Efficient Round-Optimal Blind Signatures in the Standard Model

Essam Ghadafi(✉)

University of the West of England, Bristol, UK
essam.ghadafi@uwe.ac.uk

Abstract. Blind signatures are at the core of e-cash systems and have numerous other applications. In this work we construct efficient blind and partially blind signature schemes over bilinear groups in the standard model. Our schemes yield short signatures consisting of only a couple of elements from the shorter source group and have very short communication overhead consisting of 1 group element on the user side and 3 group elements on the signer side. At 80-bit security, our schemes yield signatures consisting of only 40 bytes which is 67% shorter than the most efficient existing scheme with the same security in the standard model. Verification in our schemes requires only a couple of pairings. Our schemes compare favorably in every efficiency measure to all existing counterparts offering the same security in the standard model. In fact, the efficiency of our signing protocol as well as the signature size compare favorably even to many existing schemes in the random oracle model. For instance, our signatures are shorter than those of Brands' scheme which is at the heart of the U-Prove anonymous credential system used in practice. The unforgeability of our schemes is based on new intractability assumptions of a "one-more" type which we show are intractable in the generic group model, whereas their blindness holds w.r.t. malicious signing keys in the information-theoretic sense. We also give variants of our schemes for a vector of messages.

Keywords: Blind signatures · Round-optimal · Partial blindness E-Cash

1 Introduction

Blind signatures introduced by Chaum [23] are an interactive protocol that allows a user to obtain signatures on messages of her choice without revealing the messages to the signer. Blindness in these schemes ensures that it is infeasible for a malicious signer to link the final signatures to their corresponding signing requests. Blindness can be either proven in the honest-key model where the

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007–2013)/ERC Grant Agreement n. 307937 and EPSRC grant EP/J009520/1. The work was done while the author was at University College London.

A. Kiayias (Ed.): FC 2017, LNCS 10322, pp. 455–473, 2017.
https://doi.org/10.1007/978-3-319-70972-7_26

key pair is produced by the challenger and then revealed to the adversary or in the stronger malicious-key model [1,49] where the key pair is chosen by the adversary herself and she is not required to reveal the signing key to the challenger. On the other hand, unforgeability ensures that it is infeasible for a malicious user to obtain more valid signatures on distinct messages than the number of completed interactions with the honest signer. Such a primitive is at the core of e-cash systems [23] where the bank acts as the signer; the privacy requirement comes from the non-traceability requirement of cash. It also finds applications in e-voting [34], anonymous credentials [8] and direct anonymous attestation [12,20]. The primitive is very relevant to practice, besides its prominent role in realizing e-cash systems, blind signatures are the backbone of some anonymous credential systems deployed in practice, which include the U-Prove system [19].

Measures of importance when designing such schemes include their round complexity, i.e. the number of moves between the parties before the user can derive a signature. Round-optimal schemes [27] consisting of only two moves are known to imply security under concurrent executions.

Related Work. After their introduction by Chaum [23], a long line of research on blind signatures has evolved. Constructions of blind signatures relying on random oracles [26] include [2,8,11,15,18,23,52–54]. Most of the early constructions relying on random oracles are essentially Full-Domain-Hash (FDH) style signatures. The user sends a blinded message digest of the message to the signer who in turn returns a signature on such a digest. Upon receiving the signature, thanks to the homomorphic property of the underlying signature scheme, the user is able to transform such a signature to one on the message. This is the underlying idea behind the original (RSA based) scheme in [23] which was proven secure in [52]. The same applies to the (DLog based) scheme in [15].

Constructions dispensing with relying on random oracles but at the expense of assuming a trusted common reference string (CRS) include [6,21,40,46]. Fischlin [27] gave a generic construction of two-move schemes in the CRS model satisfying blindness in the malicious-key model. His construction requires the user to send a commitment to her message which in turn gets signed by the signer. The final signature is then merely a zero-knowledge proof of knowledge of a signature on the (hidden) commitment to the message. Most subsequent constructions in the CRS model are either direct instantiations of Fischlin's construction, e.g. [3,5], or variations thereof, e.g. [3,30]. The scheme in [3,30] adopts a similar approach as Fischlin's but instead of hiding the signed commitment, it exploits a feature of the underlying signature scheme to transform a signature on the commitment to a signature on the message itself. Other round-optimal constructions in the CRS model include [13,14,48,56].

Round-optimal constructions not relying on either of the aforementioned assumptions, i.e. in the standard model, are preferable. However, it is well-known that such schemes are harder to design. Lindell [47] showed that it is impossible to design round-optimal schemes in the standard model conforming to simulation-based (rather than game-based) security definitions. However, Hazay et al. [44] showed that (non-round-optimal) realizations are possible under game-based definitions. Abe and Ohkubo [6] showed that universally composable blind signatures, even non-committing ones, are impossible in the standard model. Okamoto [49] gave a non-round-optimal construction in the standard model which satisfies blindness in the malicious-key model. Fischlin and Schröder [29] proved that it is impossible to reduce the security of a standard-model blind signature scheme in a blackbox manner to the intractability of a non-interactive assumption if the scheme has any of the following properties: (i) the signing protocol has less than 4 moves. (ii) Its blindness holds statistically (iii) the signing transcript allows one to check if a valid signature can be derived from it.

Existing constructions in the standard model [36,37] circumvent the impossibility result by making use of a non-blackbox reduction to the underlying primitive. Garg et al. [37] gave the first round-optimal construction in the standard model solving a long-standing open problem. Their scheme combines fully homomorphic encryption with two-move witness-indistinguishable proofs known otherwise as ZAPs [25]. Their scheme is inefficient and is only considered as a feasibility result. Recently, Garg and Gupta [36] gave a more efficient round-optimal construction which combines structure-preserving signature schemes [3] and Groth-Sahai NIZK proofs [41]. To eliminate the need for a trusted party, they use two CRSs which are part of the signer's public key. The signer is forced to choose those honestly as otherwise she needs to solve an exponential-time problem in order to cheat. The security of their scheme holds w.r.t. non-uniform adversaries and relies on complexity leveraging. Consequently, it suffers from a large communication overhead and a rather large computational cost.

Recently, Fuchsbauer et al. [33] gave a semi-generic construction of round-optimal schemes in the standard model which combines the Pedersen commitment scheme [50] with structure-preserving signatures on equivalence classes [42]. Their construction satisfies blindness against malicious keys. They gave an efficient instantiation whose security relies on a couple of interactive assumptions where they used the optimal construction of signature on equivalence classes from [32]. More recently, Fuchsbauer et al. [31] weakened the assumptions on which the instantiation in [33] is based by eliminating one of the interactive assumptions on which the blindness in [33] was relying. However, the unforgeability of the new variant still relies on an interactive intractability assumption. Hanzlik and Kluczniak [43] gave a construction in the standard model in the honest-key model. The downside of their construction is that it uses an encryption scheme over composite-order groups which requires groups of a large order as well as a strong non-standard "knowledge" assumption [9]. Very recently, Döttling et al. [24] showed that blind signatures in the standard model can be constructed from maliciously circuit-private homomorphic encryption for logarithmic depth circuits.

Baldimtsi and Lysyanskaya [7] showed that existing techniques fall short for proving the security of some existing blind signatures lacking a security proof in the random oracle model. Concerned constructions include Schnorr's [54] and Brands' [18] schemes. The latter is at the core of the U-Prove system.

Abe and Fujisaki [4] put forward the notion of partially blind signatures which extends blind signatures to allow some part of the message to be public. This makes it possible to attach some public attributes, e.g. an expiration date, to the signatures. Recently, Fuchsbauer et al. [31,33] gave the first efficient round-optimal partially blind schemes in the standard model.

