return $(\mu M, \sigma')$ with $\sigma' \leftarrow \left(\psi\mu Z, \frac{1}{\psi}Y, \frac{1}{\psi}\hat{Y}\right)$.

$\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$: Given $\mathsf{sk} = (x_i)_{i\in[\ell]} \in (\mathbb{Z}_p^*)^\ell$ and $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$, output 1 if $x_i\hat{P} = \hat{X}_i \ \forall i \in [\ell]$ and 0 otherwise.

Scheme 1: EUF-CMA-secure construction of an SPS-EQ scheme

Definition 9 (Class-hiding). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ on $(\mathbb{G}_i^*)^\ell$ is called *class-hiding* if for all $\ell > 1$ and PPT adversaries $\mathcal{A}$ with oracle access to $\mathcal{O} \leftarrow \{\mathcal{O}^{RM}, \mathcal{O}^{RoR}(\cdot, \mathsf{sk}, \mathsf{pk}, b)\}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{matrix}\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa),\ b \xleftarrow{R} \{0,1\}, \\ (\mathsf{st}, \mathsf{sk}, \mathsf{pk}) \leftarrow \mathcal{A}(\mathsf{BG}, \ell),\ b^* \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{st}, \mathsf{sk}, \mathsf{pk})\end{matrix} : \begin{matrix} b^* = b \ \wedge \\ \mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1\end{matrix}\right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

Fuchsbauer, Hanser and Slamanig [29] present an EUF-CMA-secure scheme, which we give as Scheme 1, and prove the following.

Theorem 1. *Scheme 1 is EUF-CMA secure against generic forgers and class-hiding under the DDH assumption.*

3 New Results on SPS-EQ

In the following, we present the first standard-model construction of SPS-EQ as modeled in [34]. We then introduce new properties to characterize SPS-EQ constructions, strengthening the notion of class-hiding. Finally, we show how to turn any SPS-EQ construction into an SPS construction. This does not only provide a new, efficient standard-model SPS scheme derived from our SPS-EQ scheme; it also allows us to infer optimality of the SPS-EQ scheme from [29], (Scheme 1) and the impossibility of basing its EUF-CMA security on non-interactive assumptions.

$\mathsf{BGGen}'_{\mathcal{R}}(1^\kappa)$: Output $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$.

$\mathsf{KeyGen}'_{\mathcal{R}}(\mathsf{BG}, \ell)$: Given BG and $\ell > 1$, output $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell + 2)$.

$\mathsf{Sign}'_{\mathcal{R}}(M, \mathsf{sk})$: Given $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ and sk, choose $(R_1, R_2) \xleftarrow{R} (\mathbb{G}_1^*)^2$, compute $\tau \leftarrow \mathsf{Sign}_{\mathcal{R}}((M, R_1, R_2), \mathsf{sk})$ and output $\sigma \leftarrow (\tau, R_1, R_2)$.

$\mathsf{Verify}'_{\mathcal{R}}(M, \sigma, \mathsf{pk})$: Given $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$, signature $\sigma \leftarrow (\tau, R_1, R_2)$ and pk, return $\mathsf{Verify}_{\mathcal{R}}((M, R_1, R_2), \tau, \mathsf{pk})$.

$\mathsf{ChgRep}'_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$: Given $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$, $\sigma \leftarrow (\tau, R_1, R_2)$, $\mu \in \mathbb{Z}_p^*$ and pk, run $((\tilde{M}, \tilde{R}_1, \tilde{R}_2), \tilde{\tau}) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}((M, R_1, R_2), \tau, \mu, \mathsf{pk})$ and output $(\tilde{M}, \tilde{\sigma})$ with $\tilde{\sigma} \leftarrow (\tilde{\tau}, \tilde{R}_1, \tilde{R}_2)$ (or $\perp$ if $\mathsf{ChgRep}_{\mathcal{R}}$ output $\perp$).

$\mathsf{VKey}'_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$: Return $\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$.

Scheme 2: Standard-model SPS-EQ construction from Scheme 1

3.1 A Standard-Model SPS-EQ Construction

Following the approach by Abe et al. [4], we construct from scheme SPS-EQ, given as Scheme 1, an SPS-EQ scheme SPS-EQ′, given as Scheme 2, and prove that it satisfies EUF-CMA and class-hiding, both under non-interactive assumptions.

The scheme for ℓ-length messages is simply Scheme 1 with message space $(\mathbb{G}_1^*)^{\ell+2}$, where before each signing two random group elements are appended to the message. Scheme 2 features constant-size signatures ($4\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements), has public keys of size $\ell + 2$ and still uses 2 PPEs for verification.

Unforgeability follows from a q-type assumption that states that Scheme 1 for $\ell = 2$ is secure against *random-message attacks*. (That is, no PPT adversary, given the public key and signatures on q random messages, can, with non-negligible probability, output a message-signature pair for an equivalence class that was not signed.) Class-hiding follows from class-hiding of Scheme 1. Both proofs can be found in the full version.

3.2 Perfect Adaption of Signatures

We now introduce new definitions characterizing the output distribution of $\mathsf{ChgRep}_{\mathcal{R}}$, which lead to stronger notions than class-hiding. The latter only guarantees that given an *honestly* generated signature σ on M, the output $(\mu M, \sigma')$ of $\mathsf{ChgRep}_{\mathcal{R}}$ for a random μ looks like a random message-signature pair. This however does not protect a user against a signer when the user randomizes a pair obtained from the signer. We thus explicitly require that an adaption of any valid (not necessarily honestly generated) signature is distributed like a fresh signature.

