An extended abstract of this work appears in *SCN'16.* This is the full version.

Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions

Georg Fuchsbauer[1], Christian Hanser[2,†,§], Chethan Kamath[3,‡], and Daniel Slamanig[2,§]

[1] Inria, ENS, CNRS and PSL Research University, Paris, France
georg.fuchsbauer@ens.fr
[2] IAIK, Graz University of Technology, Graz, Austria
{christian.hanser|daniel.slamanig}@iaik.tugraz.at
[3] Institute of Science and Technology Austria, Klosterneuburg, Austria
ckamath@ist.ac.at

Abstract. At Crypto'15 Fuchsbauer, Hanser and Slamanig (FHS) presented the first standard-model construction of efficient round-optimal blind signatures that does not require complexity leveraging. It is conceptually simple and builds on the primitive of structure-preserving signatures on equivalence classes (SPS-EQ). FHS prove the unforgeability of their scheme assuming EUF-CMA security of the SPS-EQ scheme and hardness of a version of the DH inversion problem. Blindness under adversarially chosen keys is proven under an interactive variant of the DDH assumption.

We propose a variant of their scheme whose blindness can be proven under a non-interactive assumption, namely a variant of the bilinear DDH assumption. We moreover prove its unforgeability assuming only unforgeability of the underlying SPS-EQ but no additional assumptions as needed for the FHS scheme.

Keywords: Blind Signatures, Standard Model, SPS-EQ

1 Introduction

Blind signatures allow a user (or obtainer) to obtain a signature from a signer (or issuer) without the latter learning the message that is actually signed. They are an important building block for various privacy and anonymity related applications including e-cash, e-voting, anonymous credentials and ticketing. Since their invention by Chaum [Cha82], research has led to numerous blind signature schemes in various settings and models [Oka93, Abe01, Bol03, CKW05]. The most appealing setting is that of (*i*) *round-optimal* schemes, i.e., schemes that require only two moves (and are thus automatically concurrently secure), that (*ii*) *do not require* any heuristic assumptions (such as random oracles) *nor* (*iii*) a setup assumption, such as common reference strings or honestly generated keys.

Blindness is formalized by a game between a malicious signer and a challenger who asks for two blind signatures on messages of the signer's choice, but in random order. If both signature issuings succeed, the signer is given the resulting signatures and should not be able to tell in which order they were signed. It is natural to let the malicious signer choose its own key pair (rather than having the challenger create it), in which case we speak of the *malicious-key model.*

There are well known efficient round-optimal constructions in the honest-key model with security proofs in the random oracle model [Cha83, Bol03, BNPS03]; and there are various constructions without random oracles and in the malicious-key model, but relying on a trusted

[†] Supported by EU FP7 through project MATTHEW (GA No. 610436).
[‡] Research supported by the European Research Council, ERC starting grant (259668-PSPC) and ERC consolidator grant (682815 - TOCNeT).
[§] Supported by EU Horizon 2020 through project Prismacloud (GA No. 644962).

setup, such as a common reference string (CRS). Among those are constructions using structure-preserving signatures [AFG$^+$10] and Groth-Sahai (GS) proofs [GS08] instantiating the framework of Fischlin [Fis06], as well as other approaches in the bilinear group setting [BFPV11, BPV12b, BPV12a, SC12]. There is also a very recent construction [HK16] without a CRS but relying on non-falsifiable "knowledge" assumptions with security in the honest-key model. Some constructions [CKW05, GS12] require both a CRS and honestly generated keys.

Round-optimal schemes in the plain model. Until now, only very few schemes [GRS$^+$11, GG14, FHS15] were proposed that are round-optimal and require neither random oracles nor setup assumptions, that is, satisfying (i)–(iii). Due to known impossibility results, such constructions are indeed hard to find. Lindell [Lin03] showed that concurrently secure blind signatures are impossible in the standard model when relying on simulation-based security notions. Later, Fischlin and Schröder [FS10] proved that black-box reductions from unforgeability to non-interactive assumptions in the standard model are impossible for blind signature schemes satisfying certain conditions.