Our Contribution. We construct two efficient blind signature schemes in the standard model satisfying blindness in the malicious-key model. Our schemes yield very short signatures consisting of only a pair of elements from the shorter source group. At 80-bit security, our signatures are only 40 bytes long which means they are 67% shorter than the best existing scheme offering the same security [33]. Verifying signatures in our schemes involves evaluating a couple of pairings. The latter matches the verification overhead of the most efficient existing (non-blind) signature schemes over bilinear groups [16,17]. Such desirable efficiency means that our schemes can even be deployed on devices with limited computational power if the evaluation of pairings required for verification is outsourced to a third party, e.g. using techniques from [22]. Our schemes have a very low communication overhead on both sides. The blindness of our schemes holds in the information-theoretic sense whereas their unforgeability relies on new intractability assumptions which we show hold in the generic group model [57]. Note that it is well-known that blind signature schemes in the standard model based solely on non-interactive assumptions, e.g. [36,37], are much less efficient. Furthermore, all existing efficient round-optimal schemes in the standard model offering the same security as ours [31,33] also rely on interactive intractability assumptions.

We also construct efficient partially blind signature schemes and efficient blind signature schemes for a vector of messages. The techniques underlying our constructions are akin to the blind-unblind paradigm which usually form the basis of the efficient constructions in the random oracle model. However, to obtain the desired efficiency in the standard model, we apply various techniques. Similarly to [31,33,40], our constructions do not require expensive zero-knowledge proofs.

Paper Organization. The rest of the paper is organized as follows. In Sect. 2, we give some preliminary definitions. In Sect. 3, we introduce and prove intractability of our new assumptions. In Sect. 4, we recall the syntax and security of blind signatures. In Sect. 5, we give our blind signature constructions. We show in Sect. 6 how to extend our schemes to sign a vector of messages. In Sect. 7, we give our partially blind signature constructions.

Notation. We write $b = \mathsf{Alg}(a; r)$ when algorithm Alg on input a and randomness r outputs b. We write $b \leftarrow \mathsf{Alg}(a)$ for the process of setting $b = \mathsf{Alg}(a; r)$ where r is sampled at random. For an algorithm Alg and an oracle $\mathcal{O}$, $\mathsf{Alg}^{\mathcal{O}^k(\cdot)}$ denotes that Alg can access $\mathcal{O}$ at most k times on inputs of Alg's choice. We write $a \leftarrow \mathcal{S}$ for sampling a uniformly at random from the set $\mathcal{S}$. A function $\nu(.) : \mathbb{N} \rightarrow \mathbb{R}^+$ is negligible (in λ) if for every polynomial $\rho(\cdot)$ and all sufficiently large values of λ, it holds that $\nu(\lambda) < \frac{1}{\rho(\lambda)}$. PPT stands for running in probabilistic polynomial time in the relevant security parameter. For $\ell \in \mathbb{N} \setminus \{0\}$, by $[\ell]$ we denote the set $\{1, \ldots, \ell\}$.

2 Preliminaries

In this section we provide some preliminary definitions.

Bilinear Groups. A bilinear group is a tuple $\mathcal{P} := (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{T}, p, G, \hat{G}, e)$ where $\mathbb{G}$, $\hat{\mathbb{G}}$ and $\mathbb{T}$ are groups of a prime order p, and G and $\hat{G}$ generate $\mathbb{G}$ and $\hat{\mathbb{G}}$, respectively. The function e is a non-degenerate bilinear map $e : \mathbb{G} \times \hat{\mathbb{G}} \longrightarrow \mathbb{T}$. To distinguish between elements of $\mathbb{G}$ and $\hat{\mathbb{G}}$, the latter will be accented with $\hat{}$. We use multiplicative notation for all the groups. We let $\mathbb{G}^{\times} := \mathbb{G} \setminus \{1_{\mathbb{G}}\}$ and $\hat{\mathbb{G}}^{\times} := \hat{\mathbb{G}} \setminus \{1_{\hat{\mathbb{G}}}\}$. In this paper, we work in the efficient Type-III setting [35], where $\mathbb{G} \neq \hat{\mathbb{G}}$ and there is no efficiently computable isomorphism between the groups in either direction. We assume there is an algorithm $\mathcal{BG}$ that on input a security parameter λ, outputs a description of bilinear groups. Without loss in generality and similarly to e.g. [31,33] in this work we will assume $\mathcal{BG}$ is deterministic, which as argued by [31,33] is the case for instance in the most widely used groups based on BN curves [10].

Pedersen Commitment Scheme. We use a generalized variant of the Pedersen commitment scheme [50] which allows committing to a vector of messages at once. The scheme is information-theoretically hiding and computationally binding under the discrete logarithm assumption. The generalized variant is defined by the following algorithms:

$\mathsf{Setup}(1^{\lambda}, n)$ On input the security parameter λ and the size of the vector n, this algorithm chooses a cyclic group $\mathbb{G}$ of prime order p where $\log p \in \Theta(\lambda)$. It also samples the elements $G_1, \ldots, G_n, H \leftarrow \mathbb{G}$. It returns the commitment key $\mathsf{ck} := (G_1, \ldots, G_n, H)$ which we assume is an implicit input to the rest of the algorithms.

$\mathsf{Commit}(\boldsymbol{m}, r)$ On input a message vector $\boldsymbol{m} = (m_1, \ldots, m_n) \in \mathbb{Z}_p^n$ and a randomness $r \in \mathbb{Z}_p$, this algorithm returns the commitment $\mathsf{Co} := H^r \prod_{i=1}^{n} G_i^{m_i}$ and the opening information $d := (\boldsymbol{m}, r)$.

$\mathsf{Open}(\mathsf{Co}, d = (\boldsymbol{m}, r))$ On input a commitment Co and its associated opening information d, this algorithm verifies whether such opening information is a valid one by checking that $\mathsf{Co} = H^r \prod_{i=1}^{n} G_i^{m_i}$ returning 1 or 0 accordingly.

Since the hiding property of the scheme holds in the information-theoretic sense, such a property still holds even if we let the recipient runs the Setup algorithm which is otherwise usually run by a trusted third party. The above argument holds as long as $H \neq 1_{\mathbb{G}}$ which is easy to check.

3 New Intractability Assumptions

In this section we introduce some new assumptions of a "one-more" type where the adversary interacts with an oracle k times and is tasked with outputting $k+1$ valid tuples. They are similar in nature to the E-LRSW assumption introduced by Ghadafi and Smart [40].

3.1 The BSOM Assumption

Our first new assumption which we refer to as the BSOM (short for Blind Signature One More) assumption will form the basis for the unforgeability of our first blind signature construction. It is inspired in part by the assumption underlying the recent signature scheme by Ghadafi [38].

Definition 1 (BSOM Assumption). *Let* $\mathcal{P} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{T}, G, \hat{G}, e, p)$ *be the description of Type-III bilinear groups output by* $\mathcal{BG}(1^\lambda)$*, and let* $H := G^h$*,* $\hat{H} := \hat{G}^h$*,* $\hat{X} := \hat{G}^x$*,* $\hat{Y} := \hat{G}^y$ *for some* $h, x, y \leftarrow \mathbb{Z}_p$*. Let* $\mathcal{O}BSOM_{H,\hat{H},\hat{X},\hat{Y}}(\cdot)$ *be an oracle that on input a message* $M = G^m$ *(for some possibly unknown* $m \in \mathbb{Z}_p$*) returns a triple* $\left(A := G^a, B := (G^x M)^{\frac{a}{y}}, C := H^{\frac{a}{y}}\right) \in \mathbb{G}^3$ *for some* $a \leftarrow \mathbb{Z}_p$*. We say the BSOM assumption holds (relative to* $\mathcal{BG}$*) if for all PPT adversaries* $\mathcal{A}$*, the following advantage is negligible (in* λ*):*

$$\Pr\left[\begin{array}{l}\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, x, y \leftarrow \mathbb{Z}_p;\ (H, \hat{H}, \hat{X}, \hat{Y}) := (G^h, \hat{G}^h, \hat{G}^x, \hat{G}^y);\\ \{(A_i, B_i, m_i)\}_{i=1}^{k+1} \leftarrow \mathcal{A}^{\mathcal{O}BSOM^k_{H,\hat{H},\hat{X},\hat{Y}}(\cdot)}\left(\mathcal{P}, H, \hat{H}, \hat{X}, \hat{Y}\right) :\\ \left|\{m_i\}_{i=1}^{k+1}\right| = k+1 \ \wedge\ \forall i \in [k+1] :\ A_i \neq 1_{\mathbb{G}} \wedge e(B_i, \hat{Y}) = e(A_i, \hat{X}\hat{G}^{m_i})\end{array}\right]$$

The proof for the following theorem can be found in the full version [39].

