

Concurrently secure variants of blind (Okamoto-)Schnorr signatures

Georg Fuchsbauer, Fabian Regen, and Levente Sulyok

TU Wien, Austria

Abstract. We present variants of blind Schnorr and blind Okamoto-Schnorr signatures that are not susceptible to ROS-style attacks. We prove the schemes unforgeable in the algebraic group model and the random oracle model: the Okamoto-Schnorr variant under the discrete-logarithm assumption; the Schnorr variant under the algebraic one-more discrete-logarithm assumption. Our Schnorr variant improves on the communication complexity of Snowblind (CRYPTO 2023), the state-of-the-art “pairing-free” blind signature scheme, while matching its signature size. Moreover, we show that this communication complexity is optimal: any blind “Schnorr-like” scheme whose first message is a single group element is susceptible to a variant of the ROS attack by Benhamouda et al. (EUROCRYPT 2021).

1 Introduction

Blind signatures [Cha82] allow a user to obtain a signature on a message from a signer so that the signer does not learn any information about the message and the signature. They are applied in various settings such as e-cash [Cha82, CFN90, OO92, Bra94, BCKL09, BFQ21], e-voting [Cha88, FOO93, Oka98, BFP⁺01, KRS10], anonymous credentials [Bra94, CL01, CL04, CG08, BL13, FHS15], and privacy-preserving applications [VR15, HBG16, GCGF16, SLY⁺22]. They are also used in several recent industry applications, such as privacy-preserving ad-click measurement [PCM21], Apple’s iCloud Private Relay [App], Google One’s VPN Service [Goo], and various forms of anonymous tokens [Int, PST].

Blind signatures must satisfy two properties: *(one-more) unforgeability*, meaning a malicious user, who might open multiple concurrent signing sessions, is unable to produce more valid signatures than completed signing sessions; and *blindness*, meaning a malicious signer is unable to link a valid message-signature pair to the session that produced the signature.

There exist constructions based on RSA groups [BNPS03, Lys23] and pairing-friendly elliptic curves [Bol03, KRS23]. However, at the same security level the former lead to much larger signatures than elliptic-curve-based schemes; on the other hand, there are currently no standards for pairing-friendly curves. This makes efficient “pairing-free” schemes defined over discrete-log-hard groups, for which there are standards [LHT16, CMR⁺23], most desirable.

Another criterion is the round complexity of the signature issuing protocol, with two-move schemes being optimal. Unfortunately, Fischlin and Schröder

[FS10] showed that even a broad class of three-move schemes are impossible to prove secure via a reduction to non-interactive assumptions in the standard model. More recently, Dietz, Kastner and Tessaro [DKT26] showed that (under certain conditions on the message length and the number of random oracle queries) there exist no pairing-free and round-optimal constructions in (Maurer’s) generic group model (GGM) [Mau05] and the random oracle model (ROM) [BR93].

In pairing-free groups this leaves round-optimal constructions based on Fischlin’s paradigm [Fis06], that rely on non-black-box use of the group [KNR24, KTZ26], which have larger signatures due to their reliance on non-interactive zero-knowledge proofs, or (efficient) three-move constructions [Abe01, Sch90, Oka93, FPS20, KLX22, CKM⁺23] in the Algebraic Group Model (AGM) [FKL18] and the ROM. Furthermore there exist three-move constructions [CART26, Che26] that do not rely on the AGM, but only the ROM, that incur a much larger signature size. In particular, the more efficient scheme has signatures that comprise 15 group elements and 22 scalars, while communication comprises 17 group elements and 14 scalars. There also exist constructions that only rely on the ROM by requiring at least four moves [FW24, CATZ24, KRW24, KR25, BHKR25, KLR26, DMV26].

Schnorr signatures [Sch90] admit a simple three-move blind signing protocol [CP93]. Their concurrent security was analyzed [FPS20] in the AGM and the ROM, assuming that the one-more discrete-logarithm problem [BNPS03, BFP21], as well as ROS, a problem introduced by Schnorr, are hard. Schnorr [Sch01] had also showed that solving ROS allows an attacker to forge signatures if multiple signing sessions can be opened concurrently. Later, Wagner [Wag02] described a sub-exponential-time attack on ROS, and more recently Benhamouda et al. [BLL⁺21] gave a polynomial-time attack, which translates to attacks on many schemes, such as blind Okamoto-Schnorr signatures [Oka93], when the adversary opens a polynomial number of concurrent signing sessions.

This leaves the following efficient pairing-free blind signature schemes: Abe’s scheme [Abe01] is computationally blind and proven unforgeable under the discrete-logarithm assumption in the AGM+ROM [KLX22]; Clause Blind Schnorr [FPS20] is a variant of Schnorr relying on the “modified ROS” assumption, a strengthening of the ROS problem, against which there are sub-exponential-time attacks [TZ22]. Snowblind [CKM⁺23] improves upon the scheme by Tessaro and Zhu [TZ22], yielding smaller signatures and simplifying the proof.

The aim of this work is to find more efficient (pairing-free) blind signature schemes that are not susceptible to ROS-style attacks. In particular, we pose the following question:

Can we construct more efficient pairing-free three-move blind signature schemes that are concurrently secure?

Our schemes. Consider the (insecure) blind Schnorr issuance, where the signer first sends one group element called the “commitment”, the user responds with a field element called the “challenge”, and the “response” of the signer is another

Table 1. Short three-move blind signatures in pairing-free groups. The column Comm. refers to the communication size of the signing protocol. All schemes are proved one-more unforgeable in the AGM+ROM, all but Abe’s scheme are perfectly blind and have one group element as the public key. There exists a polynomial-time attack for ROS, and (slightly) sub-exponential attacks for the modified ROS (mROS) problem.

Blind signature	Sig. size	Comm.	Assumptions
Abe [Abe01, KLX22]	$2\mathbb{G} + 6\mathbb{Z}_p$	$3\mathbb{G} + 6\mathbb{Z}_p + \log p$	DL
Blind Schnorr [Sch90, FPS20]	$1\mathbb{G} + 1\mathbb{Z}_p$	$1\mathbb{G} + 2\mathbb{Z}_p$	OMDL+ROS
Clause Blind Schnorr [FPS20]	$1\mathbb{G} + 1\mathbb{Z}_p$	$2\mathbb{G} + 3\mathbb{Z}_p + 1\text{bit}$	OMDL+mROS
Snowblind [CKM ⁺ 23]	$1\mathbb{G} + 2\mathbb{Z}_p$	$2\mathbb{G} + 4\mathbb{Z}_p$	DL
This work: Schnorr²	$1\mathbb{G} + 2\mathbb{Z}_p$	$2\mathbb{G} + 2\mathbb{Z}_p$	AOMDL
This work: Okamoto-Schnorr²	$1\mathbb{G} + 3\mathbb{Z}_p$	$2\mathbb{G} + 3\mathbb{Z}_p$	DL

field element computed by a linear function in the challenge and secret key. The signature then comprises of one group and one field element. Based on this, Barreto and Zanon [BZ23] altered the construction such that the signer first sends two commitments, and the user answers with two challenges output by a hash function. The last message then combines both challenges and commitments into a single response, essentially yielding two applications of Schnorr. Their blind signature scheme was later shown to be insecure [RCK⁺25].

In our variant (defined in Fig. 12) the signer sends two commitments but the user responds with only one challenge. Where before the response was computed using a linear function in the challenge, here the response is computed using a non-linear function. A signature then consists of one group element and two scalars. This matches state-of-the-art pairing-free blind signatures, while improving on communication cost (see Table 1).

We prove our scheme concurrently secure in the AGM and ROM assuming the hardness of the Algebraic One-More Discrete-Logarithm (AOMDL) problem. Our proof follows the blueprint of earlier proofs, like the one for blind Schnorr [FPS20], which gives a reduction to OMDL that fails exactly when the adversary can be used to solve the ROS problem. At its core, the proof uses the algebraic representations of the forgeries returned by an adversary to compute the (one-more) discrete logarithm of the public key. For our blind signature scheme, this leads to a variant of the ROS problem with an exponential number of equations, which we show is unconditionally hard.

Analogously, we obtain a variant of the Okamoto-Schnorr scheme (defined in Fig. 13). Its signatures consist of 1 group element and 3 scalars, and it also improves on the communication cost of previous works. We show our scheme concurrently secure in the AGM and ROM assuming the hardness of the Discrete-Logarithm (DL) problem. For a detailed comparison of pairing-free blind signature schemes we refer to Table 1.

Lower bound. We show that our constructions are in some sense optimal. To do so, we adapt the framework by Hauck, Kiltz and Loss [HKL19] for constructing blind signatures from linear function families. Our extension allows for arbitrary homomorphic *evaluation functions*, which defines how the (scalar) secret key relates to the (vector) public key and is used to verify the response, and allows for arbitrary *coefficient functions*, that compute the signer’s response given the challenge. We then show that unforgeability of such schemes relates to the *Constrained Coset ROS* (CCROS) problem, and that the polynomial-time ROS attack [BLL⁺21] can be adapted to CCROS. This implies that three-move blind signature schemes within the extended HKL framework are insecure if their first signer message (“commitment”) consists of a single group element.

2 Preliminaries

The value $\lambda \in \mathbb{N}$ denotes the security parameter, $x \leftarrow X$ denotes sampling uniformly at random from a set X , $y := x$ denotes deterministic assignment of x to y , $y \leftarrow \mathcal{A}(x)$ denotes running the algorithm $\mathcal{A}$ on input x that outputs y . Vectors are denoted by boldface letters $\mathbf{v}$, and their i -th element by v_i . The standard basis vectors are denoted by $\mathbf{e}_i$, where all elements of $\mathbf{e}_i$ are 0 except the i -th which is $e_{i,i} = 1$. Functions are applied component-wise to a vector of elements of the function’s domain. The inner product between vectors $\mathbf{v}, \mathbf{u}$ is denoted by $\mathbf{v} \cdot \mathbf{u}$, and the product with a scalar s by $s \cdot \mathbf{v}$ or by the shorthand $s\mathbf{v}$. Element-wise vector multiplication is denoted by $\mathbf{v} \odot \mathbf{u}$. Exponentiation of a vector $\mathbf{v}^k$ is defined as k -times application of element-wise multiplication $\mathbf{v} \odot \dots \odot \mathbf{v}$. The set $\{1, \dots, \ell\}$ is denoted by $[\ell]$, and $[\ell] \cup \{0\}$ is denoted by $[\ell]_0$. It is assumed that there is an algorithm GrGen that on input the security parameter λ in unary returns a cyclic group $\mathbb{G}$ of prime order p of bit-length λ with generator G , where the discrete-logarithm problem is hard. Group operation is denoted additively by $+$. Schemes and their algorithms are denoted by sans-serif letters, and their individual algorithms by dot notation, e.g., Scheme.Alg(x). Oracle access to $\mathcal{O}$ given to an adversary $\mathcal{A}$ is denoted by $\mathcal{A}^{\mathcal{O}}$. The classes of negligible and polynomial functions are denoted by $\text{negl}(\lambda)$ and $\text{poly}(\lambda)$, respectively.

2.1 Algebraic Group Model (AGM)

The AGM is an idealized model where the adversary is required to supply a representation $z_i \in \mathbb{Z}_p$, for $i \in [t]$, for any group element $Z \in \mathbb{G}$ it outputs such that $Z = \sum_{i=1}^t z_i A_i$, where $A_i \in \mathbb{G}$ are the group elements the adversary has been input so far.

The AGM can be naturally extended to vector spaces. Let V be an n -dimensional vector space over a field K , e.g., $\mathbb{G}$ is a vector space over $\mathbb{Z}_p$. Then, the adversary is required to supply a representation $k_i \in K$, for $i \in [t]$, for the vector $\mathbf{v} \in V$ such that $\mathbf{v} = \sum_{i=1}^t k_i \mathbf{b}_i$, where $\mathbf{b}_i \in V$ are the vectors the adversary has been input so far. Furthermore, if the adversary is given a vector space homomorphism $f : U \rightarrow V$, where U is an m -dimensional vector space

over K with basis $\mathbf{u}_i$ for $i \in [m]$, then each vector $\mathbf{u} = a_1\mathbf{u}_1 + \dots + a_m\mathbf{u}_m \in U$ for $a_i \in K$ satisfies $f(\mathbf{u}) = a_1f(\mathbf{u}_1) + \dots + a_mf(\mathbf{u}_m)$. Thus, the adversary is additionally required to supply the representations $a_i \in K$ for $i \in [m]$ such that $\mathbf{v} = \sum_{i=1}^m a_i f(\mathbf{u}_i) + \sum_{i=1}^t k_i \mathbf{b}_i$. In other words, giving the adversary access to f is equivalent to giving it the vectors $f(\mathbf{u}_i)$. In the following, the adversary only supplies vectors $\mathbf{u} \in U$ as its representation w.r.t. f , which implicitly defines the representations $(a_i)_{i \in [m]}$.

A vector $\mathbf{v}$ with representation $k_1, \dots, k_t$ may be denoted as $\mathbf{v}_{[k_1, \dots, k_t]}$.

2.2 Blind Signatures

A three-move blind signature BS consists of the following algorithms:

- $\text{BS.PGen}(1^\lambda) \rightarrow \text{par}$ takes a security parameter and returns parameters par .
- $\text{BS.KeyGen}(\text{par}) \rightarrow (\text{sk}, \text{pk})$ takes par and returns the key pair (sk, pk) .
- $\text{BS.Sign}(\text{par}, \text{sk}), \text{BS.User}(\text{par}, \text{pk}, m)$ a pair of interactive algorithms, where the signer takes a private key sk , the user takes a public key pk and message m , such that each comprises two subalgorithms defined as:
 - $\text{BS.Sign}_1(\text{par}, \text{sk}) \rightarrow (\text{state}_s, R)$ takes a private key sk , and returns the signer's state state_s and commitment R .
 - $\text{BS.User}_1(\text{par}, \text{pk}, R, m) \rightarrow (\text{state}_u, c)$ takes a public key pk , commitment R , and message m , and returns the user's state state_u and challenge c .
 - $\text{BS.Sign}_2(\text{par}, \text{sk}, \text{state}_s, c) \rightarrow s$ takes state_s and c , and returns the response s .
 - $\text{BS.User}_2(\text{par}, \text{pk}, \text{state}_u, s) \rightarrow \sigma$ takes state_u and s , and returns the signature σ .
- $\text{BS.Verify}(\text{pk}, m, \sigma) \rightarrow b$ takes a public key pk , message m , and a signature σ , and either accepts ($b = 1$) or rejects ($b = 0$).

Correctness. A blind signature scheme BS is correct if for all $\text{par} \leftarrow \text{BS.PGen}(1^\lambda)$, all keys $(\text{sk}, \text{pk}) \leftarrow \text{BS.KeyGen}(\text{par})$, all messages m and for

$$\begin{aligned} (\text{state}_s, R) &\leftarrow \text{BS.Sign}_1(\text{par}, \text{sk}) \\ (\text{state}_u, c) &\leftarrow \text{BS.User}_1(\text{par}, \text{pk}, R, m) \\ \sigma &\leftarrow \text{BS.User}_2(\text{par}, \text{pk}, \text{state}_u, \text{BS.Sign}_2(\text{par}, \text{sk}, \text{state}_s, c)) \end{aligned}$$

it holds that $\text{BS.Verify}(\text{pk}, m, \sigma) = 1$.

One-More Unforgeability (OMUF). The advantage of an adversary $\mathcal{A}$ against the one-more unforgeability of a three-move blind signature scheme BS is defined as:

$$\text{Adv}_{\text{BS}, \mathcal{A}}^{\text{omuf}}(\lambda) := \Pr[\text{OMUF}_{\text{BS}}^{\mathcal{A}}(\lambda) = 1], \quad (1)$$

where the game OMUF is defined in Fig. 1. The scheme BS is called one-more unforgeable if for all p.p.t. adversaries $\mathcal{A}$ it holds that $\text{Adv}_{\text{BS}, \mathcal{A}}^{\text{omuf}}(\lambda) = \text{negl}(\lambda)$.

Game $\text{OMUF}_{\text{BS}}^{\mathcal{A}}(\lambda)$	Oracle $\text{Ct}()$
$\text{par} \leftarrow \text{BS.PGen}(1^\lambda)$ $(\text{sk}, \text{pk}) \leftarrow \text{BS.KeyGen}(\text{par})$ $k := 0$ $(m_i, \sigma_i)_{i \in [\ell]} \leftarrow \mathcal{A}^{\text{Ct}, \text{Rp}}(\text{par}, \text{pk})$ $q_s := \{j \mid \text{sess}_j = \text{closed}\} $ return $q_s < \ell$ $\wedge \forall i \neq j \in [\ell] : (m_i, \sigma_i) \neq (m_j, \sigma_j)$ $\wedge \forall i \in [\ell] : \text{BS.Verify}(\text{pk}, m_i, \sigma_i) = 1$	$k := k + 1; \text{sess}_k := \text{open}$ $(\text{state}_k, R_k) \leftarrow \text{BS.Sign}_1(\text{sk})$ return (k, R_k) Oracle $\text{Rp}(j, c)$ if $\text{sess}_j \neq \text{open}$ then return $\perp$ $s_j \leftarrow \text{BS.Sign}_2(\text{state}_j, c)$ $\text{sess}_j := \text{closed}$ return s_j

Fig. 1. The (strong) One-More Unforgeability game for three-move blind signature schemes.

Game $\text{Blind}_{\text{BS}}^{\mathcal{A}}(\lambda)$	Oracle $\text{Ch}(i \in \{0, 1\}, R_i)$
$\text{par} \leftarrow \text{BS.PGen}(1^\lambda)$ $b \leftarrow \{0, 1\}; b_0 := b; b_1 := 1 - b$ $(\text{pk}, m_0, m_1) \leftarrow \mathcal{A}(\text{par})$ $b' \leftarrow \mathcal{A}^{\text{Ch}, \Sigma}(\text{par})$ return $b = b'$	if $\text{sess}_i \neq \perp$ then return $\perp$ $\text{sess}_i := \text{open}$ $(\text{state}_i, c_i) \leftarrow \text{BS.User}_1(\text{pk}, R_i, m_{b_i})$ return c_i Oracle $\Sigma(i \in \{0, 1\}, s_i)$ if $\text{sess}_i \neq \text{open}$ then return $\perp$ $\text{sess}_i := \text{closed}; \sigma_{b_i} \leftarrow \text{BS.User}_2(\text{state}_i, s_i)$ if $\sigma_0 \neq \perp \wedge \sigma_1 \neq \perp$ then return (σ_0, σ_1) return $\perp$

Fig. 2. Blindness game for three-move blind signature schemes.

Blindness. The advantage of an adversary $\mathcal{A}$ against the blindness of a three-move blind signature scheme BS is defined as:

$$\text{Adv}_{\text{BS}, \mathcal{A}}^{\text{blind}}(\lambda) := 2 \cdot \Pr[\text{Blind}_{\text{BS}}^{\mathcal{A}}(\lambda) = 1] - 1, \quad (2)$$

where the game Blind is defined in Fig. 2. The scheme BS is called computationally blind if for all p.p.t. adversaries $\mathcal{A}$ it holds that $\text{Adv}_{\text{BS}, \mathcal{A}}^{\text{blind}}(\lambda) = \text{negl}(\lambda)$.