Definition 10 (Perfect adaption of signatures). SPS-EQ on $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures* if for all tuples $(\mathsf{sk}, \mathsf{pk}, M, \sigma, \mu)$ with

$$\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk}) = 1 \qquad \mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = 1 \qquad M \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

$\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$ and $(\mu M, \mathsf{Sign}_{\mathcal{R}}(\mu M, \mathsf{sk}))$ are identically distributed.

We now show the relation between Def. 10 and 9. The following is proven analogously to the proof of class-hiding of Scheme 1 in [29].

Proposition 1. *Let* SPS-EQ *be an SPS-EQ scheme on* $(\mathbb{G}_i^*)^\ell$, $\ell > 1$, *with perfect adaption of signatures. If* $M \xleftarrow{R} [M]_{\mathcal{R}}$ *is computationally indistinguishable from* $M \xleftarrow{R} (\mathbb{G}_i^*)^\ell$ *then* SPS-EQ *is class-hiding.*

Corollary 1. *If the DDH assumption holds in* $\mathbb{G}_i$ *then any SPS-EQ scheme on* $(\mathbb{G}_i^*)^\ell$ *satisfying Def. 10 is class-hiding (Def. 9).*

We note that the converse is not true, as witnessed by Scheme 2: it satisfies class-hiding, but the discrete logs of (R_1, R_2) contained in a signature σ have the same ratio as those of $(\tilde{R}_1, \tilde{R}_2)$ from the output of $\mathsf{ChgRep}_{\mathcal{R}}$.

Maliciously chosen keys. Whereas Def. 10 strengthens Def. 9 in that it considers maliciously generated signatures, the next definition strengthens this further by considering maliciously generated public keys. As there might not even be a corresponding signing key, we cannot compare the outputs of $\mathsf{ChgRep}_{\mathcal{R}}$ to those of $\mathsf{Sign}_{\mathcal{R}}$. We therefore require that $\mathsf{ChgRep}_{\mathcal{R}}$ outputs a random element that satisfies verification.

Definition 11 (Perfect adaption under malicious keys). SPS-EQ on $(\mathbb{G}_i^*)^\ell$ *perfectly adapts signatures under malicious keys* if for all tuples $(\mathsf{pk}, M, \sigma, \mu)$ with

$$\mathsf{Verify}_{\mathcal{R}}(M, \sigma, \mathsf{pk}) = 1 \qquad M \in (\mathbb{G}_i^*)^\ell \qquad \mu \in \mathbb{Z}_p^*$$

we have that $\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$ outputs $(\mu M, \sigma')$ such that σ' is a random element in the space of signatures, conditioned on $\mathsf{Verify}_{\mathcal{R}}(\mu M, \sigma', \mathsf{pk}) = 1$.

Proposition 2. *Scheme 1, from [29], satisfies both Definitions 10 and 11.*

Proof (sketch). For any $M \in (\mathbb{G}_1^*)^\ell$ and $\mathsf{pk} \in (\mathbb{G}_2^*)^\ell$, let $(x_i)_{i\in[\ell]}$ be s.t. $\mathsf{pk} = (x_i\hat{P})_{i\in[\ell]}$. A signature $(Z, Y, \hat{Y}) \in \mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ satisfying $\mathsf{Verify}_{\mathcal{R}}(M, (Z, Y, \hat{Y}), \mathsf{pk}) = 1$ must be of the form $(Z = y\sum x_i M_i, Y = \frac{1}{y}P, \hat{Y} = \frac{1}{y}\hat{P})$ for some $y \in \mathbb{Z}_p^*$. $\mathsf{ChgRep}_{\mathcal{R}}$ outputs $\sigma' = (y\psi\sum x_i \mu M_i, \frac{1}{y\psi}P, \frac{1}{y\psi}\hat{P})$, which is a random element in $\mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ satisfying $\mathsf{Verify}_{\mathcal{R}}(M, \sigma', \mathsf{pk}) = 1$. □

3.3 From SPS-EQ to (Rerandomizable) SPS Schemes

We now show how *any* EUF-CMA-secure SPS-EQ scheme that signs equivalence classes of $(\mathbb{G}_i^*)^{\ell+1}$ with $\ell > 0$ can be turned into an EUF-CMA-secure SPS scheme signing vectors of $(\mathbb{G}_i^*)^\ell$. (We note that SPS schemes typically allow messages from $\mathbb{G}_1$ and/or $\mathbb{G}_2$, which is preferable when used in combination with Groth-Sahai proofs.) The transformation works by embedding messages $(M_i)_{i\in[\ell]} \in (\mathbb{G}_i^*)^\ell$ into $(\mathbb{G}_i^*)^{\ell+1}$ as $M' = ((M_i)_{i\in[\ell]}, P)$ and signing M'. To verify

a signature σ on a message $(M_i)_{i\in[\ell]} \in (\mathbb{G}_i^*)^\ell$ under key pk, one checks whether $\mathsf{Verify}_{\mathcal{R}}(((M_i)_{i\in[\ell]}, P), \sigma, \mathsf{pk}) = 1$.

What we have done is to allow only one single representative of each class, namely the one with P as its last element, a procedure we call *normalization*. EUF-CMA of the SPS-EQ states that no adversary can produce a signature on a message from an unqueried class, which therefore implies EUF-CMA of the resulting SPS scheme.

Moreover, from any SPS-EQ with perfect adaption of signatures the above transformation yields a rerandomizable SPS scheme, since signatures can be rerandomized by running $\mathsf{ChgRep}_{\mathcal{R}}$ for $\mu = 1$ (Def. 10 guarantees that this outputs a random signature). This also means that the lower bounds for SPS over Type-3 groups given by Abe et al. in [4,5] carry over to SPS-EQ: any SPS must use at least 2 PPEs for verification and must have at least 3 signature elements, which cannot be from the same group. Moreover, EUF-CMA security of optimal (that is, 3-element-signature) SPS-EQ schemes cannot be reduced to non-interactive assumptions.