Theorem 1. *For any generic adversary* $\mathcal{A}$ *against the BSOM assumption, if* p *is the (prime) order of the bilinear group and* $\mathcal{A}$ *makes* q_G *group operation queries,* q_P *pairing queries and* q_O *queries to the BSOM oracle* $\mathcal{O}BSOM_{H,\hat{H},\hat{X},\hat{Y}}$*, then the probability of* $\mathcal{A}$ *against the BSOM assumption is* $\mathcal{O}(\frac{q_G^2 q_O + q_P^2 q_O + q_O^3}{p})$*.*

3.2 The BSOMI Assumption

Our second new assumption which we refer to as the BSOMI assumption will form the basis for the unforgeability of our second blind signature construction. It is inspired in part by the assumption underlying the recent signature scheme by Pointcheval and Sanders [51].

Definition 2 (BSOMI Assumption). *Let* $\mathcal{P} = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{T}, G, \hat{G}, e, p)$ *be the description of Type-III bilinear groups output by* $\mathcal{BG}(1^\lambda)$*, and let* $H := G^h$*,* $\hat{H}' := \hat{G}^{\frac{1}{h}}$*,* $\hat{X} := \hat{G}^x$*,* $\hat{Y} := \hat{G}^y$ *for some* $h, x, y \leftarrow \mathbb{Z}_p$*. Let* $\mathcal{O}BSOMI_{H,\hat{H}',\hat{X},\hat{Y}}(\cdot)$ *be an oracle that on input a message* $M := G^m$ *(for some possibly unknown* $m \in \mathbb{Z}_p$*) returns a triple* $\left(A := G^a, B := A^x M^{ay}, C := H^{ay}\right) \in \mathbb{G}^3$ *for some* $a \leftarrow \mathbb{Z}_p$*. We say the BSOMI assumption holds (relative to* $\mathcal{BG}$*) if for all PPT adversaries* $\mathcal{A}$*, the following advantage is negligible (in* λ*):*

$$\Pr\left[\begin{array}{l}\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, x, y \leftarrow \mathbb{Z}_p;\ (H, \hat{H}', \hat{X}, \hat{Y}) := (G^h, \hat{G}^{\frac{1}{h}}, \hat{G}^x, \hat{G}^y);\\ \{(A_i, B_i, m_i)\}_{i=1}^{k+1} \leftarrow \mathcal{A}^{\mathcal{O}BSOMI^k_{H,\hat{H}',\hat{X},\hat{Y}}(\cdot)}\left(\mathcal{P}, H, \hat{H}', \hat{X}, \hat{Y}\right) :\\ \left|\{m_i\}_{i=1}^{k+1}\right| = k+1 \ \wedge\ \forall i \in [k+1] :\ A_i \neq 1_{\mathbb{G}} \wedge e(B_i, \hat{G}) = e(A_i, \hat{X}\hat{Y}^{m_i})\end{array}\right]$$

The proof for the following theorem can be found in the full version [39].

Theorem 2. *For any generic adversary $\mathcal{A}$ against the BSOMI assumption, if p is the (prime) order of the bilinear group and $\mathcal{A}$ makes q_G group operation queries, q_P pairing queries and q_O queries to the BSOMI oracle $\mathcal{O}BSOMI_{H,\hat{H}',\hat{X},\hat{Y}}$, then the probability of $\mathcal{A}$ against the BSOMI assumption is $\mathcal{O}(\frac{q_G^2 q_O + q_P^2 q_O + q_O^3}{p})$.*

4 Syntax and Security of Blind Signatures

In this section, we define the syntax and security of blind signatures. Since we are interested in round-optimal schemes, we will specialize our definitions to this case. A blind signature scheme BS (with a two-move signature request) consists of the following polynomial-time algorithms:

$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda)$ On input a security parameter 1^λ, this probabilistic algorithm outputs a pair $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}})$ of public/secret keys for the signer. Without loss of generality we assume the security parameter is an implicit input to the rest of the algorithms.

$\mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m)$: This algorithm run by the user takes as input a message m in the message space $\mathcal{M}$ and the public key $\mathsf{vk}_{\mathsf{BS}}$, and produces a signature request ρ, plus some state st (which is assumed to contain m).

$\mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}}, \rho)$: This probabilistic algorithm run by the signer takes as input the secret key $\mathsf{sk}_{\mathsf{BS}}$ and the signature request ρ, and produces a pre-signature β.

$\mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta, \mathsf{st})$: On input the public key $\mathsf{vk}_{\mathsf{BS}}$, the pre-signature β, and the state st, this algorithm produces a blind signature σ on m, or it outputs $\perp$ if it does not accept the transcript.

$\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m, \sigma)$: This deterministic algorithm outputs 1 if σ is a valid signature on the message m, or 0 otherwise.

(Perfect) correctness of blind signatures requires that for all $\lambda \in \mathbb{N}$ and all $m \in \mathcal{M}$, we have

$$\Pr\left[\begin{array}{l}(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda);\ (\rho, \mathsf{st}) \leftarrow \mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m);\\ \beta \leftarrow \mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}}, \rho); \sigma \leftarrow \mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta, \mathsf{st}) : \mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m, \sigma) = 1\end{array}\right] = 1.$$

Security of blind signatures [45,52] which was strengthened by [28,55] requires blindness and unforgeability.

Unforgeability. Unforgeability requires that it is infeasible for an adversarial user who interacts with an honest signer on k occasions to output $k+1$ valid signatures on $k+1$ distinct messages.

Definition 3 (Unforgeability). *A blind scheme* BS *satisfies unforgeability if for all $\lambda \in \mathbb{N}$, for all PPT adversaries $\mathcal{A}$, the advantage* $\mathsf{Adv}^{Unforge}_{\mathsf{BS},\mathcal{A}}(\lambda)$ *against the game* $\mathsf{Exp}^{Unforge}_{\mathsf{BS},\mathcal{A}}$ *defined in Fig. 1. is negligible (in λ) where*

$$\mathsf{Adv}^{Unforge}_{\mathsf{BS},\mathcal{A}}(\lambda) = \Pr[\mathsf{Exp}^{Unforge}_{\mathsf{BS},\mathcal{A}}(\lambda) = 1].$$

```
Experiment: $\mathsf{Exp}^{\mathrm{Unforge}}_{\mathsf{BS},\mathcal{A}}(\lambda)$
- $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^{\lambda})$
- $\{(m_i, \sigma_i)\}_{i=1}^{k+1}\} \leftarrow \mathcal{A}^{\mathsf{Issue}^{k}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}}, \cdot)}(\mathsf{vk}_{\mathsf{BS}})$
- Return 0 if any of the following holds:
  - $\exists i, j \in [k+1]$, with $i \neq j$ but $m_i = m_j$
  - $\exists i \in [k+1]$ s.t. $\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m_i, \sigma_i) = 0$
- Return 1
```

```
Experiment: $\mathsf{Exp}^{\mathrm{Blind}}_{\mathsf{BS},\mathcal{A}}(\lambda)$
- $(\mathsf{vk}_{\mathsf{BS}}, m_0, m_1, \mathsf{st}_{\mathsf{find}}) \leftarrow \mathcal{A}_{\mathsf{find}}(\lambda)$
- $b \leftarrow \{0, 1\}$
- $(\rho_b, \mathsf{st}_b) \leftarrow \mathsf{Request}^{0}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m_0)$
- $(\rho_{1-b}, \mathsf{st}_{1-b}) \leftarrow \mathsf{Request}^{0}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m_1)$
- $(\beta_0, \beta_1, \mathsf{st}_{\mathsf{issue}}) \leftarrow \mathcal{A}_{\mathsf{issue}}(\rho_0, \rho_1, \mathsf{st}_{\mathsf{find}})$
- $\sigma_0 \leftarrow \mathsf{Request}^{1}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta_b, \mathsf{st}_b)$
- $\sigma_1 \leftarrow \mathsf{Request}^{1}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta_{1-b}, \mathsf{st}_{1-b})$
- If $\sigma_0 = \perp$ or $\sigma_1 = \perp$ Then Return 0
- $b^* \leftarrow \mathcal{A}_{\mathsf{guess}}(\sigma_0, \sigma_1, \mathsf{st}_{\mathsf{issue}})$
- Return 1 if $b = b^*$ Else Return 0
```

Fig. 1. The security experiments for unforgeability (left) and blindness w.r.t. malicious keys (right)

Blindness. Blindness (w.r.t. malicious keys [1,49]) requires that an adversarial signer who freely chooses two messages m_0 and m_1 as well as the keys and then takes part in interactions with an honest user to generate signatures on those messages cannot tell the order in which the messages were signed.