2.3 Linear Function Families

We adopt the definition of linear function families of Backendal et al. [BBSS18]. A linear function family LF consists of:

1. a p.p.t. parameter generation algorithm LF.PGen , that on input the security parameter λ returns par , which defines two vector spaces $\mathcal{D} := \mathcal{D}(\text{par}), \mathcal{R} := \mathcal{R}(\text{par})$ over the scalar field $\mathcal{S} := \mathcal{S}(\text{par})$ with null vectors $0_{\mathcal{D}}, 0_{\mathcal{R}}$, respectively;

2. a deterministic polynomial-time evaluation function $\text{LF.F}(\text{par})$ defined by par , that implements a vector space homomorphism $F := \text{LF.F}(\text{par}) : \mathcal{D} \rightarrow \mathcal{R}$, i.e.,

$$\forall s \in \mathcal{S} \forall x, y \in \mathcal{D} : F(s \cdot x + y) = s \cdot F(x) + F(y).$$

3 Linear Blind Signatures

In this section, we introduce the concept of linear blind signatures expanding on the works of [BBSS18, HKL19]. We analyze the security requirements of these constructions in the AGM and ROM giving rise to a novel hardness assumption called CCROS. We generalize the p.t. ROS attack by Benhamouda et al. [BLL⁺21] to this setting. We show that any p.t. attack on the assumption translates directly into a p.t. attack on the OMUF of linear blind signatures. Finally, we prove the impossibility to construct computationally (or statistically, or perfectly) blind and one-more unforgeable linear blind signatures.

3.1 Linear Blind Signatures from Identification Schemes

To understand linear blind signature schemes, first consider three-move identification schemes between a prover and a verifier. First, the prover sends a *commitment* to the verifier. Then, the verifier replies with some *challenge*, to which the prover responds with a *response*. At last, the verifier either accepts or rejects based on the commitment, challenge, and response. Numerous constructions in the literature are captured by three-move identification schemes instantiated from linear function families, i.e., linear identification schemes [FS87, Sch91, GQ88, Oka93, Lyu09]. At its core lies an efficiently computable homomorphism F that is used to verify the response. Namely, a public-key pair is a pair (x, X) , where $X := F(x)$ is the public key and x is sampled uniformly at random. The commitment is a value $R := F(r)$ and the response is computed as $s := c \cdot x + r$, where c is the challenge from the verifier. The verifier can verify this linear relationship using F as $F(s) = c \cdot X + R$ since $F(c \cdot x + r) = c \cdot F(x) + F(r)$.

Linear signature schemes are constructed from linear identification schemes through a Fiat-Shamir transform by hashing the commitment along a message to compute the challenge [BBSS18]. Blind signatures can be obtained similarly using the framework by Hauck, Kiltz, and Loss [HKL19]. We extend the HKL framework to allow for arbitrary coefficient functions in the response s (cf. Fig. 3). Concretely, let $s := P(c)x + r$, where P is an arbitrary efficiently computable coefficient function. Setting P to the identity function yields the original framework. Note that any linear signature scheme with response $s := P(c)x + Q(c)r$, for some coefficient functions P, Q , can be transformed into a linear signature scheme with response $s' := P'(c)x + r$, for some coefficient function P' , such that any attack on the latter implies an attack on the former (see Lemma 3).

In the following, *blind* denotes a *blinding suite* which on input the parameters par specifies the randomness set Ω and the blinding functions

$$R' : \mathcal{R}^2 \times \Omega \rightarrow \mathcal{R}, \quad c : \mathcal{R}^2 \times \mathcal{C} \times \Omega \rightarrow \mathcal{C}, \quad s' : \mathcal{R}^2 \times \mathcal{C} \times \mathcal{D} \times \Omega \rightarrow \mathcal{D}.$$

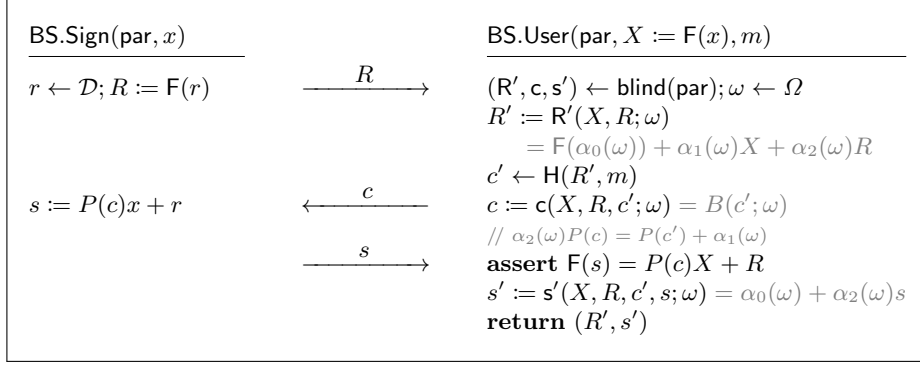


Fig. 3. Linear blind signature protocol BS[LF, H, blind]. The gray text shows the equations the blinding must satisfy, where $\alpha_0, \alpha_1, \alpha_2$ are efficiently computable functions.

Syntax. A linear blind signature BS[LF, H, blind] using the linear function family LF, random oracle H, and blinding suite $\text{blind} := (R', c, s')$ is a three-move blind signature scheme consisting of the following algorithms:

- BS.PGen(1^λ) $\rightarrow$ par takes a security parameter and outputs the parameters $\text{par} \leftarrow \text{LF.PGen}(1^\lambda)$, which implicitly define $H : \mathcal{R} \times \{0, 1\}^* \rightarrow \mathcal{C}$, $\text{blind}(\text{par})$, and the coefficient function $P : \mathcal{C} \rightarrow \mathcal{S}$.
- BS.KeyGen(par) $\rightarrow$ (sk, pk) takes parameters par and outputs the key pair (sk, pk := F(sk)), where $\text{sk} \leftarrow \mathcal{D}$ is sampled uniformly at random.
- BS.Sign(sk), BS.User(pk, m) are a pair of interactive algorithms specified by the protocol in Fig. 3.
- BS.Verify(pk, m, σ) $\rightarrow b$: takes a public key pk, message m, and a signature $\sigma = (R', s')$, and accepts ($b = 1$) (and otherwise rejects with $b = 0$)

$$F(s') = P(H(R', m)) \cdot \text{pk} + R'. \quad (3)$$

The functions R', c, s' input all previously defined values of the protocol, except the outputs of the functions themselves, which are defined implicitly by the other input values, e.g., c does not take the output R' of R' since it can recompute R' (cf. Fig. 3). Thus, this covers all possible ways to blind the construction. We assume algebraic access to $\mathcal{R}$, i.e., algorithms can only use the operations defined for $\mathcal{R}$, implying that $R'(X, R; \omega) = F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R$, for some functions $\alpha_0, \alpha_1, \alpha_2$. The rest of the blinding functions c, s' can be expressed using $\alpha_0, \alpha_1, \alpha_2$ by following the interactive protocol in Fig. 3 and using Eq. 3:

Lemma 1. Let LF be a linear function family, H a random oracle, $\text{blind} := (R', c, s')$ a blinding suite, BS[LF, H, blind] a linear blind signature with coefficient

function P , challenge set $\mathcal{C}$, and randomness space Ω . Assuming algebraic access to $\mathcal{R}$ and unforgeability of BS, there exist efficiently computable functions $\alpha_0 : \Omega \rightarrow \mathcal{D}, \alpha_1 : \Omega \rightarrow \mathcal{S}, \alpha_2 : \Omega \rightarrow \mathcal{S}, B : \mathcal{C} \times \Omega \rightarrow \mathcal{C}$ such that $\forall c' \in \mathcal{C}, \omega \in \Omega$:

$$R'(X, R; \omega) = F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R \quad (4)$$

$$c(X, R, c'; \omega) = B(c'; \omega) \quad (5)$$

$$s'(X, R, c', s; \omega) = \alpha_0(\omega) + \alpha_2(\omega)s \quad (6)$$

$$\alpha_2(\omega)P(B(c'; \omega)) = P(c') + \alpha_1(\omega) \quad (7)$$

with overwhelming probability.

Proof. Given the linear blind signature $\text{BS}[\text{LF}, \text{H}, \text{blind}]$, since R' is algebraic it can be written as

$$R'(X, R; \omega) = F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R, \quad (8)$$

where $\alpha_0, \alpha_1, \alpha_2$ are efficiently computable functions. In order for a signature $(R', s') := (R'(X, R; \omega), s'(X, R, c', s; \omega))$ to verify for message m , Eq. 3 must hold for $c' = H(R', m)$. Plugging in Eq. 8 into Eq. 3 yields

$$F(s'(X, R, c', s; \omega)) = P(c')X + F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R, \quad (9)$$

where X denotes the public key. Any valid transcript (R, c, s) satisfies $F(s) = P(c)X + R$. Substituting $R = F(s) - P(c)X$ in Eq. 9 and reordering yields

$$F(s'(X, R, c', s; \omega) - \alpha_0(\omega) - \alpha_2(\omega)s) = (P(c') + \alpha_1(\omega) - \alpha_2(\omega)P(c))X. \quad (10)$$

If the term in front of X is non-zero, then there exists a trivial attack on the OMUF of BS for $\ell = 2$:

Let $\mathcal{A}$ be an adversary against the OMUF of BS. It receives the parameters par , the public key X , and access to the oracles $\text{Ct}, \text{Rp}, \text{H}$. It queries $(1, R) \leftarrow \text{Ct}()$, samples $\omega \leftarrow \Omega$, computes $R' := R'(X, R; \omega)$, queries $c' \leftarrow H(R', m)$ for some message $m \in \{0, 1\}^*$, computes $c := c(X, R, c'; \omega)$, and queries $s \leftarrow \text{Rp}(1, c)$. At last, $\mathcal{A}$ computes

$$x := (P(c') + \alpha_1(\omega) - \alpha_2(\omega)P(c))^{-1}(s'(X, R, c', s; \omega) - \alpha_0(\omega) - \alpha_2(\omega)s),$$

samples $\hat{r} \leftarrow \mathcal{D}$, computes $\hat{R} := F(\hat{r})$, queries $\hat{c} \leftarrow H(\hat{R}, \hat{m})$ for some message $\hat{m} \in \{0, 1\}^*$, computes $\hat{s} := P(\hat{c}) \cdot x + \hat{r}$, and returns the forgeries $(R, s), (\hat{R}, \hat{s})$ on the messages $m, \hat{m}$.

The first signature is valid by definition, and the second is valid if Eq. 10 holds and therefore

$$\text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{A}}^{\text{omuf}}(\lambda) \geq \Pr[P(c') + \alpha_1(\omega) - \alpha_2(\omega)P(c) \neq 0],$$

implying that $P(c') + \alpha_1(\omega) = \alpha_2(\omega)P(c)$ with overwhelming probability. Observe that the right-hand side equals $\alpha_2(\omega)P(c(X, R, c'; \omega))$, and that the left-hand side is independent of X and R . Furthermore, these equations must hold for

any ω, c' sampled uniformly at random. Thus, there is a function $B : \mathcal{C} \times \Omega \rightarrow \mathcal{C}$ such that

$$c(X, R, c', \omega) = B(c', \omega). \quad (11)$$

Hence for c' and ω we have

$$\alpha_2(\omega)P(B(c', \omega)) = P(c') + \alpha_1(\omega). \quad (12)$$

Moreover, if the previous expression holds, then Eq. 10 implies

$$F(s'(X, R, c', s; \omega) - \alpha_0(\omega) - \alpha_2(\omega)s) = 0_{\mathcal{R}}.$$

Thus, $s'(X, R, c', s; \omega) - \alpha_0(\omega) - \alpha_2(\omega)s$ is in the kernel of F . Any blinding function s' may be redefined such that the previous expression is exactly $0_{\mathcal{D}}$ by subtracting the arising kernel element. Thus, w.l.o.g. it holds that

$$s'(X, R, c', s; \omega) = \alpha_0(\omega) + \alpha_2(\omega)s, \quad (13)$$

and Eqs. 8, 11, 12 and 13 yield the lemma. $\square$

Correctness. Let $m \in \{0, 1\}^*$ and for $x, r \leftarrow \mathcal{D}$ let

$$X := F(x) \quad \text{and} \quad R := F(r).$$

For $\omega \leftarrow \Omega$ define

$$R' := F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R,$$

and for $c' \leftarrow H(R', m)$ and $c := B(c'; \omega)$ let

$$s := P(c)x + r \quad \text{and} \quad s' := \alpha_0(\omega) + \alpha_2(\omega)s.$$

Then for $\sigma := (R', s')$ verification succeeds since

$$\begin{aligned} F(s') &= F(\alpha_0(\omega) + \alpha_2(\omega)s) = F(\alpha_0(\omega)) + \alpha_2(\omega)(P(c)X + R) \\ &\stackrel{\text{Eq. 7}}{=} F(\alpha_0(\omega)) + (P(c') + \alpha_1(\omega))X + \alpha_2(\omega)R = P(c')X + R'. \end{aligned}$$

Properties of the blinding suite. The probability that $P(B(c'; \omega)) = P(c')$, for $\omega \leftarrow \Omega$ sampled uniformly at random, must be negligible. Otherwise, there is an attack on the blindness of BS (see Lemma 2). Informally, the blinding function B does not hide the fact that the blinded challenge $c = B(c'; \omega)$ maps to the same image $P(c)$ as the challenge c' . This can be exploited to distinguish which signature containing c' was generated from which transcript containing c .

This attack succeeds as long as $P(c) \neq P(c'')$, where c'' is the challenge of the other signature not generated from the transcript containing c . If the probability that this equation holds is non-negligible, then there is an adversary against the OMUF of the scheme (see Lemma 2). Informally, the adversary uses

the function B to create two forgeries out of one. It first queries the signature (R', s') generated from the transcript (R, c, s) using the blinding suite. Then, it returns the forgeries $(R', s'), (R, s)$ on the messages m', m . The first forgery is valid due to correctness, and second forgery is valid when $P(c) = P(c'')$ for $c'' \leftarrow H(R, m)$.

The probability of $P(B(c'; \omega)) = P(c')$ being negligible implies that the probability that $P(c') + \alpha_1(\omega) = \alpha_2(\omega)P(c')$ holds is negligible (see Lemma 1). This is lower-bounded by the probability that $\alpha_1(\omega) = 0, \alpha_2(\omega) = 1$. This is used later to solve CCROS.

Lemma 2. *Let $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ be a linear blind signature with corresponding blinding functions α_1, α_2 . Then there exist p.p.t. adversaries $\mathcal{A}$ against the blindness of BS , making two random oracle queries to H , and $\mathcal{B}$ against the OMUF of BS , making one signing query and two random oracle queries, returning $\ell = 2$ forgeries, such that*

$$\text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{A}}^{\text{blind}}(\lambda) + \text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{B}}^{\text{omuf}}(\lambda) \geq \Pr_{\omega \leftarrow \Omega} [\alpha_1(\omega) = 0 \wedge \alpha_2(\omega) = 1]. \quad (14)$$

Proof. Let $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ be a linear blind signature. Let $\mathcal{A}$ be a p.p.t. distinguisher against the blindness of BS , and m_0, m_1 two distinct messages. The distinguisher samples $x \leftarrow \mathcal{D}$ and outputs $(\text{pk} := F(x), m_0, m_1)$ to the challenger. Then, $\mathcal{A}$ interacts with the challenge and signature oracles Ch, Σ (see Fig. 2) by following the protocol in Fig. 3: $\mathcal{A}$ samples $r_i \leftarrow \mathcal{D}$, queries $c_i \leftarrow \text{Ch}(i, F(r_i))$, computes $s_i := P(c_i)x + r_i$, and queries $\Sigma(i, s_i)$ for $i \in \{0, 1\}$. After the second call to Σ , $\mathcal{A}$ receives the signatures $\sigma_j := (R'_j, s'_j)$ on messages m_j for $j \in \{0, 1\}$. Then, $\mathcal{A}$ queries $c'_1 \leftarrow H(R'_1, m_1)$ and outputs 1 iff $P(c_0) = P(c'_1)$.

Let $\tau_i := (R_i, c_i, s_i)$ denote the transcripts of the two signing sessions for $i \in \{0, 1\}$. Let b be the bit of the challenger denoting that σ_j was generated during the session with the transcript $\tau_{j \oplus b}$. The advantage of $\mathcal{A}$ is

$$\begin{aligned} \text{Adv}_{\text{BS}, \mathcal{A}}^{\text{blind}}(\lambda) &= 2 \Pr[b = b'] - 1 = 2 \Pr[b = 1] \Pr_{c'_1 \leftarrow \mathcal{C}} [P(c_0) = P(c'_1) | b = 1] \\ &\quad + 2 \Pr[b = 0] \Pr_{c'_1 \leftarrow \mathcal{C}} [P(c_0) \neq P(c'_1) | b = 0] - 1 \\ &= \Pr_{\substack{c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [P(B(c'_1; \omega)) = P(c'_1)] + \Pr_{\substack{c'_0, c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [P(B(c'_0; \omega)) \neq P(c'_1)] - 1 \\ &= \Pr_{\substack{c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [\underbrace{\alpha_2(\omega)P(B(c'_1; \omega))}_{= P(c'_1) + \alpha_1(\omega)} = \alpha_2(\omega)P(c'_1) \wedge \alpha_2(\omega) \neq 0] \\ &\quad + \Pr_{\omega \leftarrow \Omega} [\alpha_2(\omega) = 0] - \Pr_{\substack{c'_0, c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [P(B(c'_0; \omega)) = P(c'_1)] \\ &\geq \Pr_{\omega \leftarrow \Omega} [\alpha_1(\omega) = 0 \wedge \alpha_2(\omega) = 1] - \Pr_{\substack{c'_0, c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [P(B(c'_0; \omega)) = P(c'_1)], \end{aligned} \quad (15)$$

where the probability that $P(B(c'_1; \omega)) = P(c'_1)$ is equivalent to the probability where both sides are multiplied by $\alpha_2(\omega)$, except when $\alpha_2(\omega) = 0$.

It remains to argue that there exists a p.p.t. adversary $\mathcal{B}$ against the OMUF of BS with advantage equal to the probability that $P(B(c'_0; \omega)) = P(c'_1)$. Adversary $\mathcal{B}$ is given the parameters par , public key X and oracles H , Ct , Rp . First, $\mathcal{B}$ samples $\omega \leftarrow \Omega$, queries $(1, R) \leftarrow \text{Ct}()$ and $c'_0 \leftarrow \text{H}(R'_0, m)$ for $R'_0 := F(\alpha_0(\omega)) + \alpha_1(\omega)X + \alpha_2(\omega)R$, and some message m'_0 . Then $\mathcal{B}$ queries $s \leftarrow \text{Rp}(1, c)$ for $c := B(c'_0; \omega)$, and sets $s'_0 := \alpha_0(\omega) + \alpha_2(\omega)s$ (cf. Lemma 1). Then, (R'_0, s'_0) is a valid signature on m'_0 due to correctness. Next, $\mathcal{B}$ sets $R'_1 := R$, $s'_1 := s$, samples some message $m'_1 \neq m'_0$, and queries $c'_1 \leftarrow \text{H}(R'_1, m'_1)$. At last, $\mathcal{B}$ returns the forgeries (R'_0, s'_0) , (R'_1, s'_1) on m'_0, m'_1 . The second signature is valid when $P(B(c'_0; \omega)) = P(c'_1)$ since

$$F(s'_1) = F(s) = P(B(c'_0; \omega))X + R = P(c'_1)X + R'_1,$$

where the second equality follows from the validity of the transcript (R, c, s) , which satisfies $F(s) = P(c)X + R$. Thus, the advantage of $\mathcal{B}$ is

$$\Pr_{\substack{c'_0, c'_1 \leftarrow \mathcal{C} \\ \omega \leftarrow \Omega}} [P(B(c'_0; \omega)) = P(c'_1)] = \text{Adv}_{\text{BS}, \mathcal{B}}^{\text{omuf}}(\lambda). \quad (16)$$

Eq. 16 and Eq. 15 yield the lemma. $\square$

Given a linear blind signature BS with response $s = P(c)x + Q(c)r$, a linear blind signature BS' with response $s = P'(c)x + r$ can be constructed by dividing out $Q(c)$ from the response of the former. This works as long as $Q(c)$ has an inverse, thus the challenge space $\mathcal{C}'$ of BS' contains only challenges c with $Q(c) \neq 0$. The reduction is then straightforward since an adversary against BS' can be perfectly simulated except when the random oracle of the challenger returns a $c \in \mathcal{C} \setminus \mathcal{C}'$. The probability of this is bounded by two constant-time adversaries against the OMUF of BS. One adversary succeeds whenever $P(c) \neq 0$ and $Q(c) = 0$, since then the response s reveals the secret key. The other succeeds whenever $P(c) = Q(c) = 0$, since then any $(R, 0_{\mathcal{D}})$ is a valid signature on m for $c = \text{H}(R, m)$.