Finally, let us investigate the possibility of SPS-EQ in the Type-1 and Type-2 pairing setting and implied lower bounds. Class-hiding requires the DDH assumption to hold on the message space. This excludes the Type-1 setting, while in Type-2 settings the message space must be $(\mathbb{G}_1^*)^\ell$. In [6] Abe et al. identified the following lower bounds for Type-2 SPS schemes with messages in $\mathbb{G}_1$: 2 PPEs for verification and 3 group elements for signatures. The above transformation converts a Type-2 SPS-EQ into a Type-2 SPS, hence these optimality criteria apply to Type-2 SPS-EQ schemes as well.

Implications. Applying the above transformation to the SPS-EQ scheme from [29] (Scheme 1) yields a perfectly rerandomizable SPS scheme in Type-3 groups with constant-size signatures of unilateral length-ℓ message vectors and public keys of size $\ell + 1$. Scheme 1 is optimal as it only uses 2 PPEs and its signatures consist of 3 bilateral group elements. Hence, by [5] there is no reduction of its EUF-CMA security to a non-interactive assumption and the generic group model proof in [29] is the best one can achieve.

Applying our transformation to Scheme 2 yields a new standard-model SPS construction for unilateral length-ℓ message vectors in Type-3 groups. It has constant-size signatures ($4\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements), a public key of size $\ell + 3$ and uses 2 PPEs for verification; it is therefore almost as efficient as the best known direct SPS construction from non-interactive assumptions in [4], whose signatures consist of $3\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements. Scheme 2 is partially rerandomizable [3], whereas the scheme in [4] is not.

4 Blind Signatures from SPS-EQ

We first present the abstract model for blind signature schemes. Security is defined by unforgeability and blindness and was initially studied in [43,36] and then strengthened in [26,45].

Definition 12 (Blind signature scheme). A blind signature scheme BS consists of the following PPT algorithms:

$\mathsf{KeyGen}_{\mathsf{BS}}(1^\kappa)$, on input a security parameter κ, returns a key pair $(\mathsf{sk}, \mathsf{pk})$.

$(\mathcal{U}_{\mathsf{BS}}(m, \mathsf{pk}), \mathcal{S}_{\mathsf{BS}}(\mathsf{sk}))$ are run by a user and a signer, who interact during execution. $\mathcal{U}_{\mathsf{BS}}$ gets input a message m and a public key pk and $\mathcal{S}_{\mathsf{BS}}$ has input a secret key sk. At the end $\mathcal{U}_{\mathsf{BS}}$ outputs σ, a signature on m, or $\perp$ if the interaction was not successful.

$\mathsf{Verify}_{\mathsf{BS}}(m, \sigma, \mathsf{pk})$ is deterministic and given a message-signature pair (m, σ) and a public key pk outputs 1 if σ is valid on m under pk and 0 otherwise.

A blind signature scheme BS must satisfy *correctness*, *unforgeability* and *blindness*.

Definition 13 (Correctness). A blind signature scheme BS is *correct* if for all $\kappa \in \mathbb{N}$, all $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^\kappa)$, all messages m and $\sigma \leftarrow (\mathcal{U}_{\mathsf{BS}}(m, \mathsf{pk}), \mathcal{S}_{\mathsf{BS}}(\mathsf{sk}))$ it holds that $\mathsf{Verify}_{\mathsf{BS}}(m, \sigma, \mathsf{pk}) = 1$.

Definition 14 (Unforgeability). BS is *unforgeable* if for all PPT algorithms $\mathcal{A}$ having access to a signer oracle, there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{matrix}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^\kappa), \\ (m_i^*, \sigma_i^*)_{i=1}^{k+1} \leftarrow \mathcal{A}^{(\cdot, \mathcal{S}_{\mathsf{BS}}(\mathsf{sk}))}(\mathsf{pk})\end{matrix} : \begin{matrix} m_i^* \neq m_j^* \ \forall i, j \in [k+1], i \neq j \ \ \wedge \\ \mathsf{Verify}_{\mathsf{BS}}(m_i^*, \sigma_i^*, \mathsf{pk}) = 1 \ \forall i \in [k+1]\end{matrix}\right] \leq \epsilon(\kappa) \ ,$$

where k is the number of completed interactions with the oracle.

There are several flavors of blindness. The strongest definition is blindness in the *malicious signer* model [1,42], which allows the adversary to create pk, whereas in the *honest-signer* model the key pair is set up by the experiment. We prove our construction secure under the stronger notion, which was also considered by the recent round-optimal standard-model constructions [31,30].

Definition 15 (Blindness). BS is called *blind* if for all PPT algorithms $\mathcal{A}$ with one-time access to two user oracles, there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{matrix} b \xleftarrow{R} \{0,1\}, \ (\mathsf{pk}, m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}(1^\kappa), \\ \mathsf{st} \leftarrow \mathcal{A}^{(\mathcal{U}_{\mathsf{BS}}(m_b, \mathsf{pk}), \cdot)^{(1)}, (\mathcal{U}_{\mathsf{BS}}(m_{1-b}, \mathsf{pk}), \cdot)^{(1)}}(\mathsf{st}), \\ \text{Let } \sigma_b \text{ and } \sigma_{1-b} \text{ be the resp. outputs of } \mathcal{U}_{\mathsf{BS}}, \\ \text{If } \sigma_0 = \perp \text{ or } \sigma_1 = \perp \text{ then } (\sigma_0, \sigma_1) \leftarrow (\perp, \perp), \\ b^* \leftarrow \mathcal{A}(\mathsf{st}, \sigma_0, \sigma_1)\end{matrix} : \ b^* = b \right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

4.1 Construction

Our construction uses commitments to the messages and SPS-EQ to sign these commitments and to perform blinding and unblinding. Signing an equivalence class with an SPS-EQ scheme lets one derive a signature for arbitrary representatives of this class without knowing the private signing key. This concept provides an elegant way to realize a blind signing process as follows.