Known constructions bypass these impossibility results in several ways: All rely on game-based security definitions [SU12] instead of simulation-based ones. The constructions due to Garg et al. [GRS$^+$11] as well as Garg and Gupta [GG14] make use of complexity leveraging in their proofs and thus do not use black-box reductions. The first scheme [GRS$^+$11] can only be considered a feasibility result and the second [GG14] is still too inefficient for practical applications. In contrast, the most recent construction by Fuchsbauer et al. [FHS15], whose signatures consist of 5 elements from a bilinear group, can be considered practical. It is based on the recent concept of structure-preserving signature schemes on equivalence classes (SPS-EQ) [HS14, FHS14], whose unforgeability is proven in the generic group model, and commitments. A drawback of the scheme is that blindness (in the malicious-key model) is proven under an interactive assumption.

The FHS construction. Before looking at the ideas underlying the FHS construction, let us recall SPS-EQ. Defined over groups equipped with a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, structure-preserving signatures [AFG$^+$10] are schemes whose verification keys, signatures and messages all consist of elements from the base groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and signatures are verified by evaluating the bilinear map on these elements. In SPS-EQ the message space, typically $\mathbb{G}_1^\ell$ for some $\ell > 1$, is partitioned into equivalence classes, where all multiples of a vector belong to one class. These classes should be indistinguishable, that is, it should be hard to tell whether two messages belong to the same class or not (which follows from DDH in $\mathbb{G}_1$).

Given an SPS-EQ signature on a message, anyone can publicly *adapt* the signature to a different representative of the same class. Unforgeability is therefore defined w.r.t. equivalence classes, that is, after being given signatures on messages of its choice, no adversary should be able to compute a signature on a message from a different class. SPS-EQ moreover guarantees that after signing a message, not even the signer is able to distinguish an adaptation of the signature to another representative of the same class from a fresh signature on a completely random message.

The FHS blind-signature scheme [FHS15] works as follows: the obtainer assembles a representative of an equivalence class as a vector containing a commitment to the message and a normalization element (the group generator). She then blinds this message by changing it to another representative and sends it to the signer. The signer signs the representative and sends the signature to the obtainer. Given this signature, the obtainer adapts it to a signature on the original representative. (Due to the normalization element, the obtainer can only switch back to the original representative.) The blind signature is then the rerandomized (unlinkable) signature for the original representative, which contains a commitment to the message, plus an opening of the commitment.

The FHS scheme uses a variant of Pedersen commitments that are perfectly hiding and computationally binding under the co-DHI_1^* assumption (cf. Section 3.1 for a more detailed discussion). The commitment key is part of the signer's public key, which guarantees that the obtainer cannot open commitments to different messages (and thereby break unforgeability). Consequently, unforgeability relies on the co-DHI_1^* assumption in addition to EUF-CMA security of the SPS-EQ scheme. To prove blindness in the malicious-key model (where the reduction has no access to the adversarially generated signing key), FHS argue that during the blindness game the adversary must always produce valid SPS-EQ signatures, as otherwise the challenger does not send any blind signatures in the end, in which case the adversary cannot win the game as all it sees are perfectly hiding commitments.

Intuitively, blindness follows, since under the DDH assumption the randomization of the representative containing the commitment during signature issuing can be replaced by a random representative of a random class. In the latter case, the order in which the messages are signed is perfectly hidden and thus the adversary cannot win. However, since the commitment key is chosen by the adversary, to actually make this replacement, FHS need an interactive assumption. Moreover, this replacement is only indistinguishable to a simulator that does not know the randomization of the representative used. This however means that the simulator cannot later adapt back the signer's SPS-EQ signatures in order to produce the blind signatures. FHS overcome this by relying on SPS-EQ security, which guarantees that adapted signatures look like fresh ones. Thus, if the reduction knew the signing key (which is the case in the honest-key model) then it could simply produce the final blind signatures by itself. In the malicious-key model, the reduction computes the fresh signatures by using the adversary as a signing oracle: it runs the adversary to obtain these signatures and then rewinds it. In the second (and actual) run, it embeds an (interactive) DDH instance and uses the signatures from the first run.