Lemma 3. *Let LF be a linear function family, H a random oracle, $\text{BS}[\text{LF}, \text{H}]$ a linear blind signature scheme with response $s := P(c)x + Q(c)r$ for efficiently computable functions P, Q . Then there exists a signature scheme $\text{BS}'[\text{LF}, \text{H}']$ with response $s := P'(c)x + r$ such that the following holds. Given an adversary $\mathcal{A}$ against the OMUF of BS' running in time τ making q_h queries to H' and q_s queries to Ct . Then there exist adversaries $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2$ against the OMUF of BS such that $\mathcal{B}_0$ runs in time τ , and makes q_h queries to H and q_s queries to Ct , adversaries $\mathcal{B}_1, \mathcal{B}_2$ run in constant time, and make a constant number of queries to H and Ct such that*

$$\text{Adv}_{\text{BS}', \mathcal{A}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{BS}, \mathcal{B}_0}^{\text{omuf}}(\lambda) + q_h \text{Adv}_{\text{BS}, \mathcal{B}_1}^{\text{omuf}}(\lambda) + q_h \text{Adv}_{\text{BS}, \mathcal{B}_2}^{\text{omuf}}(\lambda).$$

Proof. Let $\text{BS}[\text{LF}, \text{H}]$ be a linear blind signature with response $s := P(c)x + Q(c)r$ for efficiently computable functions P, Q . Consider linear blind signature scheme $\text{BS}'[\text{LF}, \text{H}']$ which is the same as BS except the response is of the form

$$s := P'(c)x + r, \quad (17)$$

where $P' : \mathcal{C}' \rightarrow \mathcal{S}; c \mapsto (Q(c))^{-1}P(c)$ with the restricted challenge set $\mathcal{C}' := \{c \in \mathcal{C} \mid Q(c) \neq 0\}$, and $H' : \mathcal{R} \times \{0, 1\}^* \rightarrow \mathcal{C}'$.

Let $\mathcal{A}$ be an adversary against the OMUF of BS' running in time τ making q_h queries to H and q_s queries to Ct . Adversary $\mathcal{B}_0$ against the OMUF of BS is constructed as follows. Adversary $\mathcal{B}_0$ is given the parameters par , defining the linear function family LF and random oracle H , the public key X , and access to the commitment and response oracles Ct, Rp . First, $\mathcal{B}_0$ runs $(m_i, \sigma_i)_{i \in [\ell]} \leftarrow \mathcal{A}^{\text{Ct}', \text{Rp}', H'}(\text{par}, X)$ simulating the oracles Ct', Rp' as follows.

- $\text{Ct}' := \text{Ct}$,
- $\text{Rp}'(i, c \in \mathcal{C}') : \text{query } s \leftarrow \text{Rp}(i, c) \text{ and return } (Q(c))^{-1} \cdot s$,
- $H'(R, m) : \text{query } c \leftarrow H(R, m) \text{ if } Q(c) \neq 0 \text{ return } c, \text{ else abort.}$

At last, $\mathcal{B}_0$ returns $(m_i, \sigma_i)_{i \in [\ell]}$. It's advantage is

$$\text{Adv}_{\text{BS}', \mathcal{A}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{BS}, \mathcal{B}_0}^{\text{omuf}}(\lambda) + \Pr[\text{abort}]. \quad (18)$$

The probability of abort is bounded by

$$\begin{aligned} \Pr[\text{abort}] &\leq q_h \cdot \Pr_{c \leftarrow \mathcal{C}}[Q(c) = 0] \\ &\leq q_h \cdot \Pr_{c \leftarrow \mathcal{C}}[P(c) \neq 0 \wedge Q(c) = 0] + q_h \cdot \Pr_{c \leftarrow \mathcal{C}}[P(c) = 0 \wedge Q(c) = 0]. \end{aligned} \quad (19)$$

Consider the following adversary $\mathcal{B}_1$ against the OMUF of BS . Adversary $\mathcal{B}_1$ is given the parameters par , defining the linear function family LF and random oracle H , the public key X , and access to the commitment and response oracles Ct, Rp . Adversary $\mathcal{B}_1$ queries $R \leftarrow \text{Ct}()$, $c^* \leftarrow H(R, m)$, and $s \leftarrow \text{Rp}(i, c^*)$, for some message m . It returns the signatures $(F(r_i), P(c_i)(P(c^*))^{-1}s + Q(c_i)r_i)$, where $c_i = H(F(r_i), m_i)$ for some message m_i , for $i \in [2]$. The signatures are valid when $P(c^*) \neq 0$ and $Q(c^*) = 0$ implying $F(s) = P(c^*)X + Q(c^*)R = P(c^*)X$ since

$$F(s_i) = P(c_i)(P(c^*))^{-1}F(s) + Q(c_i)F(r_i) = P(c_i)X + Q(c_i)F(r_i).$$

The advantage of $\mathcal{B}_1$ is

$$\text{Adv}_{\text{BS}, \mathcal{B}_1}^{\text{omuf}}(\lambda) \geq \Pr_{c \leftarrow \mathcal{C}}[P(c) \neq 0 \wedge Q(c) = 0]. \quad (20)$$

Consider the following adversary $\mathcal{B}_2$ against the OMUF of BS . Adversary $\mathcal{B}_2$ is given the parameters par , defining the linear function family LF and random oracle H , the public key X , and access to the commitment and response oracles Ct, Rp . Adversary $\mathcal{B}_2$ samples $R \leftarrow \mathcal{R}$, set $s := 0_{\mathcal{D}}$, and returns $(m, (R, s))$ for some message m . Let $c^* = H(R, m)$. The signature is valid when $P(c^*) = Q(c^*) = 0$ since

$$P(c^*)X + Q(c^*)R = 0_{\mathcal{R}} = F(s).$$

The advantage of $\mathcal{B}_2$ is

$$\text{Adv}_{\text{BS}, \mathcal{B}_2}^{\text{omuf}}(\lambda) \geq \Pr_{c \leftarrow \mathcal{C}}[P(c) = Q(c) = 0]. \quad (21)$$

In conclusion, Eqs. 18, 19, 20 and 21 yield

$$\text{Adv}_{\text{BS}', \mathcal{A}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{BS}, \mathcal{B}_0}^{\text{omuf}}(\lambda) + q_h \text{Adv}_{\text{BS}, \mathcal{B}_1}^{\text{omuf}}(\lambda) + q_h \text{Adv}_{\text{BS}, \mathcal{B}_2}^{\text{omuf}}(\lambda). \quad \square$$

3.2 Security of Linear Blind Signatures

In this section, we introduce a novel variant of the ROS problem, termed Constrained Coset ROS (CCROS). To motivate the necessity of CCROS, we show that any attack against CCROS directly translates to an attack against the OMUF of a linear blind signature.

The ROS and the CCROS problem. The Random inhomogeneities in an Overdetermined System of linear equations problem (ROS) (see Fig. 4) was first introduced by Schnorr [Sch01] studying the OMUF of Schnorr and Okamoto-Schnorr signatures. The problem states that it is difficult to solve $\ell + 1$ linear equations in ℓ indeterminates where the right-hand sides are uniformly random values computed by hashing the coefficients of the equations.

We define a generalization of ROS called CCROS as defined in the Fig. 4. This problem is parametrized by a function $P : \mathcal{C} \rightarrow \mathcal{S}$ from the challenge set $\mathcal{C}$ to the scalar field $\mathcal{S}$. CCROS is equivalent to ROS if $\mathcal{C} = \mathcal{S}$ and P is an efficiently invertible bijection. The function P essentially constrains the solution set and the right-hand sides of the equations to lie in the image of P . In addition, the random oracle takes values ξ which define the range of the right-hand side as the *coset* $\xi + P(\mathcal{C})$. The problem states that it is difficult for an adversary to find an overdetermined matrix $(\rho_{i,j})_{i \in [\ell+1], j \in [\ell]}$, constants $(\xi)_{i \in [\ell+1]}$, and a solution vector $(\gamma_j)_{j \in [\ell]}$ such that for each $i \in [\ell + 1]$:

$$\sum_{j \in [\ell]} \rho_{i,j} P(\gamma_j) = P(H(\rho_{i,1}, \dots, \rho_{i,\ell}, \xi_i)) + \xi_i, \quad (22)$$

where the adversary is free to choose in which coset parametrized by ξ_i the sum lies.

The advantage of an adversary $\mathcal{A}$ against CCROS problem in ℓ indeterminates is defined as

$$\text{Adv}_{\text{PGen}, \ell, \mathcal{A}}^{\text{ccros}}(\lambda) = \Pr[\text{CCROS}_{\text{PGen}, \ell}^{\mathcal{A}}(\lambda) = 1], \quad (23)$$

where the game CCROS is defined in Fig. 4, and PGen is an algorithm which on input the security parameter returns parameters defining the challenge set $\mathcal{C}$, scalar field $\mathcal{S}$, and constraining function $P : \mathcal{C} \rightarrow \mathcal{S}$.

```

Game  $\text{ROS}_{\text{PGen}, \ell}^{\mathcal{A}}(\lambda)$ 
par  $\leftarrow \text{PGen}(1^\lambda)$  // defines  $\mathcal{S}$  s.t.  $\text{H} : \mathcal{S}^\ell \rightarrow \mathcal{S}$ 
 $((\rho_i \in \mathcal{S}^\ell)_{i \in [\ell+1]}, \gamma \in \mathcal{S}^\ell) \leftarrow \mathcal{A}^{\text{H}}(\text{par})$ 
return  $\forall i \neq j \in [\ell+1] : \rho_i \neq \rho_j \wedge \rho_i \cdot \gamma = \text{H}(\rho_i)$ 

Game  $\text{CCROS}_{\text{PGen}, \ell}^{\mathcal{A}}(\lambda)$ 
par  $\leftarrow \text{PGen}(1^\lambda)$  // defines  $\mathcal{C}, \mathcal{S}, P$  s.t.  $P : \mathcal{C} \rightarrow \mathcal{S}, \text{H} : \mathcal{S}^{\ell+1} \rightarrow \mathcal{C}$ 
 $((\rho_i \in \mathcal{S}^\ell)_{i \in [\ell+1]}, \xi \in \mathcal{S}^{\ell+1}, \gamma \in \mathcal{C}^\ell) \leftarrow \mathcal{A}^{\text{H}}(\text{par})$ 
return  $\forall i \neq j \in [\ell+1] : (\rho_i, \xi_i) \neq (\rho_j, \xi_j) \wedge P(\gamma) = P(\text{H}(\rho_i, \xi_i)) + \xi_i$ 

```

Fig. 4. The ROS game (top) and the Constrained Coset ROS game (bottom) where H is a random oracle.

Relation of CCROS and OMUF. In this section, a reduction of the OMUF of a linear blind signature to the CCROS problem is shown. The reduction is straightforward. Informally, given the public key X and an adversary against CCROS, the reduction first issues ℓ Rp-oracle queries receiving commitments $\mathbf{R} := (R_i)_{i \in [\ell]}$. Next, the reduction runs the adversary. On the i -th random oracle query $\text{H}_{\text{ccros}}(\rho_i, \xi_i)$ the reduction returns $c'_i \leftarrow \text{H}(R'_i, m_i)$, for $R'_i := \rho_i \cdot \mathbf{R} + \xi_i X$ and some message m_i . If the adversary returns $(\rho_i, \xi_i)_{i \in [\ell+1]}$ and γ satisfying Eq. 22 for $i \in [\ell+1]$, then the reduction finishes all ℓ sessions by querying $\text{Rp}(i, \gamma_i)$ to obtain $\mathbf{s} := (s_i)_{i \in [\ell]}$. It sets $s'_i := \rho_i \cdot \mathbf{s}$, and returns the forgeries (R'_i, s'_i) on m_i . The forgeries are all distinct and valid using the correctness of the signing transcripts and Eq. 22: $\text{F}(s'_i) = \rho_i \cdot P(\gamma)X + \rho_i \cdot \mathbf{R} = P(c'_i)X + R'_i$.

Theorem 1. *Let LF be a linear function family and H a random oracle. Let $\mathcal{A}$ be an adversary against CCROS of LF with constraining function P for ℓ indeterminates running in time τ and making at most q_h queries to its random oracle H_{ccros} . Then there exists an adversary $\mathcal{B}$ against the OMUF of $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ making q_h queries to H and ℓ queries to Ct and running in time $\tau + \mathcal{O}(q_h + \ell)$ such that*

$$\text{Adv}_{\text{BS.PGen}, \ell, \mathcal{A}}^{\text{ccros}}(\lambda) \leq \text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{B}}^{\text{omuf}}(\lambda). \quad (24)$$

Proof. Let $\mathcal{A}$ be an adversary against CCROS parametrized by BS.PGen in ℓ indeterminates running in time τ making at most q_h random oracle queries. Consider the adversary $\mathcal{B}$ against the OMUF of $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ (see Fig. 5). The adversary $\mathcal{B}$ is given the public key X , system parameters par , the signing oracles Ct , Rp , and the random oracle H . It opens ℓ sessions and receives $R_i \leftarrow \text{Ct}()$ for $i \in [\ell]$. Let $\mathbf{R} := (R_i)_{i \in [\ell]}$, and $\text{M} := ()$ an empty mapping. It runs $\mathcal{A}^{\text{H}_{\text{ccros}}(\cdot)}(\text{par})$ with

$$\text{H}_{\text{ccros}}(\rho, \xi) := \text{H}(\rho \cdot \mathbf{R} + \xi X, m),$$

where $m \in \{0, 1\}^*$ is the binary representation of the counter k for the k -th query. The message m is saved in the mapping $\text{M}(\rho, \xi) := m$. It receives $((\rho_i \in$

```

Game  $\text{CCROS}_{\text{PGen}, \ell, P}^A(\lambda)$ 
 $\mathbf{T} := (); \mathbf{par} \leftarrow \text{PGen}(1^\lambda)$  // defines  $\mathcal{C}, \mathcal{S}$  s.t.  $P : \mathcal{C} \rightarrow \mathcal{S}, H : \mathcal{S}^{\ell+1} \rightarrow \mathcal{C}$ 
 $\mathbf{M} := (); k := 0; \mathbf{R} := (R_i)_{i \in [\ell]}$  for  $(i, R_i) \leftarrow \text{Ct}()$ 
 $((\rho_i \in \mathcal{S}^\ell)_{i \in [\ell+1]}, \xi \in \mathcal{S}^{\ell+1}, \mathbf{c} \in \mathcal{C}^\ell) \leftarrow \mathcal{A}^{\text{H}_{\text{ccros}}}(\mathbf{par})$ 
 $\mathbf{s} := (s_i)_{i \in [\ell]}$  for  $s_i \leftarrow \text{Rp}(i, c_i)$  //  $(\mathbf{M}(\rho_i, \xi_i), (\rho_i \cdot \mathbf{R} + \xi_i X, \rho_i \cdot \mathbf{s}))$  are OMUF forgeries
return  $\forall i \neq j \in [\ell+1] : (\rho_i, \xi_i) \neq (\rho_j, \xi_j) \wedge \langle \rho_i, P(\mathbf{c}) \rangle - \xi_i = P(H(\rho_i, \xi_i))$ 

Oracle  $\text{H}_{\text{ccros}}(\rho, \xi)$ 
if  $\mathbf{T}(\rho, \xi) \neq \perp$  then return  $\mathbf{T}(\rho, \xi)$ 
 $\mathbf{T}(\rho, \xi) \leftarrow \mathcal{C}$ 
 $k := k + 1; m := b_{\log k} \dots b_0 // k = \sum_{i=0}^{\log k} 2^i b_i$ 
 $\mathbf{M}(\rho, \xi) := m; \mathbf{T}(\rho, \xi) \leftarrow H(\rho \cdot \mathbf{R} + \xi X, m)$ 
return  $\mathbf{T}(\rho, \xi)$ 

```

Fig. 5. The CCROS game. The lightgray statements show the OMUF reduction.

$\mathcal{S}^\ell)_{i \in [\ell+1]}, \xi \in \mathcal{S}^{\ell+1}, \mathbf{c} \in \mathcal{S}^\ell$). Let $m_i \in \mathcal{M}$ be the message s.t.

$$\text{H}_{\text{ccros}}(\rho_i, \xi_i) = H(\rho_i \cdot \mathbf{R} + \xi_i X, m_i), \quad (25)$$

as either ρ_i, ξ_i was queried before, or be queried at this point by the reduction. Adversary $\mathcal{B}$ finishes all open sessions with $s_i \leftarrow \text{Rp}(i, c_i)$ for $i \in [\ell]$. Let $\mathbf{s} := (s_i)_{i \in [\ell]}$, then for all $i \in [\ell]$ we have

$$F(s_i) = P(c_i)X + R_i. \quad (26)$$

When $\mathcal{A}$ returns the forgeries $(m_i, (R'_i := \rho_i \cdot \mathbf{R} + \xi_i X, s'_i := \rho_i \cdot \mathbf{s}))$ it succeeds if all (ρ_i, ξ_i) are distinct and

$$\rho_i \cdot P(\mathbf{c}) = P(\text{H}_{\text{ccros}}(\rho_i, \xi_i)) + \xi_i. \quad (27)$$

Then the forgeries are valid since for $i \in [\ell+1]$ we have

$$\begin{aligned}
F(s'_i) &= F(\rho_i \cdot \mathbf{s}) \stackrel{\text{F homomorphism}}{=} \rho_i \cdot F(\mathbf{s}) \stackrel{\text{Eq. 26}}{=} \rho_i \cdot (P(\mathbf{c}) \cdot X + \mathbf{R}) \\
&\stackrel{\text{Eq. 27}}{=} (P(\text{H}_{\text{ccros}}(\rho_i, \xi_i)) + \xi_i) \cdot X + \rho_i \cdot \mathbf{R} \\
&\stackrel{\text{Eq. 25}}{=} P(H(\rho_i \cdot \mathbf{R} + \xi_i X, m_i)) \cdot X + \rho_i \cdot \mathbf{R} + \xi_i X = P(H(R'_i, m_i)) \cdot X + R'_i.
\end{aligned}$$

The forgeries $(m_i, (\rho_i \cdot \mathbf{R} + \xi_i X, \rho_i \cdot \mathbf{s}))$ are all distinct since $m_i \neq m_j$ for all $i \neq j$ by construction. Thus, $\mathcal{B}$ wins the OMUF game whenever $\mathcal{A}$ wins the CCROS game. $\square$

3.3 Impossibility of Linear Blind Signatures

In this section, an attack on CCROS is shown closely following the strategy for the ROS attack outlined in [BLL⁺21, Theorem 1]. Then using the lemmas and

theorems proven in the previous sections, we prove the impossibility of linear blind signatures.

Attack on CCROS. We extend the polynomial-time attack of Benhamouda et al. [BLL⁺21] to CCROS for $\ell > \log q$. The ROS attack in [BLL⁺21] is defined over the field $\mathbb{Z}_p$. It can be generalized to CCROS for any extension field $\mathcal{S}$ of prime power order $q = p^m$ when given an isomorphism $\varphi : \mathcal{S} \rightarrow \mathbb{Z}_p^m$. The attack creates two sets of ℓ equations satisfying Eq. 22. The first set is trivial: ρ_i is the unit vector e_i and $\xi_i = 0$. The second set can be created using solutions to Eq. 29. The rest of the proof proceeds as in [BLL⁺21] where the binary decomposition of the hash of the $\ell + 1$ -th equation takes place in the coordinate space $\mathbb{Z}_p^m$.