Definition 4 (Blindness w.r.t. malicious keys). *A blind scheme* BS *satisfies blindness w.r.t. malicious keys if for all* $\lambda \in \mathbb{N}$*, for all PPT adversaries* $\mathcal{A}$*, the advantage* $\mathsf{Adv}^{Blind}_{\mathsf{BS},\mathcal{A}}(\lambda)$ *defined as*

$$\mathsf{Adv}^{Blind}_{\mathsf{BS},\mathcal{A}}(\lambda) = \left|\Pr[\mathsf{Exp}^{Blind}_{\mathsf{BS},\mathcal{A}}(\lambda) = 1] - \frac{1}{2}\right|$$

is negligible (in λ*) where* $\mathsf{Exp}^{Blind}_{\mathsf{BS},\mathcal{A}}$ *is defined in Fig. 1.*

5 Blind Signature Constructions

Here we present our two constructions of blind signatures satisfying blindness in the malicious-key model.

5.1 Construction I

Here we present our first construction whose unforgeability is based on the BSOM assumption. The high-level idea is that when requesting a blind signature on the message $m \in \mathbb{Z}_p$, the user uses the Pedersen commitment scheme to commit to m as $\mathsf{Co} := G^m H^r$ and sends the commitment Co to the signer. Unlike many existing constructions, neither the user nor the signer in our construction are required to produce expensive zero-knowledge proofs to prove correctness of their computation. Note that since the Pedersen commitment is perfectly hiding, the commitment Co reveals no information about the committed message. We can think of such a commitment as the message M on which the oracle in the BSOM assumption is queried. Now the signer, playing the role of the oracle in the definition of the BSOM assumption, returns the tuple (A', B', C'). The user can check whether such a tuple corresponds to a valid pre-signature by first verifying that the last element (which is independent of the message) is constructed correctly. This is achieved by verifying that $e(C', \hat{Y}) = e(A', \hat{H})$. If such a check does not pass, the user returns $\perp$. Otherwise, since the user already knows the randomness r she used in constructing the commitment Co, she can now adapt the pre-signature (A', B') on the commitment Co to one on the message m by letting $B' := B'C'^{-r}$ and then randomizing the signature (A', B') into a new one (A, B) so that the two pairs are unlinkable. Similarly to e.g. [31,33], by assuming that the bilinear group generator $\mathcal{BG}$ is deterministic combined with the fact that the Pedersen commitment remains hiding even if the commitment key is generated maliciously, we achieve blindness w.r.t. malicious keys. The construction is detailed in Fig. 2.

```
$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, x, y \leftarrow \mathbb{Z}_p$
- $(H, \hat{H}, \hat{X}, \hat{Y}) := (G^h, \hat{G}^h, \hat{G}^x, \hat{G}^y)$
- $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}, \hat{X}, \hat{Y}), \mathsf{sk}_{\mathsf{BS}} := (h, x, y)$
- Return $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}})$

$\mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}} = (H, \hat{H}, \hat{X}, \hat{Y}), m)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
- Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{G}) \neq e(G, \hat{H})$
- $r \leftarrow \mathbb{Z}_p^\times;\ \mathsf{Co} := G^m H^r$
- Return $(\rho := \mathsf{Co}, \mathsf{st} := (m, r))$

$\mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}} = (h, x, y), \rho = \mathsf{Co})$
- $a' \leftarrow \mathbb{Z}_p^\times;\ A' := G^{a'};\ B' := (G^x \mathsf{Co})^{\frac{a'}{y}};\ C' := H^{\frac{a'}{y}}$
- Return $\beta := \big(A', B', C'\big)$

$\mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta = (A', B', C'), \mathsf{st} = (m, r))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}, \hat{X}, \hat{Y})$
- Return $\perp$ if $A' = 1_{\mathbb{G}}$ or $e(C', \hat{Y}) \neq e(A', \hat{H})$
- Set $B' := B'C'^{-r}$
- Return $\perp$ if $e(B', \hat{Y}) \neq e(A', \hat{X}\hat{G}^m)$
- $a \leftarrow \mathbb{Z}_p^\times;$ Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m, \sigma = (A, B))$
- If $A = 1_{\mathbb{G}}$ or $e(B, \hat{Y}) \neq e(A, \hat{X}\hat{G}^m)$ Then
    Return 0
- Else
    Return 1
```

Fig. 2. Our 1st blind signature construction

Note that the checks performed in the $\mathsf{Request}^0_{\mathsf{BS}}$ algorithm to verify well-formedness of the signer's verification key need only be performed once when requesting the first signature and not each time a signature is requested.

Theorem 3. *The construction is a secure blind signature scheme in the malicious-key model.*

Proof. We first show that the scheme is correct. We have that $\mathsf{Co} = G^m H^r$, $B' = (G^x \mathsf{Co})^{\frac{a'}{y}} = G^{\frac{a'x}{y}} \mathsf{Co}^{\frac{a'}{y}} = G^{\frac{a'x}{y}} (G^m H^r)^{\frac{a'}{y}}$ and $C' = H^{\frac{a'}{y}}$. We have that $B' = B'C'^{-r} = G^{\frac{a'x}{y}} (G^m H^r)^{\frac{a'}{y}} H^{\frac{-a'r}{y}} = G^{\frac{a'x}{y}} G^{\frac{ma'}{y}}$. Thus, (A', B') satisfy $e(B', \hat{Y}) = e(A', \hat{X}\hat{G}^m)$.

The following 2 lemmata complete the proof.

Lemma 1 (Unforgeability). *The construction is unforgeable if the BSOM assumption is intractable.*

Proof. Let $\mathcal{A}$ be an adversary against the unforgeability of the scheme. We show how to use $\mathcal{A}$ to construct an adversary $\mathcal{B}$ against the BSOM assumption. Adversary $\mathcal{B}$ gets the tuple $(\mathcal{P}, H, \hat{H}, \hat{X}, \hat{Y})$ from her game and she has access to the oracle $\mathcal{O}\mathrm{BSOM}_{H,\hat{H},\hat{X},\hat{Y}}(\cdot)$ which she can query polynomially many times. $\mathcal{B}$ starts $\mathcal{A}$ on $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}, \hat{X}, \hat{Y})$. When queried on Co_i, $\mathcal{B}$ forwards such query to her oracle and returns the answer to $\mathcal{A}$. Eventually, when $\mathcal{A}$ outputs her $k+1$ message-signatures tuples $\{(m_i, A_i, B_i)\}_{i=1}^{k+1}$, $\mathcal{B}$ returns that as the answer in her game. It is clear that $\mathcal{B}$ wins her game with the same advantage as that of $\mathcal{A}$ in her game. Thus, we have $\mathsf{Adv}^{\mathrm{Unforge}}_{\mathsf{BS},\mathcal{A}} = \mathsf{Adv}_{\mathrm{BSOM},\mathcal{B}}$.