$\mathsf{KeyGen}_{\mathsf{BS}}(1^\kappa)$: Compute $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$, $(\mathsf{sk}, \mathsf{pk}_{\mathcal{R}}) \xleftarrow{R} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell = 2)$, pick $q \xleftarrow{R} \mathbb{Z}_p^*$ and set $Q \leftarrow qP$, $\hat{Q} \leftarrow q\hat{P}$. Output $(\mathsf{sk}, \mathsf{pk} = (\kappa, \mathsf{pk}_{\mathcal{R}}, Q, \hat{Q}))$.

$\mathcal{U}_{\mathsf{BS}}^{(1)}(m, \mathsf{pk})$: Given $\mathsf{pk} = (\kappa, \mathsf{pk}_{\mathcal{R}}, Q, \hat{Q})$ and $m \in \mathbb{Z}_p$, compute $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$. If $Q = 0_{\mathbb{G}_1}$ or $e(Q, \hat{P}) \neq e(P, \hat{Q})$ then return $\perp$; else choose $s \xleftarrow{R} \mathbb{Z}_p^*$ and $r \xleftarrow{R} \mathbb{Z}_p$ s.t. $mP + rQ \neq 0_{\mathbb{G}_1}$ and output

$$M \leftarrow (s(mP + rQ), sP) \qquad \mathsf{st} \leftarrow (\mathsf{BG}, \mathsf{pk}_{\mathcal{R}}, Q, M, r, s)$$

$\mathcal{S}_{\mathsf{BS}}(M, \mathsf{sk})$: Given $M \in (\mathbb{G}_1^*)^2$ and secret key sk, output $\pi \leftarrow \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$.

$\mathcal{U}_{\mathsf{BS}}^{(2)}(\mathsf{st}, \pi)$: Parse st as $(\mathsf{BG}, \mathsf{pk}_{\mathcal{R}}, Q, M, r, s)$. If $\mathsf{Verify}_{\mathcal{R}}(M, \pi, \mathsf{pk}_{\mathcal{R}}) = 0$, return $\perp$. Run $((mP + rQ, P), \sigma) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(M, \pi, \frac{1}{s}, \mathsf{pk}_{\mathcal{R}})$ and output $\tau \leftarrow (\sigma, rP, rQ)$.

$\mathsf{Verify}_{\mathsf{BS}}(m, \tau, \mathsf{pk})$: Given $m \in \mathbb{Z}_p^*$, blind signature $\tau = (\sigma, R, T)$ and $\mathsf{pk} = (\kappa, \mathsf{pk}_{\mathcal{R}}, Q, \hat{Q})$, with $Q \neq 0_{\mathbb{G}_1}$ and $e(Q, \hat{P}) = e(P, \hat{Q})$, output 1 if the following holds and 0 otherwise.

$$\mathsf{Verify}_{\mathcal{R}}((mP + T, P), \sigma, \mathsf{pk}_{\mathcal{R}}) = 1 \qquad e(T, \hat{P}) = e(R, \hat{Q})$$

Scheme 3: Blind signature scheme from SPS-EQ

The signer's key contains an element Q under which the obtainer makes a Pedersen commitment $C = mP + rQ$ to the message m. (Since the commitment is perfectly hiding, the signer can be aware of q with $Q = qP$.) The obtainer then forms a vector (C, P), which can be seen as the canonical representative of equivalence class $[(C, P)]_{\mathcal{R}}$. Next, she picks $s \xleftarrow{R} \mathbb{Z}_p^*$ and moves (C, P) to a random representative (sC, sP), which hides C. She sends (sC, sP) to the signer and receives an SPS-EQ signature on it, from which she can derive a signature on the original message (C, P), which she can publish together with an opening of C. As verification will check validity of the SPS-EQ signature on a message ending with P, the unblinding is unambiguous.

Let us now discuss how the user opens the Pedersen commitment $C = mP + rQ$. Publishing (m, r) directly would break blindness of the scheme (a signer could link a pair $M = (D, S)$, received during signing, to a signature by checking whether $D = mS + rqS$). We therefore define a tweaked opening, for which we include $\hat{Q} = q\hat{P}$ in addition to $Q = qP$ in the signer's public key. We define the opening as (m, rP), which can be checked via the pairing equation $e(C - mP, \hat{P}) = e(rP, \hat{Q})$. This opening is still computationally binding under the co-DHI$_1^*$ assumption (in contrast to standard Pedersen commitments, which are binding under the discrete-log assumption). Hiding of the commitment still holds unconditionally, and we will prove the constructed blind-signature scheme secure in the malicious-signer model without requiring a trusted setup.

The scheme is presented as Scheme 3. (Note that for simplicity the blind signature contains $T = rQ$ instead of C.) Correctness follows by inspection.

4.2 Security

Theorem 2. *If the underlying SPS-EQ scheme is EUF-CMA secure and the co-DHI$_1^*$ assumption holds then Scheme 3 is unforgeable.*

The proof, which is given in the full version, follows the intuition that a forger must either forge an SPS-EQ signature on a new commitment or open a commitment in two different ways. The reduction has a natural security loss proportional to the number of signing queries.