Theorem 2. *Let $\mathcal{S}$ be a finite field of prime power order $q = p^m$ for $m \geq 1$, $\ell \geq m \lceil \log p \rceil$ an integer, $\mathcal{C}$ a challenge set, $H : \mathcal{S}^{\ell+1} \rightarrow \mathcal{C}$ a random oracle, $P : \mathcal{C} \rightarrow \mathcal{S}$ an efficiently computable function, φ an isomorphism between $\mathbb{Z}_p^m$ and $\mathcal{S}$ computable in time τ_φ . Then there is an adversary $\mathcal{A}$ against CCROS for ℓ indeterminates running in time $\mathcal{O}(\ell \cdot \tau + \tau_\varphi + \log q)$, making $\ell + 1 + \ell \cdot \kappa$ queries to H such that*

$$\text{Adv}_{\text{PGen}, \ell, \mathcal{A}}^{\text{ccros}}(\lambda) \geq \alpha^\ell, \quad (28)$$

where, for each $i \in [\ell]$, α is the probability to solve the following equation in time τ using κ random oracle queries in the indeterminates $x \in \mathcal{C}, (y, z) \in \mathcal{S}^\times \times \mathcal{S} \setminus \{(1, 0)\}$:

$$yP(x) - z = P(H(y \cdot e_i + z \cdot e_{\ell+1})). \quad (29)$$

Proof. In the following let $\hat{\rho}$ denote a polynomial of the form $\rho_0 + \rho_1 x + \dots + \rho_\ell x_\ell$ and $\rho \in \mathcal{S}[x_1, \dots, x_\ell]$ the vector $(\rho_1, \dots, \rho_\ell)$ without ρ_0 . For $i \in [\ell]$ let

$$\hat{\rho}_i^{(0)} := x_i, \mu_i^{(0)} := 1, \xi_i^{(0)} := 0, c_i^{(0)} \leftarrow H(\rho_i^{(0)}, \xi_i^{(0)}),$$

and compute the solution $c_i^{(1)}, \mu_i^{(1)}, \xi_i^{(1)}$ to Eq. 29 (in time τ with probability α using κ queries) such that $(\mu_i^{(1)}, \xi_i^{(1)}) \neq (1, 0)$, i.e.,

$$\mu_i^{(1)} \cdot P(c_i^{(1)}) - \xi_i^{(1)} = P(H(\mu_i^{(1)} \cdot e_i + \xi_i^{(1)} \cdot e_{\ell+1})). \quad (30)$$

Set $\hat{\rho}_i^{(1)} := \mu_i^{(1)} x_i$. If $\exists i^* \in [\ell] : P(c_{i^*}^{(0)}) = P(c_{i^*}^{(1)})$, then return

$$(\rho_1^{(0)}, \dots, \rho_\ell^{(0)}, \rho_{i^*}^{(1)}), (\xi_1^{(0)}, \dots, \xi_\ell^{(0)}, \xi_{i^*}^{(1)}), (c_1^{(0)}, \dots, c_\ell^{(0)}).$$

These solutions are valid since

$$\rho_i^{(0)} \cdot P(c) - \xi_i^{(0)} = P(c_i^{(0)}) = P(H(\rho_i^{(0)}, \xi_i^{(0)})) \text{ for } i \in [\ell],$$

and

$$\rho_{i^*}^{(1)} \cdot P(c) - \xi_{i^*}^{(1)} = \mu_{i^*}^{(1)} P(c_{i^*}^{(1)}) - \xi_{i^*}^{(1)} \stackrel{\text{Eq. 30}}{=} P(H(\rho_{i^*}^{(1)}, \xi_{i^*}^{(1)})).$$

Otherwise, $\forall i \in [\ell] : P(c_i^{(0)}) \neq P(c_i^{(1)})$. Observe that the finite field $\mathcal{S}$ forms a vector space over $\mathbb{Z}_p$, where vector addition is the field addition, and the product of a vector $s \in \mathcal{S}$ with a scalar $z \in \mathbb{Z}_p$ is defined as z applications of the field addition of s with itself. Furthermore, $\mathcal{S}$ is isomorphic to $\mathbb{Z}_p^m$, which also forms a vector space over $\mathbb{Z}_p$. Let $\varphi : \mathbb{Z}_p^m \rightarrow \mathcal{S}$ be the isomorphism. Then, φ defines a vector space isomorphism as well since $\varphi(z \cdot s + t) = z \cdot \varphi(s) + t$, for any $z \in \mathbb{Z}_p, s, t \in \mathbb{Z}_p^m$. Let $\ell_1, \dots, \ell_m$ be integers satisfying $\ell = \sum_{i=1}^m \ell_i, 2^{\ell_i} > p$. These integers exist since $\ell \geq m \lceil \log p \rceil$. Define

$$\hat{f}_i := \frac{x_i - P(c_i^{(0)})}{P(c_i^{(1)}) - P(c_i^{(0)})}, \quad \hat{\rho}_{\ell+1} := \sum_{i=1}^m \sum_{j=1}^{\ell_i} \hat{f}_{\ell_1+\dots+\ell_{i-1}+j} 2^{j-1} \varphi(\mathbf{e}_i).$$

The polynomial $\hat{f}_i$ is well-defined since the denominator is non-zero. Observe that $\hat{\rho}_{\ell+1}$ is a multivariate polynomial in ℓ variables, and that $\hat{f}_i(P(c_i^{(b)})) = b$. Let $y := P(c_{\ell+1}) + \rho_{\ell+1,0}$ for $c_{\ell+1} \leftarrow H(\rho_{\ell+1}, 0)$. Compute $\varphi^{-1}(y) = (y_1, \dots, y_m)$ in time τ_φ . Since $\ell_i > \log p$, it is possible to compute the binary decomposition $y_i = \sum_{j=1}^{\ell_i} b_{i,j} 2^{j-1}$, for all $i \in [m]$ in time $\mathcal{O}(\log q)$. Then,

$$\sum_{i=1}^m \sum_{j=1}^{\ell_i} b_{i,j} 2^{j-1} \varphi(\mathbf{e}_i) = \sum_{i=1}^m y_i \varphi(\mathbf{e}_i) = \varphi(\sum_{i=1}^m y_i \mathbf{e}_i) = \varphi((y_1, \dots, y_m)) = y,$$

and therefore

$$P(c_{\ell+1}) + \rho_{\ell+1,0} = \sum_{i=1}^m \sum_{j=1}^{\ell_i} b_{i,j} 2^{j-1} \varphi(\mathbf{e}_i). \quad (31)$$

Computing the bits $b_{i,j}$ takes time $\mathcal{O}(\tau_\varphi + \log q)$ in total. Return the solutions

$$\begin{aligned} &(\rho_1^{(b_{1,1})}, \dots, \rho_{\ell_1}^{(b_{1,\ell_1})}, \dots, \rho_\ell^{(b_{m,\ell_m})}, \rho_{\ell+1}), \\ &(\xi_1^{(b_{1,1})}, \dots, \xi_{\ell_1}^{(b_{1,\ell_1})}, \dots, \xi_\ell^{(b_{m,\ell_m})}, 0), \\ &(c_1^{(b_{1,1})}, \dots, c_{\ell_1}^{(b_{1,\ell_1})}, \dots, c_\ell^{(b_{m,\ell_m})}). \end{aligned}$$

These solutions are valid since for $i \in [m], j \in [\ell_i], h = \ell_1 + \dots + \ell_{i-1} + j$ we have

$$\rho_h^{b_{i,j}} \cdot P(\mathbf{c}) - \xi_h^{(b_{i,j})} = \mu_h^{(b_{i,j})} P(c_h^{(b_{i,j})}) - \xi_h^{(b_{i,j})} = P(H(\rho_h^{(b_{i,j})}, \xi_h^{(b_{i,j})})),$$

and

$$\begin{aligned} \rho_{\ell+1} \cdot P(\mathbf{c}) &= \hat{\rho}_{\ell+1}(P(\mathbf{c})) - \rho_{\ell+1,0} = \sum_{i=1}^m \sum_{j=1}^{\ell_i} \hat{f}_h(P(c_h^{(b_{i,j})})) 2^{j-1} y_i - \rho_{\ell+1,0} \\ &= \sum_{i=1}^m \sum_{j=1}^{\ell_i} b_{i,j} 2^{j-1} y_i - \rho_{\ell+1,0} \end{aligned}$$

$$\stackrel{\text{Eq. 31}}{=} P(c_{\ell+1}) + \rho_{\ell+1,0} - \rho_{\ell+1,0} = P(H(\rho_{\ell+1}, 0)).$$

This attack runs in time $\mathcal{O}(\ell \cdot \tau + \tau_\varphi + \log q)$, making $\ell + 1 + \ell \cdot \kappa$ random oracle queries, with success probability α^ℓ , depending on the time τ , probability α , and number of queries κ it takes to solve Eq. 29 for any $i \in [\ell]$. $\square$

Impossibility of linear blind signatures. When constructing a linear *blind* signature, the function P must exhibit a certain linearity (cf. Eq. 7). This, in turn, implies that the signatures themselves can be potentially combined linearly leading to a loss of security. Indeed, Eq. 29 can be solved using the blinding functions of the scheme when setting $x = B(c'; \omega)$, $y = \alpha_2(\omega)$, $z = \alpha_1(\omega)$, where c' is the hash evaluation and ω is sampled uniformly at random. The equation holds due to Eq. 7 unless $y = 1, z = 0$. If the scheme is computationally blind and one-more unforgeable, the probability that $y = 1, z = 0$ is negligible due to Lemma 2. Thus, CCROS can be solved in polynomial time when $\ell > \log q$ (Thm. 2), hence there is an adversary returning $\ell + 1$ signatures while opening ℓ signing sessions in polynomial time (Thm. 1) contradicting the assumption that the scheme is one-more unforgeable.

Theorem 3. *Let $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ be a linear blind signature, where LF is defined over the scalar field $\mathcal{S}$ of prime power order $q = p^m$, and let $\varphi : \mathcal{S} \rightarrow \mathbb{Z}_p^m$ be an isomorphism computable in time τ_φ . There does not exist BS that is computationally blind and one-more unforgeable: consider blinding a signature takes time β , then there exists an adversary $\mathcal{A}$ against OMUF of BS, for $\ell > \log q$, making at most q_h oracle queries to H, ℓ queries to Ct, and running in time $\mathcal{O}(\ell \cdot \beta + \tau_\varphi + \log q + \ell)$, such that*

$$\text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{A}}^{\text{omuf}}(\lambda) \geq 1 - \text{negl}(\lambda). \quad (32)$$

Proof. Let $\text{BS}[\text{LF}, \text{H}, \text{blind}]$ be a linear blind signature where LF is defined over the scalar field $\mathcal{S}$ of prime power order $q = p^m$ for $m \geq 1$. Given that BS is computationally blind and one-more unforgeable, for any p.p.t. $\mathcal{A}, \mathcal{B}$ due to Lemma 2 it holds that

$$\varepsilon := \Pr_{\omega \leftarrow \Omega} [\alpha_1(\omega) = 0 \wedge \alpha_2(\omega) = 1] \leq \text{Adv}_{\text{BS}, \mathcal{A}}^{\text{blind}}(\lambda) + \text{Adv}_{\text{BS}, \mathcal{B}}^{\text{omuf}}(\lambda) = \text{negl}(\lambda). \quad (33)$$

Then, Eq. 29 can be solved by sampling $\omega \leftarrow \Omega$ and setting $x := B(c'; \omega)$, $y := \alpha_2(\omega)$, $z := \alpha_1(\omega)$, for $c' \leftarrow \text{H}_{\text{ccros}}(y \cdot e_i + z \cdot e_{\ell+1})$ queried from the oracle defined in Theorem 2. Specifically for $i \in [\ell]$ we have

$$\alpha_2(\omega)P(B(c'; \omega)) - \alpha_1(\omega) = P(\text{H}_{\text{ccros}}(\alpha_2(\omega) \cdot e_i + \alpha_1(\omega) \cdot e_{\ell+1})),$$

due to Eq. 7. Using Eq. 33, the solution (y, z) is in $\mathcal{S}^\times \times \mathcal{S} \setminus \{(1, 0)\}$ with non-negligible probability $1 - \varepsilon$. Therefore, Eq. 29 can be solved in time β with probability $1 - \varepsilon$ using a single random oracle query, where β is the time it takes to blind a single transcript (R, c, s) . Thus, there is an adversary $\mathcal{A}$ solving the CCROS problem in ℓ indeterminates in time $\mathcal{O}(\ell \cdot \beta + \tau_\varphi + \log q)$ such that

$$\text{Adv}_{\text{LF}, \ell, P, \mathcal{A}}^{\text{ccros}}(\lambda) \geq (1 - \varepsilon)^\ell \geq 1 - \text{negl}(\lambda),$$

while making $2\ell + 1$ queries to H_{ccros} due to Theorem 2. Consequently, there is an adversary $\mathcal{B}$ against the OMUF of BS, making $2\ell + 1$ random oracle queries and ℓ signing queries, running in time $\tau := \mathcal{O}(\ell \cdot \beta + \tau_\varphi + \log q + \ell)$, such that by Theorem 1 we get

$$\text{Adv}_{\text{BS}[\text{LF}, \text{H}, \text{blind}], \mathcal{B}}^{\text{omuf}}(\lambda) \geq \text{Adv}_{\text{LF}, \ell, P, \mathcal{A}}^{\text{ccros}}(\lambda) \geq 1 - \text{negl}(\lambda). \quad \square$$

A direct consequence of Thm. 3 is that if BS is computationally blind and one-more unforgeable (in polynomial time), then $\mathcal{O}(\ell \cdot \beta + \tau_\varphi + \log q + \ell)$ must be super-polynomial. The values $\beta, \log q$ are polynomial (in the security parameter) by definition, otherwise the protocol cannot be executed in polynomial time as blinding or basic operations in $\mathcal{D}, \mathcal{R}, \mathcal{S}$ would take super-polynomial time. The parameter ℓ denotes the number of concurrent signing sessions any p.p.t. adversary can open, hence it is assumed to be polynomial. By elimination, τ_φ must be super-polynomial.

If adversaries only have black-box access to $\mathcal{S}^1$, then OMUF is reducible to the isomorphism problem as defined by Maurer and Raub [MR07]. This problem is efficiently reducible to the extraction problem in the prime field of $\mathcal{S}$ [MR07, Corollary 3]. A result by Boneh and Lipton shows that the extraction problem can be solved in sub-exponential time [BL96, Theorem 8] under a (plausible) number-theoretic conjecture, in particular in time

$$\exp\left((2 + o(1))\sqrt{\log p \cdot \log \log p}\right). \quad (34)$$

Thus, there is a sub-exponential-time adversary against the OMUF of BS for any scalar field $\mathcal{S}$. Moreover, there is an algorithm in the non-uniform model of computation solving the extraction—and hence the isomorphism—problem in polynomial time in $\log p$ [Mau94].

Otherwise, if $\mathcal{S} = \mathbb{Z}_{p^m}$, then $\tau_\varphi = 0$ since the prime field of $\mathcal{S}$ is $\mathbb{Z}_p$, hence φ is the identity function and need not be computed, and hence BS is forgeable.

4 Toward Concurrently Secure Blind Signature Schemes

As seen in Sec. 3, there is a sub-exponential-time attack on the OMUF of computationally blind signatures instantiated from linear function families with a single commitment. Furthermore, when the scalar field is represented as integers in $\mathbb{Z}_q$, then there is a polynomial-time attack on either blindness or OMUF of the scheme. We are not aware of any finite field implementations for which the integer counterparts of their field elements are hard to compute.

Therefore, all existing computationally blind and one-more unforgeable linear blind signatures (that use one commitment) must be instantiated using black-box scalar fields requiring impractical parameter sizes in the ROM.

In this section, linear blind signatures are extended to the setting of two commitments. First, a case study of the blind signature scheme by Barreto and Zanon [BZ23] is presented, which was later shown to be not one-more unforgeable [RCK⁺25]. Building on their construction, two perfectly blind and one-more unforgeable variants, termed Schnorr² and Okamoto-Schnorr², are presented along with a proof in the AGM+ROM.

¹ Meaning, adversaries obtain a string representation of the field elements and must query oracles to compute field operations.

4.1 Case Study: BZ

Given a cyclic abelian group $\mathbb{G}$ of prime order p and generator G such that the discrete-logarithm problem is hard in $\mathbb{G}$, and given the random oracle $\mathbf{H} : \mathbb{G}^2 \times \{0, 1\}^* \rightarrow (\mathbb{Z}_p^\times)^2$. Let $(x, X := xG)$ be a key pair where $x \leftarrow \mathbb{Z}_p$ is sampled uniformly at random. The scheme BZ proposed by Barreto and Zanon [BZ23] proceeds as follows (the blinding factors are omitted for the sake of clarity). The signer sends two group elements $R := rG, T := tG$ to the user, with $r, t \leftarrow \mathbb{Z}_p$. The user responds with two challenges $(c, d) \leftarrow \mathbf{H}(R, T, m)$ for some message m . Finally, the signer returns the response $s := cdx + dr + t$. The user verifies the transcript by checking that $sG = cdX + dR + T$.

The construction BZ can be conceptualized as two “applications” of Schnorr. Given the key pair (x, xG) , the first application computes $R := rG, s := cx + r$, for $r \leftarrow \mathbb{Z}_p$ and some challenge c , creating the one-time key pair $(s, sG = cX + R)$. The second application computes $T := tG, z := ds + t$, for $t \leftarrow \mathbb{Z}_p$ and challenge d . Thus, (T, z) is a Schnorr signature under the one-time public key sG .

BZ was shown insecure for a polynomial number of concurrent signing sessions [RCK⁺25], resulting from the realization that it is no harder than a single “application” of Schnorr. Informally, given the random oracle $\mathbf{H}$, commitment oracle $\mathbf{Ct}$, and response oracle $\mathbf{Rp}$ for BZ, querying $\mathbf{Rp}(i, c, 1)$ returns valid Schnorr responses since $s = cx + (r + t)$, where $(r + t)G$ is the Schnorr commitment. Given an adversary $\mathcal{A}_{\text{Sch}}$ against Schnorr, the reduction simulates the oracles as follows: $\mathbf{Ct}_{\text{Sch}}() := R + T$ for $(R, T) \leftarrow \mathbf{Ct}()$, $\mathbf{Rp}_{\text{Sch}}(i, c) := \mathbf{Rp}(i, c, 1)$. When simulating random oracle queries, the second commitment of BZ can be freely chosen: $\mathbf{H}_{\text{Sch}}(R_i, m_i) := c_i$ for $(c_i, d_i) \leftarrow \mathbf{H}(R_i, \delta_i G, m)$ for uniform $\delta_i \leftarrow \mathbb{Z}_p$. Thus, when $\mathcal{A}_{\text{Sch}}$ returns the forgeries $(m_i, (R'_i, s'_i))_{i \in [\ell+1]}$ satisfying $s'_i G = \mathbf{H}_{\text{Sch}}(R'_i, m_i)X + R'_i$, then the reduction returns the forgeries $(m_i, (R'_i, T'_i := \delta'_i G, z'_i := d'_i s'_i + \delta'_i))$, where $(c'_i, d'_i) = \mathbf{H}(R'_i, \delta'_i G, m_i)$. The forgeries are valid BZ signatures since

$$z'_i G = d'_i s'_i G + \delta'_i G = d'_i \mathbf{H}_{\text{Sch}}(R'_i, m_i)X + d'_i R'_i + T'_i = c'_i d'_i X + d'_i R'_i + T'_i.$$

Intuitively, splitting the challenge into two challenges increases the power of an adversary: it can always choose $d = 1$ to obtain simple Schnorr signatures. Moreover, as seen in the previous sections, single commitment schemes are impossible in general. Therefore, the main idea of the following sections is to construct a 2-commitment scheme with a *single* challenge.