Lemma 2. *The construction is perfectly blind in the malicious-key model.*

Proof. Since the Pedersen commitment is perfectly hiding, it is clear that Co sent by the user reveals no information about the committed message. Now the check we perform on the pre-signatures ensures that each pre-signature is valid on its respective commitment. If any of those pre-signatures is invalid, we return $(\bot, \bot)$. It is obvious in the latter case the adversary gains no information about the order in which the messages were signed. If the checks on the pre-signatures pass, it means the first pre-signature is a valid signature on the message m_b committed in Co_b whereas the second signature is valid on the message m_{1-b} committed in Co_{1-b}. From the adversary's point of view each signature could be on either message since the commitment could have been on either message. What remains now is to show that (A', B', C') are unlinkable to (A, B). By definition we have that $A'_0 \neq 1_{\mathbb{G}}$ and $A'_1 \neq 1_{\mathbb{G}}$. Now each final signature is computed by raising the corresponding pre-signature to a random exponent from $\mathbb{Z}_p^\times$. Thus, each final signature is uniformly distributed over the space of possible signatures and it follows that the final signature is independent of the pre-signature. □

5.2 Construction II

Here we present our second construction whose unforgeability is based on the BSOMI assumption. The high-level idea is similar to that of the first construction. When requesting a blind signature on the message $m \in \mathbb{Z}_p$, the user uses the Pedersen commitment scheme to commit to m as $\mathsf{Co} := G^m H^r$ and sends the commitment Co to the signer. Here we view the commitment as the message M on which the oracle in the BSOMI assumption is queried. Now the signer, playing the role of the oracle in the definition of the BSOMI assumption, returns the tuple (A', B', C'). The user can check whether such a tuple corresponds to a valid pre-signature by first verifying that the last element (which is independent of the message) is constructed correctly. This is achieved by verifying that $e(C', \hat{H}') = e(A', \hat{Y})$. If such a check does not pass, the user returns $\bot$. Otherwise, since the user already knows the randomness r she used in constructing the commitment Co, she can now adapt the pre-signature (A', B') on the commitment Co to one on the message m by letting $B' := B'C'^{-r}$ and then randomizing the signature (A', B') into a new one (A, B) so that the two pairs are unlinkable.

Again as in our first construction, by assuming that the bilinear group generator $\mathcal{BG}$ is deterministic combined with the fact that the Pedersen commitment remains hiding even if the commitment key is generated maliciously, we achieve blindness w.r.t. malicious keys. The construction is detailed in Fig. 3.

Note that the checks performed in the $\mathsf{Request}^0_{\mathsf{BS}}$ algorithm to verify well-formedness of the signer's verification key need only be performed once when requesting the first signature and not each time a signature is requested.

```
$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$; $h, x, y \leftarrow \mathbb{Z}_p$
- $(H, \hat{H}', \hat{X}, \hat{Y}) := (G^h, \hat{G}^{\frac{1}{h}}, \hat{G}^x, \hat{G}^y)$
- $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}', \hat{X}, \hat{Y}), \mathsf{sk}_{\mathsf{BS}} := (h, x, y)$
- Return $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}})$

$\mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}} = (H, \hat{H}', \hat{X}, \hat{Y}), m)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
- Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{H}') \neq e(G, \hat{G})$
- $r \leftarrow \mathbb{Z}_p^\times$; $\mathsf{Co} := G^m H^r$
- Return $(\rho := \mathsf{Co}, \mathsf{st} := (m, r))$

$\mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}} = (h, x, y), \rho = \mathsf{Co})$
- $a' \leftarrow \mathbb{Z}_p^\times$; $A' := G^{a'}$; $B' := A'^x \mathsf{Co}^{a' y}$; $C' := H^{a' y}$
- Return $\beta := \big(A', B', C'\big)$

$\mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta = (A', B', C'), \mathsf{st} = (m, r))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}', \hat{X}, \hat{Y})$
- Return $\perp$ if $A' = 1_{\mathbb{G}}$ or $e(C', \hat{H}') \neq e(A', \hat{Y})$
- Set $B' := B' C'^{-r}$
- Return $\perp$ if $e(B', \hat{G}) \neq e(A', \hat{X} Y^m)$
- $a \leftarrow \mathbb{Z}_p^\times$; Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, m, \sigma = (A, B))$
- If $A = 1_{\mathbb{G}}$ or $e(B, \hat{G}) \neq e(A, \hat{X} \hat{Y}^m)$ Then
    Return 0
- Else
    Return 1
```

Fig. 3. Our 2nd blind signature construction

The proof for the following theorem can be found in the full version [39].

Theorem 4. *The construction is a secure blind signature scheme in the malicious-key model in the standard model.*

Efficiency Comparison. We compare in Table 1 the efficiency of our blind signature constructions with the most efficient existing schemes offering the same security in the standard model [31,33]. As can be seen from the table, our schemes outperform existing schemes in every efficiency metric. At 80-bit security, the size of our signatures is 40 bytes, i.e. 67% shorter than those of [33]. Also, blindness in our schemes holds in the information-theoretic sense which is another advantage. The security of all schemes in the table including ours rely on interactive intractability assumptions. Note that the most efficient scheme based on non-interactive assumptions in the standard model [36] is much less efficient than the schemes in the table, e.g. the signature size in [36] is 183 group elements in symmetric bilinear groups. In the table, P stands for pairing, A for point addition, and MK Model for the malicious-key model.

Table 1. Efficiency comparison

Scheme	σ		vk		Communication				Verification	MK Model	Blindness
	$\mathbb{G}$	$\hat{\mathbb{G}}$	$\mathbb{G}$	$\hat{\mathbb{G}}$	User		Signer				
					$\mathbb{G}$	$\hat{\mathbb{G}}$	$\mathbb{G}$	$\hat{\mathbb{G}}$			
[33]	4	1	1	4	2	-	2	1	7P	Yes	Computational
[31]	7	3	-	4	4	-	2	1	15P	Yes	Computational
Ours I	2	-	1	3	1	-	3	-	2P + 1A	Yes	Perfect
Ours II	2	-	1	3	1	-	3	-	2P + 1A	Yes	Perfect

6 Blind Schemes for a Vector of Messages

In this section we give constructions of blind signatures for a vector of messages. These constructions are extensions of their single-message counterparts in which we replace the single-message Pedersen commitment scheme by its generalized variant which allows committing to a vector of messages at once, and make the necessary changes.

6.1 Construction I

We show in Fig. 4 that we can without affecting the signature size or the number of pairings involved in the verification extend our scheme from Sect. 5.1 to blindly sign a vector of messages. This variant is unforgeable under the same assumption as the single-message scheme.

```
$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda, n)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, x, y, z_1, \ldots, z_{n-1} \leftarrow \mathbb{Z}_p$
- $(H, \hat{H}, \hat{X}, \hat{Y}) := (G^h, \hat{G}^h, \hat{G}^x, \hat{G}^y)$
- $(Z_i, \hat{Z}_i) := (G^{z_i}, \hat{G}^{z_i})$ for $i = 1, \ldots, n-1$
- Set $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
- Set $\mathsf{sk}_{\mathsf{BS}} := (h, x, y, \{z_i\}_{i=1}^{n-1})$
- Return $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}})$

$\mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \boldsymbol{m} = (m_1, \ldots, m_n))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
- Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{G}) \neq e(G, \hat{H})$
- Return $\perp$ if $e(Z_i, \hat{G}) \neq e(G, \hat{Z}_i)$ for any $i \in [n-1]$.
- $r \leftarrow \mathbb{Z}_p^\times;\ \mathsf{Co} := G^{m_1} \prod_{i=2}^{n} Z_{i-1}^{m_i} H^r$
- Return $(\rho := \mathsf{Co}, \mathsf{st} := (\boldsymbol{m}, r))$

$\mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}} = (h, x, y, z_1, \ldots, z_{n-1}), \rho = \mathsf{Co})$
- $a' \leftarrow \mathbb{Z}_p^\times;\ A' := G^{a'};\ B' := (G^x \mathsf{Co})^{\frac{a'}{y}};\ C' := H^{\frac{a'}{y}}$
- Return $\beta := (A', B', C')$

$\mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta = (A', B', C'), \mathsf{st} = (\boldsymbol{m}, r))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
- Return $\perp$ if any of the following hold:
    $A' = 1_{\mathbb{G}}$
    $e(C', \hat{Y}) \neq e(A', \hat{H})$
- Set $B' := B' C'^{-r}$
- Return $\perp$ if $e(B', \hat{Y}) \neq e(A', \hat{X} \hat{G}^{m_1} \prod_{i=2}^{n} \hat{Z}_{i-1}^{m_i})$
- $a \leftarrow \mathbb{Z}_p^\times$; Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \boldsymbol{m}, \sigma = (A, B))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
- Return 1 if all the following hold:
    $A \neq 1_{\mathbb{G}}$
    $e(B, \hat{Y}) = e(A, \hat{X} \hat{G}^{m_1} \prod_{i=2}^{n} \hat{Z}_{i-1}^{m_i})$
```