Blindness. For the honest-signer model, blindness follows from the DDH assumption and perfect adaption of signatures (Def. 10) of the underlying SPS-EQ scheme. Let $Q \leftarrow qP$ and let q be part of the signing key, and let (P, rP, sP, tP) be a DDH instance. In the blindness game we compute M as $(m \cdot sP + q \cdot tP, sP)$. When the adversary returns a signature on M, we must adapt it to the unblinded message—which we cannot do as we do not know the blinding factor s. By perfect adaption however, an adapted signature is distributed as a fresh signature on the unblinded message, so, knowing the secret key, we can compute a signature σ on $(m \cdot P + q \cdot rP, P)$ and return the blind signature $(\sigma, rP, q \cdot rP)$. If the DDH instance was *real*, i.e., $t = s \cdot r$, then we perfectly simulated the game; if t was random then the adversary's view during issuing was independent of m.

For blindness in the malicious-signer model, we have to deal with two obstacles. (1) We do not have access to the adversarially generated signing key, meaning we cannot recompute the signature on the unblinded message. (2) The adversarially generated public-key values $Q, \hat{Q}$ do not allow us to embed a DDH instance for blinding and unblinding.

We overcome (1) by using the adversary $\mathcal{A}$ itself as a signing oracle by rewinding it. We first run $\mathcal{A}$ to obtain a signature on $(s'(mP + rQ), s'P)$, which, knowing s', we can transform into a signature on $(mP+rQ, P)$. We then rewind $\mathcal{A}$ to the point after outputting its public key and run it again, this time embedding our challenge. In the second run we cannot transform the received signature, instead we use the signature from the first run, which is distributed identically, due to perfect adaption under malicious keys (Def. 11) of the SPS-EQ scheme.

To deal with the second obstacle, we use an interactive variant of the DDH assumption: Instead of being given P, rP, sP and having to distinguish rsP from random, the adversary, for some Q of its choice, is given rP, rQ, sP and must distinguish rsQ from random.

Definition 16 (Assumption 1). We assume that for all PPT algorithms $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that:

$$\Pr\left[\begin{array}{ll} b \xleftarrow{R} \{0,1\},\ \mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa) & \\ (\mathsf{st}, Q, \hat{Q}) \leftarrow \mathcal{A}(\mathsf{BG}),\ r, s, t \xleftarrow{R} \mathbb{Z}_p & : \\ b^* \leftarrow \mathcal{A}(\mathsf{st}, rP, rQ, sP, ((1-b)\cdot t + b \cdot rs)Q) & \end{array} \begin{array}{l} e(Q, \hat{P}) = e(P, \hat{Q}) \\ b^* = b \end{array}\right] - \frac{1}{2} \leq \epsilon(\kappa)\ .$$

Proposition 3. *The assumption in Def. 16 holds in generic groups and reaches the optimal, quadratic simulation-error bound.*

Theorem 3. *If the underlying SPS-EQ scheme has perfect adaption of signatures under malicious keys and Assumption 1 holds then Scheme 3 is blind.*

The proofs can be found in the full version.

4.3 Discussion

Basing our scheme on non-interactive assumptions. Fischlin and Schröder [27] show that the unforgeability of a blind-signature scheme cannot be based on non-interactive hardness assumptions if (1) the scheme has 3 moves or less, (2) its blindness holds statistically and (3) from a transcript one can efficiently decide whether the interaction yielded a valid blind signature. Our scheme satisfies (1) and (3), whereas blindness only holds computationally.

They extend their result in [27] to computationally blind schemes that meet the following conditions: (4) One can efficiently check whether a public key has a matching secret key; this is the case in our setting because of group-membership tests and pairings. (5) Blindness needs to hold relative to a forgery oracle. As written in [27], this does e.g. not hold for Abe's scheme [2], where unforgeability is based on the discrete-log problem and blindness on the DDH problem.

This is the case in our construction too (as one can forge signatures by solving discrete logarithms), hence the impossibility result does not apply to our scheme. Our blind signature construction is black-box from any SPS-EQ with perfect adaption under malicious keys (Def. 11). However, the only known such scheme is the one from [29], which is EUF-CMA secure in the generic-group model, that is, it is based on an interactive assumption. Plugging this scheme into Scheme 3 yields a round-optimal blind signature scheme with unforgeability under this interactive assumption and co-DHI$_1^*$, and blindness (under adversarially chosen keys) under Assumption 1 (Def. 16), which is also interactive.

To construct a scheme under non-interactive assumptions, we would thus have to base blindness on a non-interactive assumption; and find an SPS-EQ scheme satisfying Def. 11 whose unforgeability is proven under a non-interactive assumption.

Efficiency of the construction. When instantiating our blind-signature construction with the SPS-EQ scheme from [29] (given as Scheme 1), which we showed optimal, this yields a public key size of $1\ \mathbb{G}_1 + 3\ \mathbb{G}_2$, a communication complexity of $4\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ and a signature size of $4\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements. For a 80-bit security setting, a blind signature has thus 120 Bytes.

The most efficient scheme from standard assumptions is based on DLIN [30]. Ignoring the increase of the security parameter due to complexity leveraging, their scheme has a public key size of 43 $\mathbb{G}_1$ elements, communication complexity $18 \log_2 q + 41\ \mathbb{G}_1$ elements (where, e.g., we have $\log_2 q = 155$ when assuming that the adversary runs in $\leq 2^{80}$ steps) and a signature size of 183 $\mathbb{G}_1$ elements.

4.4 Round-Optimal Partially Blind Signatures

Partially blind signatures are an extension of blind signatures, where messages contain *common information* γ, which is agreed between the user and the signer.

This requires slight modifications to the unforgeability and blindness notions: An adversary breaks unforgeability if after k signing queries it outputs $k+1$ distinct valid message-signature pairs for the same common information γ^*. In the partial-blindness game m_0 and m_1 must have the same common information γ to prevent the adversary from trivially winning the game. (Formal definitions for partially blind signatures can be found in the full version.)