4.2 2-Commitment Blind Signatures from Linear Function Families

Definition. The 2-commitment blind signature $2\text{BS}[\text{LF}, \mathbf{H}]$ using the linear function family LF and random oracle $\mathbf{H}$ consists of the following algorithms:

- $2\text{BS.PGen}(1^\lambda) \rightarrow \text{par}$ takes a security parameter, returns $\text{par} \leftarrow \text{LF.PGen}(1^\lambda)$, which defines the homomorphism $\mathbf{F} : \mathcal{D} \rightarrow \mathcal{R}$, where $\mathcal{D}, \mathcal{R}$ are vector spaces over the scalar field $\mathcal{S}$, and the random oracle $\mathbf{H} : \mathcal{R}^2 \times \{0, 1\}^* \rightarrow \mathcal{S}^\times$.

- $2BS.KeyGen(\text{par}) \rightarrow (\text{sk}, \text{pk})$ takes parameters par and returns the key pair (sk, pk) , where $\text{sk} \leftarrow \mathcal{D}$, $\text{pk} := F(\text{sk})$.
- $2BS.Sign(\text{par}, \text{sk}), 2BS.User(\text{par}, \text{pk}, m)$ are a pair of interactive algorithms specified by the protocol in Fig. 6.
- $2BS.Verify(\text{pk}, m, \sigma)$ takes a public key pk , message m , and a signature $\sigma = (R', T', s')$, sets $c' \leftarrow H(R', T', m)$, and returns

$$F(s') = c' \cdot \text{pk} + R' + (c')^{-1} \cdot T'. \quad (35)$$

Signature variants. A signature on a message m produced by 2BS consists of two commitments $R, T \in \mathcal{R}$ and a response $s \in \mathcal{D}$. Consider the variant $2BS'$ where R is replaced by the challenge $c \leftarrow H(R, T, m)$, i.e., $\sigma = (c, T, s)$. Verification for this variant works as follows: first compute $R := F(s) - c \cdot \text{pk} - c^{-1} \cdot T$ and accept iff $c = H(R, T, m)$. Blindness follows directly from the original scheme as the schemes are identical up to post-processing.

The reduction to the OMUF of the original scheme is trivial: let $\mathcal{A}$ be an adversary against the OMUF of $2BS'$, the reduction forwards the parameters par and public pk to $\mathcal{A}$, and simulates $\mathcal{A}$'s oracle queries using its own oracles. When $\mathcal{A}$ returns the forgeries $(m_i, (c_i, T_i, s_i))_{i \in [\ell+1]}$, the reduction computes $R_i := F(s_i) - c_i \cdot \text{pk} - c_i^{-1} \cdot T_i$, and returns $(m_i, (R_i, T_i, s_i))_{i \in [\ell+1]}$. The reduction's forgeries are valid whenever $\mathcal{A}$'s forgeries are valid. Thus, $\text{Adv}_{2BS'[\text{LF}, \text{H}], \mathcal{A}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{2BS[\text{LF}, \text{H}], \mathcal{B}}^{\text{omuf}}(\lambda)$.

Correctness. Let $m \in \{0, 1\}^*$ and for $\text{sk}, r, t \leftarrow \mathcal{D}$ define

$$\text{pk} := F(\text{sk}) \quad \text{and} \quad R := F(r) \quad \text{and} \quad T := F(t).$$

For $\alpha, \gamma \leftarrow \mathcal{D}$ and $\beta \leftarrow \mathcal{S}^\times$ let

$$R' := \beta \cdot R + F(\alpha) \quad \text{and} \quad T' := \beta^2 \cdot T + F(\gamma).$$

Then for $c' \leftarrow H(R', T', m)$ and $c := c'\beta^{-1}$ define

$$s := c \cdot \text{sk} + r + c^{-1} \cdot t \quad \text{and} \quad s' := \beta \cdot s + \alpha + (c')^{-1} \cdot \gamma,$$

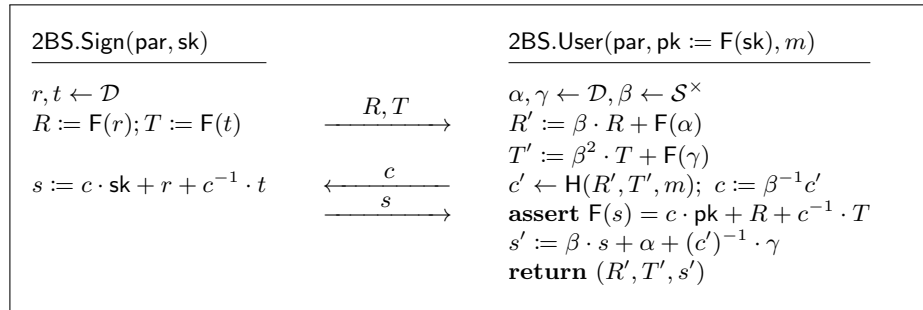


Fig. 6. The 2-commitment blind signature 2BS from the linear function family LF.

which verifies since

$$\begin{aligned}
F(s') &= \beta F(s) + F(\alpha) + (c')^{-1} F(\gamma) \\
&= \beta(c \cdot \text{pk} + R + c^{-1} \cdot T) + F(\alpha) + (c')^{-1} \cdot F(\gamma) \\
&= c' \cdot \text{pk} + \beta \cdot R + (c')^{-1} \beta^2 \cdot T + F(\alpha) + (c')^{-1} \cdot F(\gamma) \\
&= c' \cdot \text{pk} + R' + (c')^{-1} \cdot T'.
\end{aligned}$$

Blindness. The goal of an adversary against the blindness of 2BS is to determine which signature σ_j on message m_j resulted from which transcript τ_i , for $i, j \in \{0, 1\}$. For each bit $b' \in \{0, 1\}$ output by the adversary, there is a $state_{b'}$ of blinding parameters distributed independently and uniformly over $\mathcal{D} \times \mathcal{S}^\times \times \mathcal{D}$ (as defined in 2BS.User), explaining that σ_j was generated from $\tau_{b' \oplus j}$ in the view of the adversary.

The idea is that the output of the random oracle c'_j and the blinding parameters α_j, γ_j define a properly distributed state $(\alpha_{i,j}, \beta_{i,j}, \gamma_{i,j})$ such that $R'_j = \beta_{i,j} R_i + F(\alpha_{i,j})$, $T'_j = \beta_{i,j}^2 T_i + F(\gamma_{i,j})$, $c'_j = \beta_{i,j} c_i$, $s'_j = \beta_{i,j} s_i + \alpha_{i,j} + c_j'^{-1} \gamma_{i,j}$ hold. Thus, σ_j could have resulted from either transcript τ_0 or τ_1 .

Theorem 4 (Perfect blindness). *Let 2BS[LF, H] be a 2-commitment blind signature scheme using the linear function family LF with a surjective evaluation function F. For any adversary $\mathcal{A}$ against the blindness of 2BS in the ROM it holds that*

$$\text{Adv}_{2\text{BS}[\text{LF}, \text{H}], \mathcal{A}}^{\text{blind}}(\lambda) = 0. \quad (36)$$

Proof. Let $\mathcal{A}$ be an adversary against the blindness of 2BS[LF, H]. It obtains the parameters par for LF defining F, and outputs the public key pk and the messages $m_0, m_1 \in \{0, 1\}^*$. Then, $\mathcal{A}$ is given access to the random oracle H, challenge oracle Ch, and signature oracle Σ . It impersonates the signer with public key pk for two sessions generating two transcripts $\tau_i := (R_i, T_i, c_i, s_i)$ for $i \in \{0, 1\}$. After closing both sessions, $\mathcal{A}$ receives the signatures $\sigma_j := (R'_j, T'_j, s'_j)$ for $j \in \{0, 1\}$. The goal of the adversary is to determine which signature σ_j on message m_j resulted from which transcript τ_i . If there are properly distributed blinding parameters of 2BS.User for each pair (τ_i, σ_j) , then $\mathcal{A}$'s output bit is independent of whether σ_j was generated from τ_0 or τ_1 , since each case is explained by the blinding parameters defined by (τ_i, σ_j) in the view of $\mathcal{A}$.

It remains to argue that for all bits $b' \in \{0, 1\}$ output by $\mathcal{A}$, there are blinding parameters $state_{b'} := (\alpha_{i,j}, \beta_{i,j}, \gamma_{i,j})_{j \in \{0, 1\}}$, for $i = j \oplus b'$, distributed uniformly and independently over $\mathcal{D} \times \mathcal{S}^\times \times \mathcal{D}$ conditioned on the view of $\mathcal{A}$ before it obtains the signatures, and such that

$$R'_j = \beta_{i,j} \cdot R_i + F(\alpha_{i,j}) \quad (37)$$

$$T'_j = \beta_{i,j}^2 \cdot T_i + F(\gamma_{i,j}) \quad (38)$$

$$c'_j = \beta_{i,j} c_i \quad (39)$$

$$s'_j = \beta_{i,j} \cdot s_i + \alpha_{i,j} + (c'_j)^{-1} \cdot \gamma_{i,j} \quad (40)$$

for $j \in \{0, 1\}$, after $\mathcal{A}$ obtains them.

Let the bit $b \in \{0, 1\}$ define which transcript was used to produce which signature by the challenger, and define $b_0 := b, b_1 := \neg b$. Then, τ_i generates σ_{b_i} , or equivalently σ_j is generated by τ_{b_j} , for $i, j \in \{0, 1\}$.

Consider the view of $\mathcal{A}$ before it obtains the signatures. Define $\beta_{i,j} := c'_j c_i^{-1}$. The value $\beta_{i,j}$ is uniformly distributed over $\mathcal{S}^\times$ since $c'_j = H(R'_j, T'_j, m_j)$ produces uniform values.

Since F is surjective, there are preimages t_i, t'_j of T_i, T'_j , respectively. The value $\gamma_{i,j} := t'_j - \beta_{i,j}^2 \cdot t_i$ is uniform in $\mathcal{D}$ if $t'_j := \beta_j^2 \cdot t_{b_j} + \gamma_j$ is uniform in $\mathcal{D}$ independent of $\beta_{i,j}$. Uniformity of t'_j is implied by the uniformity of γ_j sampled by the challenger.

The value $\alpha_{i,j} := s'_j - \beta_{i,j} \cdot s_i - (c'_j)^{-1} \cdot \gamma_{i,j}$ is uniform in $\mathcal{D}$ if $s'_j := \beta_j \cdot s_{b_j} + \alpha_j + (c'_j)^{-1} \cdot \gamma_j$ is uniform in $\mathcal{D}$ independent of $\beta_{i,j}, \gamma_{i,j}$. Uniformity of s'_j is implied by the uniformity of α_j sampled by the challenger.

Therefore, the random variables in $state_{b'}$ are mutually independent and distributed uniformly over $\mathcal{D} \times \mathcal{S}^\times \times \mathcal{D}$, for any $b' \in \{0, 1\}$ conditioned on the view of $\mathcal{A}$ before receiving the signatures.

After $\mathcal{A}$ observes the signatures, Eqs. 38, 39 and 40 are satisfied by definition. It remains to argue that Eq. 37 holds. Consider the case when $\mathcal{A}$ closes its signing sessions honestly, thus receiving signatures $\sigma_0 \neq \perp$ and $\sigma_1 \neq \perp$. Otherwise, there is nothing to compare and $\mathcal{A}$ has no better advantage than guessing. Adversary $\mathcal{A}$ receives valid signatures whenever the assertion $F(s_i) = c_i \cdot \mathbf{pk} + R_i + c_i^{-1} \cdot T_i$ holds, for $i \in \{0, 1\}$. Then, the signatures themselves must be valid as well, thus $F(s'_j) = c'_j \cdot \mathbf{pk} + R'_j + (c'_j)^{-1} \cdot T'_j$. Therefore,

$$\begin{aligned} \beta_{i,j} \cdot R_i + F(\alpha_{i,j}) &= \beta_{i,j} \cdot R_i + F(s'_j) - \beta_{i,j} \cdot F(s_i) - (c'_j)^{-1} \cdot F(\gamma_{i,j}) \\ &= \beta_{i,j} \cdot R_i + c'_j \cdot \mathbf{pk} + R'_j + (c'_j)^{-1} \cdot T'_j \\ &\quad - \beta_{i,j} \cdot (c_i \cdot \mathbf{pk} + R_i + c_i^{-1} \cdot T_i) - (c'_j)^{-1} \cdot F(\gamma_{i,j}) \\ &= \beta_{i,j} \cdot R_i + c'_j \cdot \mathbf{pk} + R'_j + (c'_j)^{-1} \cdot T'_j \\ &\quad - c'_j \cdot \mathbf{pk} - \beta_{i,j} \cdot R_i - (c'_j)^{-1} \beta_{i,j}^2 \cdot T_i - (c'_j)^{-1} \cdot F(\gamma_{i,j}) \\ &= R'_j + (c'_j)^{-1} \cdot T'_j - (c'_j)^{-1} \beta_{i,j}^2 \cdot T_i - (c'_j)^{-1} \cdot F(\gamma_{i,j}) \\ &= R'_j + (c'_j)^{-1} \cdot T'_j - (c'_j)^{-1} \beta_{i,j}^2 \cdot T_i - (c'_j)^{-1} \cdot T'_j + (c'_j)^{-1} \beta_{i,j}^2 \cdot T_i = R'_j, \end{aligned}$$

and for all $b' \in \{0, 1\}$ $state_{b'} = (\alpha_{j \oplus b', j}, \beta_{j \oplus b', j}, \gamma_{j \oplus b', j})_{j \in \{0, 1\}}$ defines independently and uniformly distributed blinding parameters implying that σ_j was generated by $\tau_{j \oplus b'}$. Hence, $\mathcal{A}$ has no better advantage than guessing. $\square$

One-more unforgeability. The OMUF of 2BS reduces to solving either the Algebraic One-More Preimage problem (AOMP_{Pre}), the Second Preimage problem (2ndPre), or solving the quadratic ROS over a boolean Hypercube problem (HyperROqS).

AOMP_{Pre} is a falsifiable assumption which generalizes the algebraic one-more discrete-logarithm problem (cf. Fig. 10). Given a linear function family LF, the adversary succeeds if it returns the preimages (w.r.t. F) of all elements it received

Game $\text{AOMPre}_{\text{PGen}}^{\mathcal{A}}(\lambda)$	Oracle $\text{Chal}()$	Oracle $\text{Pre}((\alpha_i)_{i \in [c]_0})$
$\text{par} \leftarrow \text{PGen}(1^\lambda); c, d := 0$ $(y_1, \dots, y_c) \leftarrow \mathcal{A}^{\text{Chal}, \text{Pre}}(\text{par})$ return $d < c \wedge \forall i \in [c] : F(x_i) = F(y_i)$	$c := c + 1$ $x_c \leftarrow \mathcal{D}$ return $F(x_c)$	$// X := F(\alpha_0) + \sum_{i \in [c]} \alpha_i F(x_i)$ $d := d + 1$ return $\alpha_0 + \sum_{i \in [c]} \alpha_i x_i$

Fig. 7. Algebraic One-More Preimage resistance (AOMPre) game.

Game $\text{2ndPre}_{\text{PGen}}^{\mathcal{A}}(\lambda)$
$\text{par} \leftarrow \text{PGen}(1^\lambda); x \leftarrow \mathcal{D}$ $x' \leftarrow \mathcal{A}(\text{par}, x, F(x))$ return $x \neq x' \wedge F(x) = F(x')$

Fig. 8. Second-preimage resistance (2ndPre) game, where F is a many-to-one mapping.

from the challenge oracle, while issuing fewer preimage queries than challenge queries. Furthermore, on each preimage query of an $\mathcal{R}$ element, a representation explaining how the queried element was computed using previous challenges must be supplied (see Sec. 2.1). The advantage of an adversary $\mathcal{A}$ against the AOMPre problem w.r.t. the linear function family LF is defined as

$$\text{Adv}_{\text{LF}, \mathcal{A}}^{\text{aompre}}(\lambda) = \Pr[\text{AOMPre}_{\text{LF.PGen}}^{\mathcal{A}}(\lambda) = 1], \quad (41)$$

where the game AOMPre is defined in Fig. 7.

Given a linear function family LF , the 2ndPre problem states that it is hard to find second preimages of F . The advantage of an adversary $\mathcal{A}$ against the second-preimage resistance problem w.r.t. the linear function family LF is defined as

$$\text{Adv}_{\text{LF}, \mathcal{A}}^{\text{2ndpre}}(\lambda) = \Pr[\text{2ndPre}_{\text{LF.PGen}}^{\mathcal{A}}(\lambda) = 1], \quad (42)$$

where the game 2ndPre is defined in Fig. 11.

HyperROqS is a statistically hard variant of ROS (see Thm. 6). The advantage of an adversary $\mathcal{A}$ against HyperROqS for ℓ indeterminates for the parameter generation algorithm PGen is defined as

$$\text{Adv}_{\text{PGen}, \ell, \mathcal{A}}^{\text{hyperroqs}}(\lambda) = \Pr[\text{HyperROqS}_{\text{PGen}, \ell}^{\mathcal{A}}(\lambda) = 1], \quad (43)$$

where the game HyperROqS is defined in Fig. 9.

In the following, a high-level overview of the proof of OMUF is given. Consider an adversary that returns $\ell + 1$ forgeries $(m_i, (R'_i, T'_i, s'_i))$ after issuing ℓ signing queries resulting in the responses (R_j, T_j) and s_j . Since the adversary is algebraic, it must output the representations $\gamma_i^{(1)}, \gamma_i^{(2)}, \xi_i^{(1)}, \xi_i^{(2)}, \rho_i^{(1)}, \theta_i^{(1)}, \rho_i^{(2)}$,

```

Game HyperROqSPGen,ℓA(λ)
par ← PGen(1λ) // par defines finite field  $\mathbb{F}$  of order  $q$ 
 $((\alpha_i \in \mathbb{F}^{2\ell+1}, \beta_i \in \mathbb{F}^{2\ell+1})_{i \in [\ell+1]}, \mathbf{c} \in (\mathbb{F}^\times)^\ell) \leftarrow \mathcal{A}^H(\text{par}, \ell)$  //  $H: \mathbb{F}^{4\ell+2} \rightarrow \mathbb{F}^\times$  rand.orac.
return  $\forall i \neq j \in [\ell+1] : (\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ 
 $\wedge \forall i \in [\ell+1] \forall \mathbf{b} \in \{0, 1\}^\ell :$  // let  $\neg \mathbf{b} := \mathbf{1} - \mathbf{b}$  and “ $\odot$ ” denote inner prod.
 $(H(\alpha_i, \beta_i))^2 + (H(\alpha_i, \beta_i)\alpha_i + \beta_i) \cdot (1, \mathbf{b} \odot \mathbf{c}, \neg \mathbf{b} \odot \mathbf{c}^2) = 0$ 

```

Fig. 9. The HyperROqS game (Random inhomogeneities in an Overdetermined quadratic System of equations on a boolean Hypercube).