Fig. 4. A blind signature scheme I for a vector of messages $\in \mathbb{Z}_p^n$

All the checks performed in the $\mathsf{Request}^0_{\mathsf{BS}}$ algorithm to verify well-formedness of the signer's verification key need only be performed once when requesting the first signature and not each time a signature is requested.

Theorem 5. *The scheme in Fig. 4 is a secure blind signature.*

Proof. Correctness is straightforward to verify. Perfect blindness in the malicious-key model holds similarly to the perfect blindness of the single-message scheme. The following lemma proves unforgeability of the scheme.

Lemma 3 (Unforgeability). *The scheme is unforgeable if the BSOM assumption is intractable.*

Proof. Let $\mathcal{A}$ be an adversary against the unforgeability of the scheme. We show how to use $\mathcal{A}$ to construct an adversary $\mathcal{B}$ against the BSOM assumption. Adversary $\mathcal{B}$ gets the tuple $(\mathcal{P}, H, \hat{H}, \hat{X}, \hat{Y})$ from her game and she has access to the oracle $\mathcal{O}\mathrm{BSOM}_{H,\hat{H},\hat{X},\hat{Y}}(\cdot)$ which she can query polynomially many times. $\mathcal{B}$ chooses $z_1, \ldots, z_{n-1} \leftarrow \mathbb{Z}_p^\times$ and computes $(Z_i, \hat{Z}_i) := (G^{z_i}, \hat{G}^{z_i})$ for all $i \in [n-1]$. She then starts $\mathcal{A}$ on $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$. When queried on Co_i, $\mathcal{B}$ forwards such query to her oracle and returns the answer to $\mathcal{A}$. Eventually, when $\mathcal{A}$ outputs her $k+1$ message-signature tuples $\{(\boldsymbol{m}_i = (m_{i,1}, \ldots, m_{i,n}), A_i, B_i)\}_{i=1}^{k+1}$ where the vectors $\boldsymbol{m}_i$ are distinct, $\mathcal{B}$ computes $m'_i = m_{i,1} + \sum_{j=2}^{n} z_{j-1} m_{i,j}$ for all $i \in [k+1]$ and returns the $k+1$ tuples $\{(m'_i, A_i, B_i)\}_{i=1}^{k+1}$ as the answer in her game. It is clear that $\mathcal{B}$ wins her game with the same advantage as that of $\mathcal{A}$ in her game. Thus, we have $\mathsf{Adv}^{\mathrm{Unforge}}_{\mathsf{BS},\mathcal{A}} = \mathsf{Adv}_{\mathrm{BSOM},\mathcal{B}}$. □

6.2 Construction II

We extend our scheme from Sect. 5.2 to blindly sign a vector of messages as shown in Fig. 5. This scheme is unforgeable under the same assumption as the single-message scheme.

All the checks performed in the $\mathsf{Request}^0_{\mathsf{BS}}$ algorithm to verify well-formedness of the signer's verification key need only be performed once when requesting the first signature and not each time a signature is requested.

The proof for the following theorem can be found in the full version [39].

Theorem 6. *The scheme in Fig. 5 is a secure blind signature.*

```
$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda, n)$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$;  $h, x, y, z_1, \ldots, z_{n-1} \leftarrow \mathbb{Z}_p$
- $(H, \hat{H}', \hat{X}, \hat{Y}) := (G^h, \hat{G}^{\frac{1}{h}}, \hat{G}^x, \hat{G}^y)$
- $(Z_i, \hat{Z}'_i) := (G^{z_i}, \hat{Y}^{z_i})$ for $i = 1, \ldots, n-1$
- Set $\mathsf{vk}_{\mathsf{BS}} := (H, \hat{H}', \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
- Set $\mathsf{sk}_{\mathsf{BS}} := (h, x, y, \{z_i\}_{i=1}^{n-1})$
- Return $(\mathsf{vk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}})$

$\mathsf{Request}^0_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \boldsymbol{m} = (m_1, \ldots, m_n))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}', \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
- $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
- Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{H}') \neq e(G, \hat{G})$
- Return $\perp$ if $e(Z_i, \hat{Y}) \neq e(G, \hat{Z}'_i)$ for any $i \in [n-1]$
- $r \leftarrow \mathbb{Z}_p^\times$;  $\mathsf{Co} := G^{m_1} \prod_{i=2}^{n} Z_{i-1}^{m_i} H^r$
- Return $(\rho := \mathsf{Co}, \mathsf{st} := (\boldsymbol{m}, r))$

$\mathsf{Issue}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}} = (h, x, y, z_1, \ldots, z_{n-1}), \rho = \mathsf{Co})$
- $a' \leftarrow \mathbb{Z}_p^\times$;  $A' := G^{a'}$;  $B' := A'^x \mathsf{Co}^{a'y}$;  $C' := H^{a'y}$
- Return $\beta := (A', B', C')$
```

```
$\mathsf{Request}^1_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \beta = (A', B', C'), \mathsf{st} = (\boldsymbol{m}, r))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}', \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
- Return $\perp$ if any of the following hold:
    $A' = 1_{\mathbb{G}}$
    $e(C', \hat{H}') \neq e(A', \hat{Y})$
- Set $B' := B' C'^{-r}$
- Return $\perp$ if $e(B', \hat{G}) \neq e(A', \hat{X}\hat{Y}^{m_1} \prod_{i=2}^{n} \hat{Z}'^{m_i}_{i-1})$
- $a \leftarrow \mathbb{Z}_p^\times$;  Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{BS}}(\mathsf{vk}_{\mathsf{BS}}, \boldsymbol{m}, \sigma = (A, B))$
- Parse $\mathsf{vk}_{\mathsf{BS}}$ as $(H, \hat{H}', \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
- Return 1 if all the following hold:
    $A \neq 1_{\mathbb{G}}$
    $e(B, \hat{G}) = e(A, \hat{X}\hat{Y}^{m_1} \prod_{i=2}^{n} \hat{Z}'^{m_i}_{i-1})$
- Else Return 0
```

Fig. 5. A blind signature scheme II for a vector of messages $\in \mathbb{Z}_p^n$

7 Partially Blind Signature Schemes

Here we show how to modify our schemes in Sects. 6.1 and 6.2 to obtain partially blind signature schemes. For more generality, we give schemes where the public information is also a vector $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_{n'}) \in \mathbb{Z}_p^{n'}$. This allows to attach multiple attributes to the signature.

7.1 Construction I

To realize our first construction, we modify the blind scheme on vector messages from Sect. 6.1 to attach a vector $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_{n'}) \in \mathbb{Z}_p^{n'}$ of public information to the signature. To do so, we add to the public key of the scheme in Fig. 4 the elements $\hat{W}_i := \hat{G}^{w_i}$ for some randomly chosen elements $w_i \leftarrow \mathbb{Z}_p$ for $i = 1, \ldots, n'$. When asked to sign a commitment Co along with the public information $\boldsymbol{\tau}$, the signer signs the modified commitment $\mathsf{Co}' := \mathsf{Co} G^{\sum_{i=1}^{n'} \tau_i w_i}$. Upon receiving the pre-signature, the user checks that it is valid on the tuple $(\boldsymbol{m}, \boldsymbol{\tau})$. The details of the construction are in Fig. 6. The unforgeability of the scheme relies on a slight extension of the BSOM assumption which we refer to as the E-BSOM assumption. See full version [39] for details.