Construction. We construct a round-optimal partially blind signature scheme $\mathsf{PBS} = (\mathsf{KeyGen}_{\mathsf{PBS}}, (\mathcal{U}_{\mathsf{PBS}}, \mathcal{S}_{\mathsf{PBS}}), \mathsf{Verify}_{\mathsf{PBS}})$ secure in the standard model from an SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ by modifying Scheme 3 as follows. To include common information $\gamma \in \mathbb{Z}_p^*$, $\mathsf{SPS\text{-}EQ}$ is set up for $\ell = 3$. On input $M \leftarrow (s(mP+rQ), sP)$, $\mathcal{S}_{\mathsf{PBS}}$ returns a signature for $M \leftarrow (s(mP+rQ), \gamma \cdot sP, sP)$ and $\mathcal{U}_{\mathsf{PBS}}^{(2)}$ additionally checks correctness of the included γ and returns $\perp$ if this is not the case. Otherwise, it runs $((mP+rQ, \gamma P, P), \sigma) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(M, \pi, \frac{1}{s}, \mathsf{pk})$ and outputs signature $\tau \leftarrow (\sigma, rP, rQ)$ for message m and common information γ. For this construction we obtain the following, whose proofs are analogous to those for Scheme 3.

Theorem 4. *If* $\mathsf{SPS\text{-}EQ}$ *is EUF-CMA secure and the co-DHI*$_1^*$ *assumption holds, then the resulting partially blind signature scheme is unforgeable.*

Theorem 5. *If* $\mathsf{SPS\text{-}EQ}$ *has perfect adaption under malicious keys and Assumption 1 holds, then the resulting partially blind signature scheme is partially blind.*

5 One-Show Anonymous Credentials from SPS-EQ

Baldimtsi and Lysyanskaya [8] introduced blind signatures with attributes and show that they directly yield a one-show anonymous credential system in the vein of Brands [15]. In contrast to Brands' original construction, their construction relies on a provably secure three-move blind signature scheme (in the ROM). In this section we show how to construct two-move blind signatures on message vectors, which straightforwardly yield anonymous one-show credentials that are secure in the standard model.

5.1 Blind Signatures on Message Vectors

Our construction BSV of round-optimal blind signatures on message vectors $\boldsymbol{m} \in \mathbb{Z}_p^n$ simply replaces the Pedersen commitment $mP + rQ$ in Scheme 3 with a generalized Pedersen commitment $\sum_{i\in[n]} m_i P_i + rQ$. Thus, $\mathsf{KeyGen}_{\mathsf{BSV}}$, on input $1^\kappa, n$, additionally outputs generators $(P_i)_{i\in[n]}$ and $\mathsf{Verify}_{\mathsf{BSV}}(\boldsymbol{m}, (\sigma, R, T), \mathsf{pk})$ checks $\mathsf{Verify}_{\mathcal{R}}((\sum_{i\in[n]} m_i P_i + T, P), \sigma, \mathsf{pk}_{\mathcal{R}}) = 1$ and $e(T, \hat{P}) = e(R, \hat{Q})$. Due to space constraints, the construction BSV is detailed in the full version, where we also show the following.

Theorem 6. *If the underlying SPS-EQ scheme is EUF-CMA secure and the co-DHI*$_1^*$ *assumption holds then* BSV *is unforgeable.*

Theorem 7. *If the underlying SPS-EQ scheme has perfect adaption under malicious keys and Assumption 1 holds then* BSV *is blind.*

5.2 Anonymous Credentials Light

The intuition behind our construction is comparable to [8], which roughly works as follows. In the *registration phase*, a user registers (once) a generalized Pedersen commitment C to her attributes and gives a zero-knowledge (ZK) proof of the opening (some attributes may be opened and some may remain concealed). In the *preparation* and *validation phase*, the user engages in a blind-signature-with-attributes protocol for some message m (which is considered the credential serial number) and another commitment C'. C' is a so-called combined commitment obtained from C and a second credential-specific commitment provided by the user. Finally, the credential is the user output of a blind-signature-with-attributes protocol resulting in a signature on message m and a so-called blinded Pedersen commitment C''. The latter contains the same attributes as C, but is unlinkable to C and C'. Showing a credential amounts to presenting C'' along with the blind signature and proving in ZK a desired relation about attributes within C''.

Our construction combines BSV with efficient ZK proofs and is conceptually simpler than the one in [8]. For issuing, the user sends the issuer a blinded version $M \leftarrow (sC, sP)$ of a commitment C to the user's attributes (M corresponds to the blinded generalized Pedersen commitment in [8]). In addition, the user engages in a ZK proof (denoted PoK) proving knowledge of an opening of C (potentially revealing some of the committed attributes). The user obtains a BSV-signature π on M and turns it into a blind signature σ for commitment C by running $((C,P),\sigma) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(M, \pi, \frac{1}{s}, \mathsf{pk})$. The credential consists of C, σ and the randomness r used to produce the commitment. It is showed by sending C and σ and proving in ZK a desired relation about attributes within C.