$\theta_i^{(2)}$ such that

$$\begin{aligned}
R'_i &= F(\gamma_i^{(1)}) + \xi_i^{(1)} \cdot \mathbf{pk} + \sum_{j=1}^{\ell} \rho_{i,j}^{(1)} \cdot R_j + \sum_{j=1}^{\ell} \theta_{i,j}^{(1)} \cdot T_j, \\
T'_i &= F(\gamma_i^{(2)}) + \xi_i^{(2)} \cdot \mathbf{pk} + \sum_{j=1}^{\ell} \rho_{i,j}^{(2)} \cdot R_j + \sum_{j=1}^{\ell} \theta_{i,j}^{(2)} \cdot T_j.
\end{aligned}$$

Furthermore, since the forgeries are valid, it holds that

$$F(s'_i) = c'_i \cdot X + R'_i + (c'_i)^{-1} \cdot T'_i, \quad (44)$$

where $c'_i = H(R'_i, T'_i, m_i)$. The reduction embeds 2ℓ AOMPre challenges into the commitments R_j, T_j , and simulates $\mathbf{Rp}$ -queries using its $\mathbf{Pre}$ oracle as $s_j \leftarrow \mathbf{Pre}(c_j \cdot X + R_j + c_j^{-1} \cdot T_j)$. Then using the definition of s_j , the validity of the forgeries, and the representations of R'_i, T'_i , one can construct the following set of equations:

$$a \cdot X = F(b) + \sum_{k \in K} d_k \cdot R_k + \sum_{j \in [\ell] \setminus K} e_j \cdot T_j, \quad (45)$$

for $a, d_k, e_k \in \mathcal{S}, b \in \mathcal{D}, K \subseteq [\ell]$. Then, the reduction queries the preimages of R_k, T_j for $k \in K$ and $j \in [\ell] \setminus K$. Together with the queries made to $\mathbf{Rp}$, this amounts to a total of 2ℓ queries. Using these preimages, Eq. 45 can be solved for $\log X$ if $a \neq 0$. Given $\log X$, the rest of the commitments R_j, T_k are computed using the correctness of the signing sessions. The probability that $a = 0$ can be reduced to the probability of solving the HyperROqS problem given that (m_i, R'_i, T'_i) are distinct for $i \in [\ell+1]$, i.e., each forgery is verified using a distinct hash function evaluation. If there are two distinct forgeries where (m_i, R'_i, T'_i) coincide, then there is a reduction against the 2ndPre problem. In Thm. 6 we then show that the probability of solving HyperROqS is information-theoretically upper-bounded by $(q_H^2 + 3q_H + 4)/(2(q-1))$. Thus, the security of the scheme comes down to breaking AOMPre for 2ℓ challenges or 2ndPre.

Theorem 5. *Let $\mathbf{LF}$ be a linear function family, which defines the scalar field $\mathcal{S}$ of order q . Let $\mathcal{A}_{\text{alg}}$ be an algebraic adversary against the OMUF of $2\mathbf{BS}[\mathbf{LF}, H]$ running in time τ making at most ℓ signing queries and q_H random oracle*

queries. Then, there exists an adversary $\mathcal{B}$ against the AOMPre problem w.r.t. LF, making at most 2ℓ queries to Pre and $q_H + \ell + 1$ random oracle queries, running in time τ , and an adversary $\mathcal{C}$ against 2ndPre w.r.t LF running in time τ such that

$$\text{Adv}_{2\text{BS}[\text{LF}, \text{H}], \mathcal{A}_{\text{alg}}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{LF}, \mathcal{B}}^{\text{aompre}}(\lambda) + \text{Adv}_{\text{LF}, \mathcal{E}}^{\text{2ndpre}}(\lambda) + \frac{q_H^2 + 3q_H + 4}{2(q-1)}. \quad (46)$$

The following is a straightforward adaptation of [FPS20, Lemma 3] to our setting and is proven analogously. It will simplify the proof of Theorem 5.

Lemma 4. *Let LF be a linear function family and let $\mathcal{A}$ be an adversary against the OMUF of 2BS[LF, H] running in time τ and making at most ℓ queries to Ct. Then there exists an adversary $\mathcal{B}$ that makes exactly ℓ queries to Ct and ℓ queries to Rp, and returns $\ell + 1$ forgeries, running in time at most $\tau + \mathcal{O}(\ell)$, such that*

$$\text{Adv}_{2\text{BS}[\text{LF}, \text{H}], \mathcal{A}}^{\text{omuf}}(\lambda) = \text{Adv}_{2\text{BS}[\text{LF}, \text{H}], \mathcal{B}}^{\text{omuf}}(\lambda).$$

Proof of Thm. 5. Let 2BS[LF, H] be a 2-commitment blind signature using the linear function family LF and the random oracle H. Let $\mathcal{A}_{\text{alg}}$ be an algebraic adversary against the OMUF of 2BS making at most ℓ queries to Ct and q_H random oracle queries to H. W.l.o.g. it follows from Lemma 4 that $\mathcal{A}_{\text{alg}}$ closes all ℓ sessions, and returns $\ell + 1$ forgeries.

Assuming $\mathcal{A}_{\text{alg}}$ succeeds, consider the adversary $\mathcal{B}$ against the AOMPre problem w.r.t. LF, defined in Fig. 7. Adversary $\mathcal{B}$ receives par defining LF, and has access to the challenge and preimage oracles Chal, Pre. It queries $X \leftarrow \text{Chal}()$, and runs $\mathcal{A}_{\text{alg}}$ with par and X as the public key, and simulates the oracles H, Ct, Rp as follows:

- On the j -th Ct query: query $R_j \leftarrow \text{Chal}()$, $T_j \leftarrow \text{Chal}()$, and return (R_j, T_j) .
- $\text{Rp}(j, c_j)$: query $s_j \leftarrow \text{Pre}(c_j X + R_j + c_j^{-1} T_j, (\beta_i)_{i \in [2\ell+1]_0})$, with representation $\beta_1 = c_j, \beta_{2j} = 1, \beta_{2j+1} = c_j^{-1}$, and $\beta_i = 0$ otherwise.

Since $\mathcal{A}_{\text{alg}}$ succeeds, it returns $\ell + 1$ valid forgeries $(m_i, (R'_i, T'_i, s'_i))$ and representations $(\gamma_i^{(1)}, \gamma_i^{(2)}, \xi_i^{(1)}, \xi_i^{(2)}, \rho_i^{(1)}, \theta_i^{(1)}, \rho_i^{(2)}, \theta_i^{(2)})$ satisfying

$$R'_i = F(\gamma_i^{(1)}) + \xi_i^{(1)} X + \sum_{j=1}^{\ell} \rho_{i,j}^{(1)} R_j + \sum_{j=1}^{\ell} \theta_{i,j}^{(1)} T_j, \quad (47)$$

$$T'_i = F(\gamma_i^{(2)}) + \xi_i^{(2)} X + \sum_{j=1}^{\ell} \rho_{i,j}^{(2)} R_j + \sum_{j=1}^{\ell} \theta_{i,j}^{(2)} T_j, \quad (48)$$

for $i \in [\ell + 1]$. The reduction $\mathcal{B}$ queries $c'_i \leftarrow H(R'_i, T'_i, m_i)$ for $i \in [\ell + 1]$. From the validity of the forgeries it follows that

$$F(s'_i) = c'_i X + R'_i + (c'_i)^{-1} T'_i. \quad (49)$$

Furthermore, the same relation is valid for the closed signing session transcripts (R_j, T_j, c_j, s_j) , i.e.,

$$R_j = F(s_j) - c_j X - c_j^{-1} T_j, \quad T_j = c_j(F(s_j) - c_j X - R_j), \quad (50)$$

for $j \in [\ell]$. Substituting R'_i, T'_i in Eq. 49 with Eqs. 47 and 48, respectively, and grouping by $\mathcal{R}$ elements yields

$$\begin{aligned} (\xi_i^{(1)} + c'_i + (c'_i)^{-1} \xi_i^{(2)})X &= \mathbf{F}(-\gamma_i^{(1)} + s'_i - (c'_i)^{-1} \gamma_i^{(2)}) \\ &+ \sum_{j=1}^{\ell} (-\rho_{i,j}^{(1)} - (c'_i)^{-1} \rho_{i,j}^{(2)})R_j + \sum_{j=1}^{\ell} (-\theta_{i,j}^{(1)} - (c'_i)^{-1} \theta_{i,j}^{(2)})T_j. \end{aligned} \quad (51)$$

Substituting every R_k, T_j in Eq. 51 with Eq. 50, respectively, for any index partition $K \subseteq [\ell], \bar{K} := [\ell] \setminus K$, and grouping by $\mathcal{R}$ elements yields

$$\begin{aligned} &(\xi_i^{(1)} - \sum_{j \in \bar{K}} \rho_{i,j}^{(1)} c_j - \sum_{k \in K} \theta_{i,k}^{(1)} c_k^2 + c'_i \\ &+ (c'_i)^{-1} \xi_i^{(2)} - (c'_i)^{-1} \sum_{j \in \bar{K}} \rho_{i,j}^{(2)} c_j - (c'_i)^{-1} \sum_{k \in K} \theta_{i,k}^{(2)} c_k^2)X \\ &= \mathbf{F}\left(-\gamma_i^{(1)} - \sum_{j \in \bar{K}} \rho_{i,j}^{(1)} s_j - \sum_{k \in K} \theta_{i,k}^{(1)} c_k s_k + s'_i \right. \\ &\quad \left. - (c'_i)^{-1} \gamma_i^{(2)} - (c'_i)^{-1} \sum_{j \in \bar{K}} \rho_{i,j}^{(2)} s_j - (c'_i)^{-1} \sum_{k \in K} \theta_{i,k}^{(2)} c_k s_k \right) \\ &\quad + \sum_{k \in K} (-\rho_{i,k}^{(1)} + \theta_{i,k}^{(1)} c_k - (c'_i)^{-1} \rho_{i,k}^{(2)} + (c'_i)^{-1} \theta_{i,k}^{(2)} c_k)R_k \\ &\quad + \sum_{j \in \bar{K}} (\rho_{i,j}^{(1)} c_j^{-1} - \theta_{i,j}^{(1)} + (c'_i)^{-1} \rho_{i,j}^{(2)} c_j^{-1} - (c'_i)^{-1} \theta_{i,j}^{(2)})T_j. \end{aligned}$$

Let Ξ_i^K be the term in front of X and Γ_i^K be the argument of $\mathbf{F}$ for the index set K , and let $P_{i,k}, \Theta_{i,j}$ be the terms in front of R_k, T_j , respectively, i.e.,

$$\Xi_i^K X = \mathbf{F}(\Gamma_i^K) + \sum_{k \in K} P_{i,k} R_k + \sum_{j \in \bar{K}} \Theta_{i,j} T_j.$$

Let B be the (“bad”) event that $\forall K \subseteq [\ell] \forall i \in [\ell+1] : \Xi_i^K = 0$.

Assuming B does not occur, there exist $K \subseteq [\ell]$ and $i \in [\ell+1]$ such that $\Xi_i^K \neq 0$. Then, $\mathcal{B}$ queries

$$r_k \leftarrow \text{Pre}(R_k, (\beta_i)_{i \in [2\ell+1]_0}) \quad \text{and} \quad t_j \leftarrow \text{Pre}(T_j, (\gamma_i)_{i \in [2\ell+1]_0}),$$

for $k \in K, j \in \bar{K}$ (with $\beta_{2k} = \gamma_{2j+1} = 1$, and $\beta_i = \gamma_i = 0$ otherwise). It computes the private key

$$x = (\Xi_i^K)^{-1} (\Gamma_i^K + \sum_{k \in K} P_{i,k} r_k + \sum_{j \in \bar{K}} \Theta_{i,j} t_j),$$

and for $j \in \bar{K}, k \in K$ the commitments (Eq. 50)

$$r_j := s_j - c_j x - c_j^{-1} t_j \quad \text{and} \quad t_k := c_k (s_k - c_k x - r_k).$$

It returns the AOMP solution $(x, r_1, t_1, \dots, r_\ell, t_\ell)$. Note that the number of Dlog-queries is 2ℓ since it is queried for s_j for all $j \in [\ell]$, and for r_k, t_j for $k \in K, j \in \bar{K}$, where $|K| + |\bar{K}| = \ell$. Therefore, $\mathcal{B}$ succeeds except when B occurs, hence

$$\text{Adv}_{2\text{BS}[\text{LF}, \text{H}], \mathcal{A}_{\text{alg}}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{LF}, \mathcal{B}}^{\text{aompre}}(\lambda) + \Pr[B \wedge \text{OMUF}_{2\text{BS}[\text{LF}, \text{H}]}^{\mathcal{A}_{\text{alg}}}(\lambda) = 1]. \quad (52)$$

It remains to consider the case when B occurs. We reduce this event to solving the HyperROqS problem, defined in Fig. 9, as follows: Reduction $\mathcal{H}$ is given the parameters par, ℓ defining LF and the number of equations in HyperROqS, and the random oracle $\text{H}_{\text{hros}} : \mathcal{S}^{4\ell+2} \rightarrow \mathcal{S}^\times$. It samples $x \leftarrow \mathcal{D}$, and sets $X := \text{F}(x)$. Then, $\mathcal{H}$ runs $\mathcal{A}_{\text{alg}}^{\text{H}, \text{Ct}, \text{Rp}}(\text{par}, X)$ simulating its oracle queries as follows.

- Ct and Rp are simulated using $2\text{BS}.\text{Sign}(\text{par}, x)$ with the private key x .
- $\text{H}\left(R_{[\gamma_i^{(1)}, \xi_i^{(1)}, \rho_i^{(1)}, \theta_i^{(1)}]}, T_{[\gamma_i^{(2)}, \xi_i^{(2)}, \rho_i^{(2)}, \theta_i^{(2)}]}, m_i\right)$: check if there exists δ_i, d_i such that $(R, T, m_i, \delta_i, d_i) \in Q$, if so, return $\delta_i d_i$. Else sample $\delta_i \leftarrow \mathcal{S}^\times$ as long as no entry in Q has its last component equal to

$$d_i \leftarrow \text{H}_{\text{hros}}(\delta_i^{-1}(\xi_i^{(1)}, -\rho_i^{(1)}, -\theta_i^{(1)}), \delta_i^{-2}(\xi_i^{(2)}, -\rho_i^{(2)}, -\theta_i^{(2)})).$$

Store $(R, T, m_i, \delta_i, d_i)$ in Q and return $c'_i := \delta_i d_i$.

At last, $\mathcal{A}_{\text{alg}}$ returns the $\ell + 1$ forgeries $(m_i, (R'_i, T'_i, s'_i))$ with representations satisfying Eqs. 47 and 48. Let C be the event that $\exists i \neq j \in [\ell + 1] : (m_i, R'_i, T'_i) = (m_j, R'_j, T'_j)$.

Assuming C does not occur, the values (m_i, R'_i, T'_i) are all distinct for $i \in [\ell + 1]$. The reduction $\mathcal{H}$ makes $\ell + 1$ distinct queries to H for each (m_i, R'_i, T'_i) , and returns

$$\left((\alpha_i := \delta_i^{-1}(\xi_i^{(1)}, -\rho_i^{(1)}, -\theta_i^{(1)}), \beta_i := \delta_i^{-2}(\xi_i^{(2)}, -\rho_i^{(2)}, -\theta_i^{(2)}))_{i \in [\ell + 1]}, \mathbf{c} \right),$$

where c_j is the value that was queried to $\text{Rp}(j, c_j)$, and δ_i is the value chosen in the simulation of H and stored in Q . Note that $(\alpha_i, \beta_i)_{i \in [\ell + 1]}$ are $\ell + 1$ distinct points due to how δ_i was chosen. Whenever B occurs, $\forall K \subseteq [\ell] \forall i \in [\ell + 1] :$

$$\begin{aligned} & \left(\xi_i^{(1)} - \sum_{j \in [\ell] \setminus K} \rho_{i,j}^{(1)} c_j - \sum_{k \in K} \theta_{i,k}^{(1)} c_k^2 \right) + c'_i \\ & + (c'_i)^{-1} \left(\xi_i^{(2)} - \sum_{j \in [\ell] \setminus K} \rho_{i,j}^{(2)} c_j - \sum_{k \in K} \theta_{i,k}^{(2)} c_k^2 \right) = 0, \end{aligned} \quad (53)$$

holds, where $c'_i = \text{H}(R'_i, T'_i, m_i)$. We identify (the complement of) each set $K \subseteq [\ell]$ by the bitvector $\mathbf{b} \in \{0, 1\}^\ell$ on the boolean hypercube, i.e., $b_i = 1$ iff $i \in [\ell] \setminus K$. The sums may be rewritten as scalar products masked by $\mathbf{b}$, e.g., $\sum_{j \in [\ell] \setminus K} \rho_{i,j}^{(1)} c_j = \sum_{j \in [\ell]} \rho_{i,j}^{(1)} b_j c_j = \rho_i^{(1)} \cdot (\mathbf{b} \odot \mathbf{c})$. Thus, Eq. 53 is equivalent to $\forall \mathbf{b} \in \{0, 1\}^\ell \forall i \in [\ell + 1] :$

$$\begin{aligned} & \xi_i^{(1)} - \rho_i^{(1)} \cdot (\mathbf{b} \odot \mathbf{c}) - \theta_i^{(1)} \cdot (-\mathbf{b} \odot \mathbf{c}^2) + c'_i \\ & + (c'_i)^{-1} \left(\xi_i^{(2)} - \rho_i^{(2)} \cdot (\mathbf{b} \odot \mathbf{c}) - \theta_i^{(2)} \cdot (-\mathbf{b} \odot \mathbf{c}^2) \right) = 0. \end{aligned}$$

Defining $\alpha_i := \delta_i^{-1}(\xi_i^{(1)}, -\rho_i^{(1)}, -\theta_i^{(1)})$ (corresponding to the representation of R'_i) and $\beta_i := \delta_i^{-2}(\xi_i^{(2)}, -\rho_i^{(2)}, -\theta_i^{(2)})$ (corresponding to the representation of T'_i), and substituting $c'_i = \delta_i d_i$ yields

$$\delta_i \alpha_i \cdot (1, \mathbf{b} \odot \mathbf{c}, -\mathbf{b} \odot \mathbf{c}^2) + \delta_i d_i + \delta_i d_i^{-1} \beta_i \cdot (1, \mathbf{b} \odot \mathbf{c}, -\mathbf{b} \odot \mathbf{c}^2) = 0.$$

Multiplying by $\delta_i^{-1}d_i$ and rearranging yields

$$d_i^2 + (d_i\alpha_i + \beta_i) \cdot (1, \mathbf{b} \odot \mathbf{c}, -\mathbf{b} \odot \mathbf{c}^2) = 0,$$

where $d_i = H_{\text{hros}}(\alpha_i, \beta_i)$. Given that B holds, $\mathcal{H}$ solves the HyperROqS problem except when C occurs, hence

$$\Pr[B] \leq \text{Adv}_{\text{LF.PGen}, \ell, \mathcal{H}}^{\text{hyperroqs}}(\lambda) + \Pr[C]. \quad (54)$$

It remains to consider the case when C occurs. This can be reduced to solving 2ndPre, defined in Fig. 11. The reduction $\mathcal{C}$ is given as input $\text{par}, x, F(x)$ and runs $\mathcal{A}_{\text{alg}}^{\text{H,Ct,Rp}}(\text{par}, X)$, simulating its oracle queries honestly:

- Ct and Rp are simulated using $2\text{BS}.\text{Sign}(\text{par}, x)$ with the private key x .
- the random oracle is simulated by sampling a random response and recording input-output pairs in a table.

Since $\mathcal{A}_{\text{alg}}$ breaks strong unforgeability $(m_i, R'_i, T'_i, s'_i) \neq (m_j, R'_j, T'_j, s'_j)$ for $i \neq j \in [\ell + 1]$ holds. Therefore when $\mathcal{A}_{\text{alg}}$ succeeds and returns $\ell + 1$ forgeries such that C occurs, then there exist two forgeries (m, R, T, s_1) and (m, R, T, s_2) with $s_1 \neq s_2$. Then by the verification equation we get that $F(s_1) = F(s_2)$ and therefore $s_1 - s_2 \in \ker F$. Therefore $\mathcal{C}$ returns $x + s_1 - s_2$ which is not equal to x as $s_1 \neq s_2$, and since

$$F(x + s_1 - s_2) = F(x) + F(s_1 - s_2) = F(x),$$

$\mathcal{C}$ solves 2ndPre. Therefore,

$$\Pr[C] \leq \text{Adv}_{\text{LF}, \mathcal{C}}^{2\text{ndpre}}(\lambda),$$

and the theorem follows by combining this with Eqs. 52, 54 and Thm. 6. $\square$

Hardness of HyperROqS. The polynomial-time attack by Benhamouda et al. [BLL⁺21] against ROS takes advantage of the fact that one can create 2ℓ equations such that there are 2^ℓ different valid solutions $\mathbf{c}$ for ℓ of those equations. Thus, there is a large enough solution set to solve one more equation. HyperROqS differs in that per “equation” i , there are actually 2^ℓ conditions (represented by different values of $\mathbf{b}$) that must be satisfied. This restricts the set of solutions making it improbable that another equation can be satisfied.