All the checks performed in the $\mathsf{Request}^0_{\mathsf{BS}}$ algorithm to verify well-formedness of the signer's verification key need only be performed once when requesting the first signature and not each time a signature is requested.

The proof for the following theorem can be found in the full version [39].

Theorem 7. *The scheme in Fig. 6 is a secure partially blind signature.*

```
$\mathsf{KeyGen}_{\mathsf{PBS}}(1^\lambda, n, n')$
    - $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, x, y, z_1, \ldots, z_{n-1}, w_1, \ldots, w_{n'} \leftarrow \mathbb{Z}_p$
    - $(H, \hat{H}, \hat{X}, \hat{Y}) := (G^h, \hat{G}^h, \hat{G}^x, \hat{G}^y)$
    - $(Z_i, \hat{Z}_i) := (G^{z_i}, \hat{G}^{z_i})$ for all $i \in [n-1]$
    - $\hat{W}_i := \hat{G}^{w_i}$ for all $i \in [n']$
    - $\mathsf{vk}_{\mathsf{PBS}} := (H, \hat{H}, \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
    - $\mathsf{sk}_{\mathsf{PBS}} := (h, \{w_i\}_{i=1}^{n'}, x, y, \{z_i\}_{i=1}^{n-1})$
    - Return $(\mathsf{vk}_{\mathsf{PBS}}, \mathsf{sk}_{\mathsf{PBS}})$

$\mathsf{Request}^0_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \boldsymbol{m} = (m_1, \ldots, m_n), \boldsymbol{\tau} = (\tau_1, \ldots, \tau_{n'}))$
    - Parse $\mathsf{vk}_{\mathsf{PBS}}$ as $(H, \hat{H}, \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
    - $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
    - Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{G}) \neq e(G, \hat{H})$
    - Return $\perp$ if $e(Z_i, \hat{G}) \neq e(G, \hat{Z}_i)$ for any $i \in [n-1]$
    - $r \leftarrow \mathbb{Z}_p^\times;\ \mathsf{Co} := G^{m_1} \prod_{i=2}^{n} Z_{i-1}^{m_i} H^r$
    - Return $(\rho := \mathsf{Co}, \mathsf{st} := (\boldsymbol{m}, r))$

$\mathsf{Issue}_{\mathsf{PBS}}(\mathsf{sk}_{\mathsf{PBS}} = (h, \{w_i\}_{i=1}^{n'}, x, y, \{z_i\}_{i=1}^{n-1}), \rho = \mathsf{Co}, \boldsymbol{\tau})$
    - $a' \leftarrow \mathbb{Z}_p^\times;\ A' := G^{a'};\ B' := \left(\mathsf{Co}G^{x + \sum_{i=1}^{n'} \tau_i w_i}\right)^{\frac{a'}{y}};\ C' := H^{\frac{a'}{y}}$
    - Return $\beta := (A', B', C')$

$\mathsf{Request}^1_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \beta = (A', B', C'), \mathsf{st} = (\boldsymbol{m}, r), \boldsymbol{\tau})$
    - Parse $\mathsf{vk}_{\mathsf{PBS}}$ as $(H, \hat{H}, \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}_i\}_{i=1}^{n-1})$
    - Return $\perp$ if $A' = 1_{\mathbb{G}}$ or $e(C', \hat{Y}) \neq e(A', \hat{H})$
    - Set $B' := B'C'^{-r}$
    - Return $\perp$ if $e(B', \hat{Y}) \neq e(A', \hat{X}\hat{G}^{m_1} \prod_{i=2}^{n} \hat{Z}_{i-1}^{m_i} \prod_{i=1}^{n'} \hat{W}_i^{\tau_i})$
    - $a \leftarrow \mathbb{Z}_p^\times;$ Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \boldsymbol{m}, \boldsymbol{\tau}, \sigma = (A, B))$
    - Return 1 if the following holds and 0 otherwise:
        $A \neq 1_{\mathbb{G}}$ and $e(B, \hat{Y}) = e(A, \hat{X}\hat{G}^{m_1} \prod_{i=2}^{n} \hat{Z}_{i-1}^{m_i} \prod_{i=1}^{n'} \hat{W}_i^{\tau_i})$
```

Fig. 6. A partially blind signature scheme I for a vector of messages $\in \mathbb{Z}_p^n$

7.2 Construction II

Our second partially blind signature construction shown in Fig. 7 is an extension of our blind construction from Fig. 5 in a similar manner to the first construction. The unforgeability of the scheme relies on a slight extension of the BSOMI assumption which we refer to as the E-BSOMI assumption. See full version [39] for details.

The proof for the following theorem can be found in the full version [39].

Theorem 8. *The scheme in Fig. 7 is a secure partially blind signature.*

```
$\mathsf{KeyGen}_{\mathsf{PBS}}(1^\lambda, n, n')$
    - $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda);\ h, w_1, \ldots, w_{n'}, x, y, z_1, \ldots, z_{n-1} \leftarrow \mathbb{Z}_p$
    - $(H, \hat{H}, \hat{X}, \hat{Y}) := (G^h, \hat{G}^{\frac{1}{h}}, \hat{G}^x, \hat{G}^y)$
    - $(Z_i, \hat{Z}'_i) := (G^{z_i}, \hat{Y}^{z_i})$ for all $i \in [n-1]$
    - $\hat{W}_i := \hat{G}^{w_i}$ for all $i \in [n']$
    - $\mathsf{vk}_{\mathsf{PBS}} := (H, \hat{H}', \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
    - $\mathsf{sk}_{\mathsf{PBS}} := (h, \{w_i\}_{i=1}^{n'}, x, y, \{z_i\}_{i=1}^{n-1})$
    - Return $(\mathsf{vk}_{\mathsf{PBS}}, \mathsf{sk}_{\mathsf{PBS}})$

$\mathsf{Request}^0_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \boldsymbol{m} = (m_1, \ldots, m_n), \boldsymbol{\tau} = (\tau_1, \ldots, \tau_{n'}))$
    - Parse $\mathsf{vk}_{\mathsf{PBS}}$ as $(H, \hat{H}', \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
    - $\mathcal{P} \leftarrow \mathcal{BG}(1^\lambda)$
    - Return $\perp$ if $H = 1_{\mathbb{G}}$ or $e(H, \hat{H}') \neq e(G, \hat{G})$
    - Return $\perp$ if $e(Z_i, \hat{Y}) \neq e(G, \hat{Z}'_i)$ for any $i \in [n-1]$
    - $r \leftarrow \mathbb{Z}_p^\times;\ \mathsf{Co} := G^{m_1} \prod_{i=2}^{n} Z_{i-1}^{m_i} H^r$
    - Return $(\rho := \mathsf{Co}, \mathsf{st} := (\boldsymbol{m}, r))$

$\mathsf{Issue}_{\mathsf{PBS}}(\mathsf{sk}_{\mathsf{PBS}} = (h, \{w_i\}_{i=1}^{n'}, x, y, \{z_i\}_{i=1}^{n-1}), \rho = \mathsf{Co}, \boldsymbol{\tau})$
    - $a' \leftarrow \mathbb{Z}_p^\times;\ A' := G^{a'};\ B' := A'^x \mathsf{Co}^{a'y} G^{a' \sum_{i=1}^{n'} \tau_i w_i};\ C' := H^{a'y}$
    - Return $\beta := (A', B', C')$

$\mathsf{Request}^1_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \beta = (A', B', C'), \mathsf{st} = (\boldsymbol{m}, r), \boldsymbol{\tau})$
    - Parse $\mathsf{vk}_{\mathsf{PBS}}$ as $(H, \hat{H}', \{\hat{W}_i\}_{i=1}^{n'}, \hat{X}, \hat{Y}, \{Z_i, \hat{Z}'_i\}_{i=1}^{n-1})$
    - Return $\perp$ if $A' = 1_{\mathbb{G}}$ or $e(C', \hat{H}') \neq e(A', \hat{Y})$
    - Set $B' := B'C'^{-r}$
    - Return $\perp$ if $e(B', \hat{G}) \neq e(A', \hat{X}\hat{Y}^{m_1} \prod_{i=2}^{n} \hat{Z}'^{m_i}_{i-1} \prod_{i=1}^{n'} \hat{W}_i^{\tau_i})$
    - $a \leftarrow \mathbb{Z}_p^\times;$ Return $\sigma = (A, B) := (A'^a, B'^a)$

$\mathsf{Verify}_{\mathsf{PBS}}(\mathsf{vk}_{\mathsf{PBS}}, \boldsymbol{m}, \boldsymbol{\tau}, \sigma = (A, B))$
    - Return 1 if the following holds and 0 otherwise:
        $A \neq 1_{\mathbb{G}}$ and $e(B, \hat{G}) = e(A, \hat{X}\hat{Y}^{m_1} \prod_{i=2}^{n} \hat{Z}'^{m_i}_{i-1} \prod_{i=1}^{n'} \hat{W}_i^{\tau_i})$
```