For ease of presentation, we only consider selective attribute disclosure below. We note that proofs for a rich class of relations [24,20,17] w.r.t. generalized Pederson commitments, as used by our scheme, could be used instead. Henceforth, we denote by S the index set of attributes to be shown and by U those to be withheld. During a showing, a ZK proof of knowledge for a commitment $C = \sum_{i\in[n]} m_i P_i + rQ$ to attributes $(m_i)_{i\in[n]}$ amounts to proving

$$\mathsf{PoK}_{\mathsf{P}}\big\{\big((\alpha_j)_{j\in U}, \beta\big) : C = \textstyle\sum_{i\in S} m_i P_i + \sum_{j\in U} \alpha_j P_j + \beta Q\big\} \ . \tag{1}$$

The proof for a *blinded* commitment $(A,B) = (sC, sP)$ during the obtain phase is done as follows.

$$\mathsf{PoK}_{\mathsf{BP}}\left\{\big((\alpha_j)_{j\in U}, \beta, \gamma\big) : \begin{array}{l} A = \sum_{i\in S} m_i H_i + \sum_{j\in U} \alpha_j H_j + \beta H_Q \ \ \wedge \\ \bigwedge_{i\in[n]}(H_i = \gamma P_i) \wedge H_Q = \gamma Q \wedge B = \gamma P \end{array}\right\} \ . \tag{2}$$

Here the representation is with respect to bases $H_i = sP_i$, $H_Q = sQ$, which are published and guaranteed to be correctly formed by $\mathsf{PoK}_{\mathsf{BP}}$.[4]

[4] In the blindness game, given $B = sP$ from a DDH instance, these bases are simulated as $H_j \leftarrow p_j B$ and $H_Q \leftarrow qB$. We can even prove security in the malicious-signer model by extending the assumption from Def. 16: in addition to Q the adversary outputs $(P_i)_{i\in[n]}$ and receives $(sP_i)_{i\in[n]}$ and sQ.

Construction. As we combine scheme BSV with ZK proofs, we need the following conceptual modifications. The signature $\tau \leftarrow (\sigma, R, T)$ reduces to $\tau \leftarrow \sigma$, since the user provides a ZK-PoK proving knowledge of the randomness r in C. Moreover, verification takes C instead of $\boldsymbol{m}$ as verifiers have only access to the commitment. Consequently, $\mathsf{Verify}_{\mathsf{BSV}}$ of scheme BSV only runs $\mathsf{Verify}_{\mathcal{R}}$.

Setup. The issuer runs $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathsf{BSV}}(1^\kappa, n)$, where n is the number of attributes in the system, and publishes pk as her public key.

Issuing. A user with attribute values $\boldsymbol{m}$ runs $(M, \mathsf{st}) \leftarrow \mathcal{U}^{(1)}_{\mathsf{BSV}}(\boldsymbol{m}, \mathsf{pk}; (s, r))$ (where (s, r) is the chosen randomness), sends the blinded commitment $M = (sC, sP)$ to the issuer and gives a proof $\mathsf{PoK}_{\mathsf{BP}}$ from (2) that M commits to $\boldsymbol{m}$ (where the sets U and S depend on the application). The issuer returns $\pi \leftarrow \mathcal{S}_{\mathsf{BSV}}(M, \mathsf{sk})$ and after running $\sigma \leftarrow \mathcal{U}^{(2)}_{\mathsf{BSV}}(\mathsf{st}, \pi)$ (the outputs rP and rQ are not needed), the user holds a credential (C, σ, r).

Showing. Assume a user with credential (C, σ, r) to the attributes $\boldsymbol{m} = (m_i)_{i \in [n]}$ wants to conduct a selective showing of attributes with a verifier who holds the issuer's public key pk. They engage in a proof $\mathsf{PoK}_{\mathsf{P}}$ from (1) and the verifier additionally checks the signature for the credential by running $\mathsf{Verify}_{\mathsf{BSV}}(C, \sigma, \mathsf{pk})$. If both verifications succeed, the verifier accepts the showing.

Let us finally note that there is no formal security model for one-show credentials. Theorem 2 in [8] informally states that a secure commitment scheme together with a blind signature scheme with attributes implies a one-show credential system. Using the same argumentation as [8], our construction yields a one-show credential system in the standard model.

Acknowledgements

We would like to thank the anonymous reviewers for their valuable comments.

References

1. Abdalla, M., Namprempre, C., Neven, G.: On the (Im)possibility of Blind Message Authentication Codes. In: CT-RSA. LNCS, vol. 3860, pp. 262–279. Springer (2006)
2. Abe, M.: A Secure Three-Move Blind Signature Scheme for Polynomially Many Signatures. In: EUROCRYPT. LNCS, vol. 2045, pp. 136–151. Springer (2001)
3. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-Preserving Signatures and Commitments to Group Elements. In: CRYPTO. LNCS, vol. 6223, pp. 209–236. Springer (2010)
4. Abe, M., Groth, J., Haralambiev, K., Ohkubo, M.: Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. In: CRYPTO. LNCS, vol. 6841, pp. 649–666. Springer (2011)
5. Abe, M., Groth, J., Ohkubo, M.: Separating Short Structure-Preserving Signatures from Non-interactive Assumptions. In: ASIACRYPT. LNCS, vol. 7073, pp. 628–646. Springer (2011)
6. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Structure-Preserving Signatures from Type II Pairings. In: CRYPTO. LNCS, vol. 8616, pp. 390–407. Springer (2014)