These 2^ℓ equations ensure that each random oracle query falls into one of two cases: either the query already uniquely defines the (relevant part of the) possible solution vector $\mathbf{c}$ before seeing the response to the random oracle query, or there exist two distinct queries that define the same component of a possible solution vector $\mathbf{c}$. In either case the query defines a polynomial before the answer to the random oracle query is known, such that if that query is part of a valid solution, then said answer has to be a root of that polynomial. As the answer is a uniform element, this is unlikely.

Theorem 6. Let $\ell \in \mathbb{N}$, $\mathbb{F}$ be a finite field of order q output by PGen , and $\mathcal{A}$ be an adversary against HyperROqS (Fig. 9) making q_H queries to the random oracle $\mathbf{H}$, then

$$\text{Adv}_{\text{PGen}, \ell, \mathcal{A}}^{\text{hyperroqs}}(\lambda) \leq \frac{q_H^2 + 3q_H + 4}{2(q-1)}. \quad (55)$$

Proof. First consider the case that there exists (α, β) in the output of $\mathcal{A}$ not queried to the random oracle. Since $h := \mathbf{H}(\alpha, \beta)$ is unknown to $\mathcal{A}$ its win condition for $\mathbf{b} = (1, 1, \dots, 1)$ and a solution $\mathbf{c}$ is

$$h^2 + (\alpha_0 h + \beta_0) + \sum_{j \leq \ell} c_j (\alpha_j h + \beta_j) = 0,$$

a monic polynomial of degree 2 evaluated at a random point h . By Schwartz-Zippel $\mathcal{A}$ succeeds with probability at most $2/(q-1)$.

Now consider that the output of $\mathcal{A}$ is a subset of all q_H random oracle queries $\{(\alpha_i, \beta_i) : 1 \leq i \leq q_H\}$. Let $h_i = \mathbf{H}(\alpha_i, \beta_i)$ denote the answer to the i -th oracle query and let

$$\begin{aligned} \gamma_{i,j}(X) &:= X\alpha_{i,j} + \beta_{i,j} && \text{for } 0 \leq j \leq \ell, \\ \hat{\gamma}_{i,j}(X) &:= X\alpha_{i,j+\ell} + \beta_{i,j+\ell} && \text{for } 1 \leq j \leq \ell. \end{aligned}$$

For a vector $\mathbf{b} \in \{0, 1\}^\ell$ consider its “neighboring” vector $\mathbf{b} \oplus \mathbf{e}_j$, differing only in the j -th bit, then the win condition yields

$$\begin{aligned} 0 &= h_i^2 + (h_i \alpha_i + \beta_i) \cdot (1, \mathbf{b} \odot \mathbf{c}, -\mathbf{b} \odot \mathbf{c}^2) \\ &\quad - \left(h_i^2 + (h_i \alpha_i + \beta_i) \cdot (1, (\mathbf{b} \oplus \mathbf{e}_j) \odot \mathbf{c}, \neg(\mathbf{b} \oplus \mathbf{e}_j) \odot \mathbf{c}^2) \right) \\ &= (h_i \alpha_i + \beta_i) \cdot (0, (\mathbf{b} - \mathbf{b} \oplus \mathbf{e}_j) \odot \mathbf{c}, (\neg \mathbf{b} - \neg(\mathbf{b} \oplus \mathbf{e}_j)) \odot \mathbf{c}^2) \\ &= (h_i \alpha_i + \beta_i) \cdot (0, (\mathbf{0}, b_j - \neg b_j, \mathbf{0}) \odot \mathbf{c}, (\mathbf{0}, \neg b_j - b_j, \mathbf{0}) \odot \mathbf{c}^2) \\ &= (h_i \alpha_{i,j} + \beta_{i,j}) \cdot (-1)^{-b_j} c_j + (h_i \alpha_{i,j+\ell} + \beta_{i,j+\ell}) \cdot (-1)^{b_j} c_j^2, \end{aligned}$$

and since $c_j \neq 0$ we get

$$\gamma_{i,j}(h_i) = c_j \hat{\gamma}_{i,j}(h_i). \quad (56)$$

We will show that every random oracle query will fall into one of two classes, which is determined before the query is answered: for $i \leq q_H$ define

$$S_i := \{j \in [\ell] : \alpha_{i,j} \beta_{i,j+\ell} - \beta_{i,j} \alpha_{i,j+\ell} \neq 0\},$$

then for each query this set will either be empty or non-empty. Observe that whenever $j \in S_i$ then $\gamma_{i,j}$ and $\hat{\gamma}_{i,j}$ are linearly independent polynomials for $1 \leq j \leq \ell$, as the determinant of the coefficient matrix of the linear system is non-zero. Moreover, $j \in S_i$ implies $\gamma_{i,j}(h_i) \neq 0 \vee \hat{\gamma}_{i,j}(h_i) \neq 0$ as otherwise $\gamma_{i,j}(h_i) = 0$ and $\alpha_{i,j} = 0$ contradicts $j \in S_i$, and $\alpha_{i,j} \neq 0$ implies

$$-\frac{\beta_{i,j}}{\alpha_{i,j}} \alpha_{i,j+\ell} + \beta_{i,j+\ell} = 0,$$

contradicting $j \in S_i$.

Now if for the i -th query $S_i = \emptyset$ then since $\gamma_{i,j}$ and $\hat{\gamma}_{i,j}$ are linearly dependent define $\lambda_{i,j} \in \mathbb{F}$ such that

$$\gamma_{i,j} = \lambda_{i,j} \hat{\gamma}_{i,j},$$

whenever $\hat{\gamma}_{i,j} \neq 0$, and $\lambda_{i,j} = 0$ otherwise. The polynomial

$$P_i(X) := X^2 + \gamma_{i,0}(X) + \sum_{j=1}^{\ell} \lambda_{i,j} \gamma_{i,j}(X),$$

is defined before the answer h_i to the random oracle query is observed by $\mathcal{A}$.

If on the other hand for the k -th query $S_k \neq \emptyset$ and there exists $i < k$ such that $S_i \cap S_k \neq \emptyset$ then let $j \in S_i \cap S_k$. The polynomial

$$Q_{i,j,k}(X) := \gamma_{i,j}(h_i) \hat{\gamma}_{k,j}(X) - \hat{\gamma}_{i,j}(h_i) \gamma_{k,j}(X),$$

is defined before the answer h_k to the random oracle query is observed by $\mathcal{A}$.

Let $R \subseteq [q_H]$ with $|R| = \ell + 1$ denote the indices of random oracle queries that are used in the solution by $\mathcal{A}$ and consider two cases:

- if there exists $i \in R$ such that $S_i = \emptyset$. By the definition of $\lambda_{i,j}$ and by (56) we have that

$$\begin{aligned} P_i(h_i) &= h_i^2 + \gamma_{i,0}(h_i) + \sum_{j=1}^{\ell} \lambda_{i,j} \gamma_{i,j}(h_i) \\ &= h_i^2 + \gamma_{i,0}(h_i) + \sum_{j=1}^{\ell} c_j \gamma_{i,j}(h_i) = 0, \end{aligned}$$

since $i \in R$ and the win-condition for $\mathbf{b} = (1, 1, \dots, 1)$. By Schwartz-Zippel the probability of this happening is at most $2/(q-1)$.

- if for all $i \in R$ we have $S_i \neq \emptyset$ then since $|S_i| \leq \ell$ and $|R| = \ell + 1$ by the pigeonhole principle there exists $i < k$ with $i, k \in R$ such that $S_i \cap S_k \neq \emptyset$. Let $j = \min S_i \cap S_k$, then $Q_{i,j,k}$ is a non-zero polynomial as $j \in S_i$ implies $\gamma_{i,j}(h_i) \neq 0 \vee \hat{\gamma}_{i,j}(h_i) \neq 0$, and $j \in S_k$ means that $\gamma_{k,j}$ and $\hat{\gamma}_{k,j}$ are linearly independent, hence $Q_{i,j,k}$ is a non-trivial linear combination. Now since for $i, k \in R$ by (56) we have

$$\begin{aligned} Q_{i,j,k}(h_k) &= \gamma_{i,j}(h_i) \hat{\gamma}_{k,j}(h_k) - \hat{\gamma}_{i,j}(h_i) \gamma_{k,j}(h_k) \\ &= c_j \hat{\gamma}_{i,j}(h_i) \hat{\gamma}_{k,j}(h_k) - c_j \hat{\gamma}_{i,j}(h_i) \hat{\gamma}_{k,j}(h_k) = 0, \end{aligned}$$

and by Schwartz-Zippel conditioned on the previously observed transcript this happens with probability at most $1/(q-1)$.

For each query $i \leq q_H$ define the event W_i as

$$W_i := \begin{cases} P_i(h_i) = 0 & S_i = \emptyset, \\ Q_{m,j,i}(h_i) = 0 & \exists m < i : S_m \cap S_i \neq \emptyset \wedge j = \min S_m \cap S_i, \end{cases}$$

and let $W := \bigcup_{i \leq q_H} W_i$. Note that the event W_i is defined before the random oracle query returns h_i . We just showed that whenever $\mathcal{A}$ wins and queries all of its output to the random oracle then W occurs. Then by the union bound we get

$$\Pr[W] \leq \sum_{i \leq q_H} \Pr[W_i] \leq \sum_{i \leq q_H} \frac{2+i-1}{q-1} \leq \frac{2q_H + \binom{q_H}{2}}{q-1}.$$

Let E denote the event that $\mathcal{A}$ queries each of its output to the random oracle, then $\mathcal{A}$'s winning probability is bounded by

$$\begin{aligned} \Pr[\mathcal{A} \text{ wins}] &\leq \Pr[W] + \Pr[\mathcal{A} \text{ wins} \wedge \neg E] \\ &\leq \frac{2q_H + \binom{q_H}{2}}{q-1} + \frac{2}{q-1} \\ &\leq \frac{q_H^2 + 3q_H + 4}{2(q-1)}, \end{aligned}$$

since $\binom{q_H}{2} = (q_H^2 - q_H)/2$. □

4.3 Instantiations

We propose two instantiations of 2-commitment blind signature schemes from linear function families, one based on the hardness of the discrete-logarithm problem, one based on the hardness of the algebraic one-more discrete-logarithm problem.

Hardness assumptions

Algebraic One-More Discrete-Logarithm (AOMDL) problem. The advantage of an adversary $\mathcal{A}$ against the algebraic one-more discrete-logarithm problem w.r.t. the group-generation algorithm GrGen is defined as:

$$\text{Adv}_{\text{GrGen}, \mathcal{A}}^{\text{aomdl}}(\lambda) := \Pr[\text{AOMDL}_{\text{GrGen}}^{\mathcal{A}}(\lambda) = 1], \quad (57)$$

where the game AOMDL is defined in Fig. 10.

Game $\text{AOMDL}_{\text{GrGen}}^{\mathcal{A}}(\lambda)$	Oracle $\text{Chal}()$	Oracle $\text{Dlog}((\alpha_i)_{i \in [c+1]})$
$(\mathbb{G}, p, G) \leftarrow \text{GrGen}(1^\lambda)$	$c := c + 1$	// $X := \alpha_0 G + \sum_{i \in [c]} \alpha_i x_i G$
$c := 0; d := 0;$	$x_i \leftarrow \mathbb{Z}_p$	$d := d + 1$
$(y_1, \dots, y_c) \leftarrow \mathcal{A}^{\text{Chal}, \text{Dlog}}(\mathbb{G}, p, G)$	return $x_i G$	return $\alpha_0 + \sum_{i \in [c]} \alpha_i x_i$
return $d < c \wedge \forall i \in [c] : x_i = y_i$		

Fig. 10. Algebraic One-More Discrete-Logarithm (AOMDL) game [NRS21].

Game $\text{DL}_{\text{GrGen}}^{\mathcal{A}}(\lambda)$ $(\mathbb{G}, p, G) \leftarrow \text{GrGen}(1^\lambda)$ $x \leftarrow \mathbb{Z}_p; X := xG$ $y \leftarrow \mathcal{A}(\mathbb{G}, p, G, X)$ return $x = y$

Fig. 11. Discrete-Logarithm (DL) game.

Discrete-Logarithm (DL) problem. The advantage of an adversary $\mathcal{A}$ against the discrete-logarithm problem w.r.t. the group generation-algorithm GrGen is defined as:

$$\text{Adv}_{\text{GrGen}, \mathcal{A}}^{\text{dlog}}(\lambda) := \Pr[\text{DL}_{\text{GrGen}}^{\mathcal{A}}(\lambda) = 1], \quad (58)$$

where the game DL is defined in Fig. 11.

Schnorr². Let LF be the linear function family where $\text{LF.PGen} := \text{GrGen}$ returns cyclic groups $\mathbb{G}$ of prime order p with generator G . The evaluation function is defined as $F(x) = xG$ mapping inputs from the domain $\mathcal{D} := \mathbb{Z}_p$ to the range $\mathcal{R} := \mathbb{G}$, where both $\mathbb{Z}_p$ and $\mathbb{G}$ form vector spaces over the scalar field $\mathcal{S} := \mathbb{Z}_p$. The properties of vector spaces and homomorphisms can be easily checked, and thus are omitted. The game AOMPre for LF defined above is exactly the AOMDL problem (compare Figs. 7 and 10) as first defined in [NRS21]. As F is bijective, $\text{Adv}_{\text{LF}, \mathcal{A}}^{\text{2ndpre}}(\lambda) = 0$ for all adversaries.

Let $\text{Sch}^2[\text{GrGen}] := 2\text{BS}[\text{LF}]$ be the 2-commitment blind signature scheme instantiated with LF using GrGen (see Fig. 12). It follows from Thm. 5 that for any algebraic adversary $\mathcal{A}_{\text{alg}}$ against the OMUF of $\text{Sch}^2[\text{GrGen}]$, making at most ℓ signing queries and q_H random oracle queries, there exists an adversary $\mathcal{B}$ against the AOMDL problem making 2ℓ queries to the discrete-logarithm oracle and $q_H + \ell + 1$ queries to the random oracle such that

$$\text{Adv}_{\text{Sch}^2[\text{GrGen}], \mathcal{A}_{\text{alg}}}^{\text{omuf}}(\lambda) \leq \text{Adv}_{\text{GrGen}, \mathcal{B}}^{\text{aomdl}}(\lambda) + \frac{q_H^2 + 3q_H + 4}{2(q - 1)}.$$

Furthermore, perfect blindness follows from Thm. 4. The variant where signatures are of the form $(c, R, s) \in \mathbb{Z}_p^\times \times \mathbb{G} \times \mathbb{Z}_p$ has equivalent security (see Sec. 4.2).

Okamoto-Schnorr². We show a reduction from AOMPre to 2ndPre for linear function families with non-injective evaluation functions, which is used to argue OMUF based on the hardness of the discrete-logarithm problem.

$\text{Sch}^2.\text{PGen}(1^\lambda)$	$\text{Sch}^2.\text{KeyGen}(\mathbb{G}, p, G)$	$\text{Sch}^2.\text{Verify}(\text{pk}, m, \sigma)$
$(\mathbb{G}, p, G) \leftarrow \text{GrGen}(1^\lambda)$ $\text{H} : \mathbb{G}^2 \times \{0, 1\}^* \rightarrow \mathbb{Z}_p^\times$ return $(\mathbb{G}, p, G)$	$\text{sk} \leftarrow \mathbb{Z}_p$ $\text{pk} := \text{sk}G$ return sk, pk	$(R', T', s') \leftarrow \sigma$ $c' \leftarrow \text{H}(R', T', m)$ return $s'G = c'\text{pk} + R' + (c')^{-1}T'$
$\text{Sch}^2.\text{Sign}_1((\mathbb{G}, p, G), \text{sk})$	$\text{Sch}^2.\text{User}_1((\mathbb{G}, p, G), \text{pk}, R, T, m)$	
$r, t \leftarrow \mathbb{Z}_p$ $R := rG; T := tG$ $\text{state}_s := (r, t)$ return $\text{state}_s, (R, T)$	$\alpha, \gamma \leftarrow \mathbb{Z}_p; \beta \leftarrow \mathbb{Z}_p^\times$ $R' := \beta R + \alpha G; T' := \beta^2 T + \gamma G$ $c' \leftarrow \text{H}(R', T', m); c := \beta^{-1}c' \bmod p$ $\text{state}_u := (\alpha, \beta, \gamma, R, R', T, T', c, c')$ return state_u, c	
$\text{Sch}^2.\text{Sign}_2((\mathbb{G}, p, G), \text{sk}, \text{state}_s, c)$	$\text{Sch}^2.\text{User}_2((\mathbb{G}, p, G), \text{pk}, \text{state}_u, s)$	
$(r, t) \leftarrow \text{state}_s$ $s := c \cdot \text{sk} + r + c^{-1} \cdot t \bmod p$ return s	$(\alpha, \beta, \gamma, R, R', T, T', c, c') \leftarrow \text{state}_u$ if $sG \neq c \cdot \text{pk} + R + c^{-1} \cdot T$ return $\perp$ $s' := \beta \cdot s + \alpha + (c')^{-1} \cdot \gamma \bmod p$ $\sigma := (R', T', s')$ return σ	

Fig. 12. Blind Schnorr² signature scheme.

Lemma 5. *Let LF be a linear function family where F is not injective. Let $\mathcal{A}$ be an adversary against the AOMP_{Pre} of LF running in time τ . Then there exists an adversary $\mathcal{B}$ against the 2ndPre of LF running in time $\mathcal{O}(\tau)$ such that*

$$\text{Adv}_{\text{LF}, \mathcal{A}}^{\text{aompre}}(\lambda) \leq 2\text{Adv}_{\text{LF}, \mathcal{B}}^{\text{2ndpre}}(\lambda). \quad (59)$$

Proof. Let $\mathcal{A}$ be an adversary against the AOMP_{Pre} of LF running in time τ . Consider the reduction $\mathcal{B}$ against 2ndPre of LF . The reduction $\mathcal{B}$ is given the 2ndPre challenge par, x, X satisfying $\text{F}(x) = X$, runs $\mathcal{A}^{\text{Chal}, \text{Pre}}(\text{par})$, and simulates the oracles Chal, Pre as follows: let $c := 0$,

- On the i -th Chal query sample $x_i \leftarrow \mathcal{D}$ and return $\text{F}(x_i)$. Increment c by 1.
- On $\text{Pre}((\alpha_i)_{i \in [c]_0})$ return $\alpha_0 + \sum_{i \in [c]} \alpha_i x_i$.

Let $K := \ker F$ then $K \neq \{0\}$, as F is not injective. When a successful $\mathcal{A}$ returns $(y_1, \dots, y_c)$ then $\mathcal{B}$ computes $\delta_i := y_i - x_i \in K$. Now if there exists i such that $\delta_i \neq 0$ then $\mathcal{B}$ returns $x + \delta_i$, and aborts if no such i exists. Since $\text{F}(x + \delta_i) = \text{F}(x) + \text{F}(\delta_i) = \text{F}(x)$ this is a valid 2nd preimage.

As the queries to Pre define an underdetermined system of d linear equations in $c > d$ unknowns $x_1, \dots, x_c$, there exists an index i such that x_i is a free variable. As every element in the image of F has at least two pre-images and since Chal selected a uniform preimage x_i of $\text{F}(x_i)$, the probability that $y_i = x_i$ is at most $1/2$.