Open questions. As the FHS scheme is the most efficient scheme having all the discussed properties, it would be desirable to base its security (or that of a related scheme) on weaker assumptions. The first question we ask is whether one can relate the unforgeability of a blind signature scheme based on SPS-EQ directly to the EUF-CMA security of the latter without necessitating any further assumptions. Even more interesting would be whether it is possible to remove the requirement for an interactive assumption for blindness. To address the first question, instead of the perfectly hiding commitment, one could use a perfectly binding one, as then each SPS-EQ signature from the signer can only be opened in one way, meaning that SPS-EQ unforgeability would directly imply blind-signature unforgeability. This however means that the commitment key cannot be chosen by the signer anymore, as knowing the underlying randomness could allow the signer to break hiding of the commitment and thus blindness of the scheme. But even if we let the user choose the commitment key, the information-theoretic argument by FHS that a signer must send valid SPS-EQ signatures does not apply anymore: even when not seeing the final blind signatures, the signer still obtains information on which message corresponds to which issuing, as the commitments are only computationally hiding.

Our contribution. We answer the two above questions in the affirmative and reduce the strength of the required assumptions for both security notions. We construct a variant of the FHS blind signature scheme and prove unforgeability solely under the EUF-CMA security of the underlying SPS-EQ scheme. More importantly, we show that our scheme is blind in the malicious-key model under a non-interactive (and non-"q-type") assumption, namely an extension of the bilinear DDH assumption in asymmetric bilinear groups.

Our scheme replaces the perfectly hiding commitments in FHS by perfectly binding ones, which means unforgeability follows directly from SPS-EQ unforgeability. As there are no trusted parameters, we let the user choose the commitment key during signature issuing and include it in the final signature. Straight-forward implementation of this approach however turns out not to result in a blind scheme. We therefore "distribute" the commitment key over several group elements, which enables us to show blindness.

Our blindness proof follows FHS's idea of rewinding the signer in order to use it as a signing oracle for signatures which the simulator cannot adapt on its own. The proof is however much more involved, since we need to consider adversaries that might return invalid SPS-EQ signatures but still break blindness. Our proof works by rewinding the blindness adversary numerous times to increase the success probability of the reduction noticeably beyond one half. We moreover show that these multiple rewinds are *necessary* by giving a counterexample for the case of only rewinding once (see Appendix B.1).

Organization. Section 2 discusses preliminaries including signature schemes on equivalence classes (SPS-EQ). Section 3 discusses blind signatures, the FHS construction and presents our construction of round-optimal blind signatures and the extension to partially blind signatures.

2 Preliminaries

A function $\epsilon\colon \mathbb{N} \to \mathbb{R}^+$ is called negligible if for all $c > 0$ there is a k_0 such that $\epsilon(k) < 1/k^c$ for all $k > k_0$. By $a \xleftarrow{R} S$, we denote that a is chosen uniformly at random from a set S. Furthermore, we write $\mathsf{A}(a_1, \ldots, a_n; r)$ if we want to make the randomness r used by a probabilistic algorithm $\mathsf{A}(a_1, \ldots, a_n)$ explicit and denote by $[\mathsf{A}(a_1, \ldots, a_n)]$ the set of points with positive probability of being output by A. For an (additive) group $\mathbb{G}$ we use $\mathbb{G}^*$ to denote $\mathbb{G} \setminus \{0_{\mathbb{G}}\}$.

Definition 1 (Bilinear map). Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic groups of prime order p, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive and $\mathbb{G}_T$ is multiplicative. Let P and $\hat{P}$ be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, resp. We call $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ a *bilinear map* or *pairing* if it is efficiently computable and it is:

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

If $\mathbb{G}_1 = \mathbb{G}_2$ then e is *symmetric* (Type-1) and *asymmetric* (Type-2 or 3) otherwise. For Type-2 pairings there is an efficiently computable isomorphism $\Psi\colon \mathbb{G}_2 \to \mathbb{G}_1$; for Type-3 pairings no such isomorphism is known. Type-3 pairings are currently the optimal choice in terms of efficiency for a given security level [CM11].

Definition 2 (Bilinear-group generator). A *bilinear-group generator* BGGen is a (possibly probabilistic[4]) polynomial-time algorithm that takes a security parameter 1^κ and outputs a bilinear group description $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$ consisting of groups $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle \hat{P} \rangle$ and $\mathbb{G}_T$ of prime order p with $\log_2 p = \lceil \kappa \rceil$ and an asymmetric pairing $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.