Fig. 7. A partially blind signature scheme II for a vector of messages $\in \mathbb{Z}_p^n$

Acknowledgments. We thank Ian Goldberg for pointing out an issue in the description of the partially blind scheme in an earlier version.

References

1. Abdalla, M., Namprempre, C., Neven, G.: On the (im)possibility of blind message authentication codes. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 262–279. Springer, Heidelberg (2006). https://doi.org/10.1007/11605805_17
2. Abe, M.: A secure three-move blind signature scheme for polynomially many signatures. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 136–151. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_9
3. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_12
4. Abe, M., Fujisaki, E.: How to date blind signatures. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 244–251. Springer, Heidelberg (1996). https://doi.org/10.1007/BFb0034851
5. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133. http://eprint.iacr.org/2010/133.pdf
6. Abe, M., Ohkubo, M.: A framework for universally composable non-committing blind signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 435–450. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_26
7. Baldimtsi, F., Lysyanskaya, A.: On the security of one-witness blind signature schemes. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8270, pp. 82–99. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42045-0_5
8. Baldimtsi, F., Lysyanskaya, A.: Anonymous credentials light. In: ACM-CCS 2013, pp. 1087–1098. ACM (2013)
9. Barbosa, M., Farshim, P.: Strong knowledge extractors for public-key encryption schemes. In: Steinfeld, R., Hawkes, P. (eds.) ACISP 2010. LNCS, vol. 6168, pp. 164–181. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14081-5_11
10. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006). https://doi.org/10.1007/11693383_22
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. Cryptol. **16**(3), 185–215 (2003)
12. Bernhard, D., Fuchsbauer, G., Ghadafi, E., Smart, N.P., Warinschi, B.: Anonymous attestation with user-controlled linkability. Int. J. Inf. Secur. **12**(3), 219–249 (2013)
13. Blazy, O., Fuchsbauer, G., Pointcheval, D., Vergnaud, D.: Signatures on randomizable ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 403–422. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_25
14. Blazy, O., Pointcheval, D., Vergnaud, D.: Compact round-optimal partially-blind signatures. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 95–112. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_6
15. Boldyreva, A.: Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-Group signature scheme. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 31–46. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36288-6_3
16. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol. **21**(2), 149–177 (2008)

17. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004)
18. Brands, S.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge (2000)
19. Brands, S., Paquin, C.: U-Prove Cryptographic Specification v1 (2010)
20. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: CCS 2004, pp. 132–145. ACM (2004)
21. Camenisch, J., Koprowski, M., Warinschi, B.: Efficient blind signatures without random oracles. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 134–148. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30598-9_10
22. Canard, S., Devigne, J., Sanders, O.: Delegating a pairing can be both secure and efficient. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 549–565. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07536-5_32
23. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) CRYPTO 1982, pp. 199–203. Springer, Cham (1983). https://doi.org/10.1007/978-1-4757-0602-4_18
24. Döttling, N., Fleischhacker, N., Krupp, J., Schröder, D.: Two-message, oblivious evaluation of cryptographic functionalities. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9816, pp. 619–648. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_22
25. Dwork, C., Naor, M.: Zaps and their applications. In: FOCS 2000, pp. 283–293. IEEE (2000)
26. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
27. Fischlin, M.: Round-optimal composable blind signatures in the common reference string model. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 60–77. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_4
28. Fischlin, M., Schröder, D.: Security of blind signatures under aborts. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 297–316. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_17
29. Fischlin, M., Schröder, D.: On the impossibility of three-move blind signature schemes. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 197–215. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_10
30. Fuchsbauer, G.: Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320. http://eprint.iacr.org/2009/320.pdf
31. Fuchsbauer, G., Hanser, C., Kamath, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model from weaker assumptions. In: Zikas, V., De Prisco, R. (eds.) SCN 2016. LNCS, vol. 9841, pp. 391–408. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44618-9_21
32. Fuchsbauer, G., Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. Cryptology ePrint Archive, Report 2014/944. http://eprint.iacr.org/2014/944.pdf
33. Fuchsbauer, G., Hanser, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 233–253. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_12

34. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 244–251. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-57220-1_66
35. Galbraith, S., Paterson, K., Smart, N.P.: Pairings for cryptographers. Discrete Appl. Math. **156**, 3113–3121 (2008)
36. Garg, S., Gupta, D.: Efficient round optimal blind signatures. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 477–495. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_27
37. Garg, S., Rao, V., Sahai, A., Schröder, D., Unruh, D.: Round optimal blind signatures. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 630–648. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_36
38. Ghadafi, E.: More efficient structure-preserving signatures - or: bypassing the type-III lower bounds. Cryptology ePrint Archive, Report 2016/255. http://eprint.iacr.org/2016/255.pdf
39. Ghadafi, E.: Efficient round-optimal blind signatures in the standard model. Cryptology ePrint Archive, Report 2017/045. http://eprint.iacr.org/2017/045.pdf
40. Ghadafi, E., Smart, N.P.: Efficient two-move blind signatures in the common reference string model. In: Gollmann, D., Freiling, F.C. (eds.) ISC 2012. LNCS, vol. 7483, pp. 274–289. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33383-5_17
41. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. SIAM J. Comput. **41**(5), 1193–1232 (2012)
42. Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 491–511. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_26
43. Hanzlik, L., Kluczniak, K.: A short paper on blind signatures from knowledge assumptions. In: Grossklags, J., Preneel, B. (eds.) FC 2016. LNCS, vol. 9603, pp. 535–543. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54970-4_31
44. Hazay, C., Katz, J., Koo, C.-Y., Lindell, Y.: Concurrently-secure blind signatures without random oracles or setup assumptions. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 323–341. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_18
45. Juels, A., Luby, M., Ostrovsky, R.: Security of blind digital signatures. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 150–164. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052233
46. Kiayias, A., Zhou, H.-S.: Concurrent blind signatures without random oracles. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 49–62. Springer, Heidelberg (2006). https://doi.org/10.1007/11832072_4
47. Lindell, Y.: Bounded-concurrent secure two-party computation without setup assumptions. In: STOC 2003, pp. 683–692. ACM (2003)
48. 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: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 519–538. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_30
49. Okamoto, T.: Efficient blind and partially blind signatures without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 80–99. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_5

50. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_9
51. Pointcheval, D., Sanders, O.: Short randomizable signatures. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 111–126. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29485-8_7
52. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. **13**(3), 361–396 (2000)
53. Rückert, M.: Lattice-based blind signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 413–430. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_24
54. Schnorr, C.P.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_22
55. Schröder, D., Unruh, D.: Security of blind signatures revisited. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 662–679. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_39
56. Seo, J.H., Cheon, J.H.: Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 133–150. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28914-9_8
57. Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_18