Hence the probability that there exists i such that $\delta_i \neq 0$ is at least $1/2$ and therefore

$$\begin{aligned} \text{Adv}_{\text{LF}, \mathcal{B}}^{\text{2ndpre}}(\lambda) &= \Pr[\exists i \delta_i \neq 0 \wedge \text{AOMP}_{\text{LF}, \text{PGen}}^{\mathcal{A}}(\lambda) = 1] \\ &= \Pr[\exists i \delta_i \neq 0 \mid \text{AOMP}_{\text{LF}, \text{PGen}}^{\mathcal{A}}(\lambda) = 1] \cdot \Pr[\text{AOMP}_{\text{LF}, \text{PGen}}^{\mathcal{A}}(\lambda) = 1] \\ &\geq \frac{1}{2} \cdot \Pr[\text{AOMP}_{\text{LF}, \text{PGen}}^{\mathcal{A}}(\lambda) = 1] = \frac{1}{2} \text{Adv}_{\text{LF}, \mathcal{A}}^{\text{aompre}}(\lambda), \end{aligned}$$

concluding the proof. $\square$

Let LF be the linear function family where $\text{LF.PGen} := \text{GrGen}$ returns cyclic groups $\mathbb{G}$ of prime order p with generators $G \neq H$, where $\log_G H$ is assumed to be unknown. The evaluation function is defined as

$$\text{F}(x, y) = xG + yH,$$

mapping tuples $(x, y) \in \mathbb{Z}_p^2$ to the group $\mathbb{G}$, where the sets $\mathbb{Z}_p^2$ and $\mathbb{G}$ form vector spaces over $\mathbb{Z}_p$. Observe that F is non-injective since $\text{F}(x + \log_G H, y - 1) = \text{F}(x, y) + \text{F}(\log_G H, -1) = \text{F}(x, y)$. Therefore, Lemma 5 applies reducing AOMP_{LF} to 2ndPre .

Given an adversary $\mathcal{A}$ against the 2ndPre of LF defined as above, the reduction $\mathcal{B}$ to DL is straightforward. The reduction receives the group instance $(\mathbb{G}, p, G)$ and the challenge $H \in \mathbb{G}$ (defining LF). If $G = H$ then $\mathcal{B}$ returns 1, otherwise it samples $x, y \leftarrow \mathbb{Z}_p$, and runs $\mathcal{A}$ on the 2ndPre instance $((x, y), xG + yH)$. When $\mathcal{A}$ returns a solution (x', y') with $(x', y') \neq (x, y)$ and $x'G + y'H = xG + yH$, then $H = (y - y')^{-1}(x' - x)G$, hence $\mathcal{B}$ returns $(y - y')^{-1}(x' - x) \bmod p$ as the discrete logarithm of H . The inverse of $y - y'$ exists because $y = y'$ would imply $xG = x'G$, which contradicts $(x', y') \neq (x, y)$. Thus,

$$\text{Adv}_{\text{LF}, \mathcal{A}}^{\text{2ndpre}}(\lambda) \leq \text{Adv}_{\text{GrGen}, \mathcal{B}}^{\text{dlog}}(\lambda). \quad (60)$$

Let $\text{OkaSch}^2[\text{GrGen}] := 2\text{BS}[\text{LF}]$ be the 2-commitment blind signature scheme instantiated with LF above (see Fig. 13). Then, Thm. 5, Lemma 5, and Eq. 60 imply the existence of an adversary $\mathcal{B}$ against DL such that

$$\text{Adv}_{\text{OkaSch}^2[\text{GrGen}], \mathcal{A}_{\text{alg}}}^{\text{omuf}}(\lambda) \leq 3\text{Adv}_{\text{GrGen}, \mathcal{B}}^{\text{dlog}}(\lambda) + \frac{q_H^2 + 3q_H + 4}{2(q - 1)}. \quad (61)$$

Furthermore, OkaSch^2 is perfectly blind due to Thm. 4. The variant where the signature is of the form $(c, R, s_1, s_2) \in \mathbb{Z}_p^\times \times \mathbb{G} \times \mathbb{Z}_p^2$ has equivalent security (see Sec. 4.2).

Acknowledgments. This work was funded by the Vienna Science and Technology Fund (WWTF) [10.47379/VRG18002] and [10.47379/ICT25-075] and by the Austrian Science Fund (FWF) [10.55776/F8503]. AI was not used for substantive scholarly contributions to this work; its use was limited to minor technical assistance.

OkaSch².PGen (1^λ)	OkaSch².KeyGen ($\mathbb{G}, p, G, H$)
$(\mathbb{G}, p, G) \leftarrow \text{GrGen}(1^\lambda); H \leftarrow \mathbb{G}^\times \setminus \{G\}$ $H : \mathbb{G}^2 \times \{0, 1\}^* \rightarrow \mathbb{Z}_p^\times$ return $(\mathbb{G}, p, G, H)$	$\text{sk}_1, \text{sk}_2 \leftarrow \mathbb{Z}_p; \text{sk} := (\text{sk}_1, \text{sk}_2)$ $\text{pk} := \text{sk}_1 G + \text{sk}_2 H$ return sk, pk
OkaSch².Verify (pk, m, σ)	
$(R', T', s'_1, s'_2) \leftarrow \sigma; c' \leftarrow H(R', T', m)$ return $s'_1 G + s'_2 H = c' \cdot \text{pk} + R' + (c')^{-1} \cdot T'$	
OkaSch².Sign₁ ($(\mathbb{G}, p, G, H), \text{sk}$)	OkaSch².User₁ ($(\mathbb{G}, p, G, H), \text{pk}, R, T, m$)
$r_1, r_2, t_1, t_2 \leftarrow \mathbb{Z}_p$ $R := r_1 G + r_2 H$ $T := t_1 G + t_2 H$ $\text{state}_s := (r_1, r_2, t_1, t_2)$ return $\text{state}_s, (R, T)$	$\alpha_1, \alpha_2, \gamma_1, \gamma_2 \leftarrow \mathbb{Z}_p, \beta \leftarrow \mathbb{Z}_p^\times$ $R' := \beta R + \alpha_1 G + \alpha_2 H$ $T' := \beta^2 T + \gamma_1 G + \gamma_2 H$ $c' \leftarrow H(R', T', m); c := \beta^{-1} c' \bmod p$ $\text{state}_u := (\alpha_1, \alpha_2, \gamma_1, \gamma_2, \beta, R, R', T, T', c, c')$ return state_u, c
OkaSch².Sign₂ ($(\mathbb{G}, p, G, H), \text{sk}, \text{state}_s, c$)	OkaSch².User₂ ($(\mathbb{G}, p, G, H), \text{pk}, \text{state}_u, s$)
$(r_1, r_2, t_1, t_2) \leftarrow \text{state}_s; (\text{sk}_1, \text{sk}_2) \leftarrow \text{sk}$ $s_1 := c \cdot \text{sk}_1 + r_1 + c^{-1} \cdot t_1 \bmod p$ $s_2 := c \cdot \text{sk}_2 + r_2 + c^{-1} \cdot t_2 \bmod p$ $s := (s_1, s_2)$ return s	$(\alpha_1, \alpha_2, \gamma_1, \gamma_2, \beta, R, R', T, T', c, c') \leftarrow \text{state}_u$ $(s_1, s_2) \leftarrow s$ if $s_1 G + s_2 H \neq c \cdot \text{pk} + R + c^{-1} \cdot T$ return $\perp$ $s'_1 := \beta \cdot s_1 + \alpha_1 + (c')^{-1} \cdot \gamma_1 \bmod p$ $s'_2 := \beta \cdot s_2 + \alpha_2 + (c')^{-1} \cdot \gamma_2 \bmod p$ $\sigma := (R', T', s'_1, s'_2)$ return σ

Fig. 13. Blind Okamoto-Schnorr² signature scheme.

References

- Abe01. Masayuki Abe. A secure three-move blind signature scheme for polynomially many signatures. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 136–151. Springer, Berlin, Heidelberg, May 2001.
- App. Apple. iCloud private relay. Available at https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.
- BBSS18. Matilda Backendal, Mihir Bellare, Jessica Sorrell, and Jiahao Sun. The Fiat-Shamir zoo: Relating the security of different signature variants. *Cryptology ePrint Archive*, Report 2018/775, 2018.
- BCKL09. Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. Compact e-cash and simulatable VRFs revisited. In Hovav Shacham and

- Brent Waters, editors, *PAIRING 2009*, volume 5671 of *LNCS*, pages 114–131. Springer, Berlin, Heidelberg, August 2009.
- BFP⁺01. Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. Practical multi-candidate election system. In Ajay D. Kshemkalyani and Nir Shavit, editors, *20th ACM PODC*, pages 274–283. ACM, August 2001.
- BFP21. Balthazar Bauer, Georg Fuchsbaauer, and Antoine Plouviez. The one-more discrete logarithm assumption in the generic group model. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 587–617. Springer, Cham, December 2021.
- BFQ21. Balthazar Bauer, Georg Fuchsbaauer, and Chen Qian. Transferable E-cash: A cleaner model and the first practical instantiation. In Juan Garay, editor, *PKC 2021, Part II*, volume 12711 of *LNCS*, pages 559–590. Springer, Cham, May 2021.
- BHKR25. Nicholas Brandt, Dennis Hofheinz, Michael Klooß, and Michael Reichle. Tightly-secure blind signatures in pairing-free groups. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part VI*, volume 16250 of *LNCS*, pages 337–369. Springer, Singapore, December 2025.
- BL96. Dan Boneh and Richard J. Lipton. Algorithms for black-box fields and their application to cryptography (extended abstract). In Neal Koblitz, editor, *CRYPTO’96*, volume 1109 of *LNCS*, pages 283–297. Springer, Berlin, Heidelberg, August 1996.
- BL13. Foteini Baldimtsi and Anna Lysyanskaya. Anonymous credentials light. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 1087–1098. ACM Press, November 2013.
- BLL⁺21. Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova. On the (in)security of ROS. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 33–53. Springer, Cham, October 2021.
- BNPS03. Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The one-more-RSA-inversion problems and the security of Chaum’s blind signature scheme. *Journal of Cryptology*, 16(3):185–215, June 2003.
- Bol03. Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In Yvo Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 31–46. Springer, Berlin, Heidelberg, January 2003.
- BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.
- Bra94. Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In Douglas R. Stinson, editor, *CRYPTO’93*, volume 773 of *LNCS*, pages 302–318. Springer, Berlin, Heidelberg, August 1994.
- BZ23. Paulo L. Barreto and Gustavo H. M. Zanon. Blind signatures from zero-knowledge arguments. Cryptology ePrint Archive, Report 2023/067, 2023.
- CART26. Rutchathon Chairattana-Apirom, Michael Reichle, and Stefano Tessaro. Playing tag with okamoto-schnorr: Three-move pairing-free blind signatures from DDH. Cryptology ePrint Archive, Paper 2026/571, 2026.
- CATZ24. Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. Pairing-free blind signatures from CDH assumptions. In Leonid Reyzin and

- Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 174–209. Springer, Cham, August 2024.
- CFN90. David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In Shafi Goldwasser, editor, *CRYPTO’88*, volume 403 of *LNCS*, pages 319–327. Springer, New York, August 1990.
- CG08. Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 2008*, pages 345–356. ACM Press, October 2008.
- Cha82. David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *CRYPTO’82*, pages 199–203. Plenum Press, New York, USA, 1982.
- Cha88. David Chaum. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In C. G. Günther, editor, *EUROCRYPT’88*, volume 330 of *LNCS*, pages 177–182. Springer, Berlin, Heidelberg, May 1988.
- Che26. Yanbo Chen. Three-move blind signatures in pairing-free groups. Cryptology ePrint Archive, Paper 2026/593, 2026.
- CKM⁺23. Elizabeth C. Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. Snowblind: A threshold blind signature in pairing-free groups. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part I*, volume 14081 of *LNCS*, pages 710–742. Springer, Cham, August 2023.
- CL01. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93–118. Springer, Berlin, Heidelberg, May 2001.
- CL04. Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer, Berlin, Heidelberg, August 2004.
- CMR⁺23. Lily Chen, Dustin Moody, Andrew Regenscheid, Angela Robinson, and Karen Randall. Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. Technical Report NIST SP 800-186, National Institute of Standards and Technology, Gaithersburg, MD, February 2023.
- CP93. David Chaum and Torben P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *CRYPTO’92*, volume 740 of *LNCS*, pages 89–105. Springer, Berlin, Heidelberg, August 1993.
- DKT26. Marian Dietz, Julia Kastner, and Stefano Tessaro. On the impossibility of round-optimal pairing-free blind signatures in the ROM. *IACR Cryptol. ePrint Arch.*, 2026:90, 2026.
- DMV26. Pierpaolo Della Monica and Ivan Visconti. Improved concurrent-secure blind schnorr signatures. In Nadia Heninger and Mike Rosulek, editors, *Advances in Cryptology – CRYPTO 2026*, pages 457–489, Cham, 2026. Springer Nature Switzerland.
- FHS15. Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 233–253. Springer, Berlin, Heidelberg, August 2015.

- Fis06. Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 60–77. Springer, Berlin, Heidelberg, August 2006.
- FKL18. Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 33–62. Springer, Cham, August 2018.
- FOO93. Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, *AUSCRYPT’92*, volume 718 of *LNCS*, pages 244–251. Springer, Berlin, Heidelberg, December 1993.
- FPS20. Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 63–95. Springer, Cham, May 2020.
- FS87. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO’86*, volume 263 of *LNCS*, pages 186–194. Springer, Berlin, Heidelberg, August 1987.
- FS10. Marc Fischlin and Dominique Schröder. On the impossibility of three-move blind signature schemes. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 197–215. Springer, Berlin, Heidelberg, May / June 2010.
- FW24. Georg Fuchsbauer and Mathias Wolf. Concurrently secure blind Schnorr signatures. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 124–160. Springer, Cham, May 2024.
- GCGF16. Yanmin Gong, Ying Cai, Yuanxiong Guo, and Yuguang Fang. A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid. *IEEE Transactions on Smart Grid*, 7(3):1304–1313, May 2016.
- Goo. Google. VPN by Google One. Available at <https://one.google.com/about/vpn/howitworks>.
- GQ88. Louis C. Guillou and Jean-Jacques Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In C. G. Günther, editor, *EUROCRYPT’88*, volume 330 of *LNCS*, pages 123–128. Springer, Berlin, Heidelberg, May 1988.
- HBG16. Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. Blindly signed contracts: Anonymous on-blockchain and off-blockchain Bitcoin transactions. In Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan S. Wallach, Michael Brenner, and Kurt Rohloff, editors, *FC 2016 Workshops*, volume 9604 of *LNCS*, pages 43–60. Springer, Berlin, Heidelberg, February 2016.
- HKL19. Eduard Hauck, Eike Kiltz, and Julian Loss. A modular treatment of blind signatures from identification schemes. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 345–375. Springer, Cham, May 2019.
- Int. Internet Engineering Task Force. Private access tokens. Available at <https://datatracker.ietf.org/wg/privacypass/documents/>.
- KLR26. Michael Kloof, Russell W. F. Lai, and Michael Reichle. Blind signatures from arguments of inequality. In Nadia Heninger and Mike Rosulek, editors, *Advances in Cryptology – CRYPTO 2026*, pages 426–456, Cham, 2026. Springer Nature Switzerland.

- KLX22. Julia Kastner, Julian Loss, and Jiayu Xu. On pairing-free blind signature schemes in the algebraic group model. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part II*, volume 13178 of *LNCS*, pages 468–497. Springer, Cham, March 2022.
- KNR24. Julia Kastner, Ky Nguyen, and Michael Reichle. Pairing-free blind signatures from standard assumptions in the ROM. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 210–245. Springer, Cham, August 2024.
- KR25. Michael Klooß and Michael Reichle. Blind signatures from proofs of inequality. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part VI*, volume 16005 of *LNCS*, pages 157–189. Springer, Cham, August 2025.
- KRS10. Steve Kremer, Mark Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. In Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou, editors, *ESORICS 2010*, volume 6345 of *LNCS*, pages 389–404. Springer, Berlin, Heidelberg, September 2010.
- KRS23. Shuichi Katsumata, Michael Reichle, and Yusuke Sakai. Practical round-optimal blind signatures in the ROM from standard assumptions. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part II*, volume 14439 of *LNCS*, pages 383–417. Springer, Singapore, December 2023.
- KRW24. Michael Klooß, Michael Reichle, and Benedikt Wagner. Practical blind signatures in pairing-free groups. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part I*, volume 15484 of *LNCS*, pages 363–395. Springer, Singapore, December 2024.
- KTZ26. Julia Kastner, Stefano Tessaro, and Greg Zaverucha. Round-optimal pairing-free blind signatures. *IACR Cryptol. ePrint Arch.*, 2026:91, 2026.
- LHT16. Adam Langley, Mike Hamburg, and Sean Turner. Elliptic Curves for Security. Request for Comments RFC 7748, Internet Engineering Task Force, January 2016.
- Lys23. Anna Lysyanskaya. Security analysis of RSA-BSSA. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 251–280. Springer, Cham, May 2023.
- Lyu09. Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Berlin, Heidelberg, December 2009.
- Mau94. Ueli M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete algorithms. In Yvo Desmedt, editor, *CRYPTO’94*, volume 839 of *LNCS*, pages 271–281. Springer, Berlin, Heidelberg, August 1994.
- Mau05. Ueli M. Maurer. Abstract models of computation in cryptography (invited paper). In Nigel P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12. Springer, Berlin, Heidelberg, December 2005.
- MR07. Ueli M. Maurer and Dominik Raub. Black-box extension fields and the inexistence of field-homomorphic one-way permutations. In Kaoru Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 427–443. Springer, Berlin, Heidelberg, December 2007.
- NRS21. Jonas Nick, Tim Ruffing, and Yannick Seurin. MuSig2: Simple two-round Schnorr multi-signatures. In Tal Malkin and Chris Peikert, editors,

- CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 189–221, Virtual Event, August 2021. Springer, Cham.
- Oka93. Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 31–53. Springer, Berlin, Heidelberg, August 1993.
- Oka98. Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Bruce Christianson, Bruno Crispo, Mark Lomas, and Michael Roe, editors, *Security Protocols*, pages 25–35, Berlin, Heidelberg, 1998. Springer.
- OO92. Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 324–337. Springer, Berlin, Heidelberg, August 1992.
- PCM21. Click fraud prevention and attribution sent to advertiser, 2021. Available at <https://webkit.org/blog/11940/pcm-click-fraud-prevention-and-attribution-sent-to-advertiser/>.
- PST. Private state tokens. Available at <https://developer.chrome.com/docs/privacy-security/private-state-tokens>.
- RCK⁺25. Bruno M. F. Ricardo, Lucas C. Cardoso, Leonardo T. Kimura, Paulo S. Barreto, and Marcos A. Simplicio Jr. Introducing two ROS attack variants: breaking one-more unforgeability of BZ blind signatures. *Cryptology ePrint Archive*, Report 2025/1353, 2025.
- Sch90. Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 239–252. Springer, New York, August 1990.
- Sch91. Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, January 1991.
- Sch01. Claus-Peter Schnorr. Security of blind discrete log signatures against interactive attacks. In Sihon Qing, Tatsuaki Okamoto, and Jianying Zhou, editors, *ICICS 01*, volume 2229 of *LNCS*, pages 1–12. Springer, Berlin, Heidelberg, November 2001.
- SLY⁺22. Yi Sun, Jie Liu, Keping Yu, Mamoun Alazab, and Kaixiang Lin. PMRSS: Privacy-Preserving Medical Record Searching Scheme for Intelligent Diagnosis in IoT Healthcare. *IEEE Transactions on Industrial Informatics*, 18(3):1981–1990, March 2022.
- TZ22. Stefano Tessaro and Chenzhi Zhu. Short pairing-free blind signatures with exponential security. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 782–811. Springer, Cham, May / June 2022.
- VR15. Luke Valenta and Brendan Rowan. Blindcoin: Blinded, accountable mixes for Bitcoin. In Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff, editors, *FC 2015 Workshops*, volume 8976 of *LNCS*, pages 112–126. Springer, Berlin, Heidelberg, January 2015.
- Wag02. David Wagner. A generalized birthday problem. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 288–303. Springer, Berlin, Heidelberg, August 2002.