7. Abe, M., Okamoto, T.: Provably Secure Partially Blind Signatures. In: CRYPTO. LNCS, vol. 1880, pp. 271–286. Springer (2000)
8. Baldimtsi, F., Lysyanskaya, A.: Anonymous Credentials Light. In: ACM CCS (2013)
9. Baldimtsi, F., Lysyanskaya, A.: On the Security of One-Witness Blind Signature Schemes. In: ASIACRYPT (2). LNCS, vol. 8270, pp. 82–99. Springer (2013)
10. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: SAC. pp. 319–331 (2005)
11. Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. J. Cryptology 16(3), 185–215 (2003)
12. Blazy, O., Fuchsbauer, G., Pointcheval, D., Vergnaud, D.: Signatures on Randomizable Ciphertexts. In: PKC. LNCS, vol. 6571, pp. 403–422. Springer (2011)
13. Blazy, O., Pointcheval, D., Vergnaud, D.: Compact Round-Optimal Partially-Blind Signatures. In: SCN. LNCS, vol. 7485, pp. 95–112. Springer (2012)
14. Boldyreva, A.: Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: PKC. LNCS, vol. 2567, pp. 31–46. Springer (2003)
15. Brands, S.: Rethinking Public-Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press (2000)
16. Brands, S., Paquin, C.: U-Prove Cryptographic Specification v1 (2010)
17. Bresson, E., Stern, J.: Proofs of Knowledge for Non-monotone Discrete-Log Formulae and Applications. In: ISC. LNCS, vol. 2433, pp. 272–288. Springer (2002)
18. Camenisch, J., Dubovitskaya, M., Haralambiev, K.: Efficient Structure-Preserving Signature Scheme from Standard Assumptions. In: SCN. LNCS, vol. 7485, pp. 76–94. Springer (2012)
19. Camenisch, J., Koprowski, M., Warinschi, B.: Efficient Blind Signatures Without Random Oracles. In: SCN. pp. 134–148 (2004)
20. Camenisch, J., Michels, M.: Proving in Zero-Knowledge that a Number Is the Product of Two Safe Primes. In: EUROCRYPT. LNCS, vol. 1592, pp. 107–122. Springer (1999)
21. Chatterjee, S., Menezes, A.: On cryptographic protocols employing asymmetric pairings - the role of ψ revisited. Discrete Applied Mathematics 159(13), 1311–1322 (2011)
22. Chaum, D.: Blind Signatures for Untraceable Payments. In: CRYPTO'82. pp. 199–203. Plenum Press (1982)
23. Chaum, D.: Blind signature system. In: CRYPTO. p. 153 (1983)
24. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In: CRYPTO'94. LNCS, vol. 839, pp. 174–187. Springer
25. Fischlin, M.: Round-Optimal Composable Blind Signatures in the Common Reference String Model. In: CRYPTO. LNCS, vol. 4117, pp. 60–77. Springer (2006)
26. Fischlin, M., Schröder, D.: Security of Blind Signatures under Aborts. In: PKC. LNCS, vol. 5443, pp. 297–316. Springer (2009)
27. Fischlin, M., Schröder, D.: On the Impossibility of Three-Move Blind Signature Schemes. In: EUROCRYPT. LNCS, vol. 6110, pp. 197–215. Springer (2010)
28. Fuchsbauer, G.: Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014. Cryptology ePrint Archive, Report 2014/892 (2014)
29. Fuchsbauer, G., Hanser, C., Slamanig, D.: EUF-CMA-Secure Structure-Preserving Signatures on Equivalence Classes. Cryptology ePrint Archive, Report 2014/944 (2014)

30. Garg, S., Gupta, D.: Efficient Round Optimal Blind Signatures. In: EUROCRYPT. LNCS, vol. 8441, pp. 477–495. Springer (2014)
31. Garg, S., Rao, V., Sahai, A., Schröder, D., Unruh, D.: Round Optimal Blind Signatures. In: CRYPTO. pp. 630–648 (2011)
32. Ghadafi, E., Smart, N.P.: Efficient Two-Move Blind Signatures in the Common Reference String Model. In: ISC. LNCS, vol. 7483, pp. 274–289. Springer (2012)
33. Groth, J., Sahai, A.: Efficient Non-interactive Proof Systems for Bilinear Groups. In: EUROCRYPT'08. LNCS, vol. 4965, pp. 415–432. Springer (2008)
34. Hanser, C., Slamanig, D.: Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials. In: ASIACRYPT (2014), Full version: Cryptology ePrint Archive, Report 2014/705
35. Hazay, C., Katz, J., Koo, C.Y., Lindell, Y.: Concurrently-Secure Blind Signatures Without Random Oracles or Setup Assumptions. In: TCC. LNCS, vol. 4392, pp. 323–341. Springer (2007)
36. Juels, A., Luby, M., Ostrovsky, R.: Security of Blind Digital Signatures (Extended Abstract). In: CRYPTO '97. LNCS, vol. 1294, pp. 150–164. Springer (1997)
37. Kiayias, A., Zhou, H.S.: Concurrent Blind Signatures Without Random Oracles. In: SCN. LNCS, vol. 4116, pp. 49–62. Springer (2006)
38. Lindell, Y.: Bounded-concurrent secure two-party computation without setup assumptions. In: STOC. pp. 683–692. ACM (2003)
39. Lysyanskaya, A., Rivest, R.L., Sahai, A., Wolf, S.: Pseudonym Systems. In: SAC '00. LNCS, vol. 1758, pp. 184–199. Springer (2000)
40. Meiklejohn, S., Shacham, H., Freeman, D.M.: Limitations on Transformations from Composite-Order to Prime-Order Groups: The Case of Round-Optimal Blind Signatures. In: ASIACRYPT. LNCS, vol. 6477, pp. 519–538. Springer (2010)
41. Okamoto, T.: Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In: CRYPTO. LNCS, vol. 740, pp. 31–53. Springer (1992)
42. Okamoto, T.: Efficient Blind and Partially Blind Signatures Without Random Oracles. In: TCC. LNCS, vol. 3876, pp. 80–99. Springer (2006)
43. Pointcheval, D., Stern, J.: Security Arguments for Digital Signatures and Blind Signatures. J. Cryptology 13(3), 361–396 (2000)
44. Rückert, M.: Lattice-based blind signatures. In: ASIACRYPT. pp. 413–430 (2010)
45. Schröder, D., Unruh, D.: Security of Blind Signatures Revisited. In: PKC. LNCS, vol. 7293, pp. 662–679. Springer (2012)
46. Seo, J.H., Cheon, J.H.: Beyond the Limitation of Prime-Order Bilinear Groups, and Round Optimal Blind Signatures. In: TCC. LNCS, vol. 7194, pp. 133–150. Springer (2012)