Definition 3 (DDH). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. For $i \in \{1, 2\}$ the *decisional Diffie-Hellman assumption* holds in $\mathbb{G}_i$ for BGGen if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

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

The next assumption is in the spirit of the bilinear Diffie-Hellman assumption (BDDH) [Jou00], which in *symmetric* bilinear groups states that given rP, uP, vP, the element $ruvP$ looks random. In asymmetric groups, we can additionally give uvP, $u\hat{P}$ and $v\hat{P}$. We therefore call the assumption ABDDH$^+$.

[4] For BN-curves [BN06], the most common choice for Type-3 pairings, group generation is deterministic.

Definition 4 (ABDDH$^+$). Let BGGen be a bilinear-group generator that outputs $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1 = P, P_2 = \hat{P})$. The ABDDH$^+$ assumption holds for BGGen if for all PPT algorithms $\mathcal{A}$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l} b \xleftarrow{R} \{0,1\},\ \mathsf{BG} \xleftarrow{R} \mathsf{BGGen}(1^\kappa),\ r,u,v,t \xleftarrow{R} \mathbb{Z}_p \\ b^* \xleftarrow{R} \mathcal{A}\big(\mathsf{BG}, rP, uP, uvP, u\hat{P}, v\hat{P}, ((1-b)\cdot t + b\cdot ruv)P\big) \end{array} : b^* = b\right] - \frac{1}{2} \leq \epsilon(\kappa) \ .$$

In the generic group model, in order to distinguish $ruvP$ from random, one basically needs to construct this element in the target group. It is easily seen that this cannot be done from the remaining elements, which we now make formal:

Proposition 1. *The assumption in Definition 4 holds in generic groups and reaches the optimal, quadratic simulation error bound.*

We prove the above proposition in Appendix C. Moreover, note that given an ABDDH$^+$ instance $(\mathsf{BG}, R, U, W, \hat{U}, \hat{V}, T)$, we could use a DDH oracle to decide it: simply query (BG, R, W, T) to the oracle and return the result. We thus have:

Lemma 1. *If ABDDH$^+$ holds for a bilinear-group generator* BGGen *then DDH in* $\mathbb{G}_1$ *also holds for it.*

2.1 Structure-Preserving Signatures on Equivalence Classes

Structure-preserving signatures (SPS) [Fuc09, AHO10, AFG$^+$10, AGHO11, ACD$^+$12, AGOT14a, AGOT14b, BFF$^+$15, KPW15, Gha16] can handle messages that are elements of a bilinear group, without requiring any prior encoding. In such a scheme public keys, messages and signatures consist only of group elements and the verification algorithm evaluates a signature by deciding group membership of signature elements and by evaluating pairing-product equations (PPEs).

The notion of SPS on equivalence classes (SPS-EQ) was introduced by Hanser and Slamanig [HS14]. Their initial instantiation was only secure against random-message attacks, but together with Fuchsbauer [FHS14] they subsequently presented a scheme that they proved EUF-CMA-secure in the generic group model.

The idea is as follows. For a prime p, $\mathbb{Z}_p^\ell$ is a vector space. Thus, if $\ell > 1$ we can define a projective equivalence relation on it, which propagates to $\mathbb{G}_i^\ell$ and partitions $\mathbb{G}_i^\ell$ into equivalence classes. Let $\sim_\mathcal{R}$ be this relation, i.e., for $M, N \in \mathbb{G}_i^\ell$ we have $M \sim_\mathcal{R} N \Leftrightarrow \exists\, s \in \mathbb{Z}_p^* : M = sN$. An SPS-EQ scheme signs an equivalence class $[M]_\mathcal{R}$ for $M \in (\mathbb{G}_i^*)^\ell$ by actually signing a representative M of $[M]_\mathcal{R}$. It then allows to switch to other representatives of $[M]_\mathcal{R}$ and to update the corresponding signature without having access to the secret key. If the DDH assumption holds on the message space, then a random representative of a given class $[M]_\mathcal{R}$ is indistinguishable from a message vector outside of $[M]_\mathcal{R}$. Moreover, the malicious-key perfect adaptation property (defined in Definition 9) guarantees that updated signatures are random elements in the corresponding space of signatures. The combination of both properties implies the unlinkability of message-signature pairs (under the same pk) corresponding to the same class.

The abstract signature scheme. Here, we discuss the abstract model, the security model of such a signature scheme [HS14, FHS14, FHS15] and a concrete construction, as presented in [FHS14].

Definition 5 (SPS-EQ). A *structure-preserving signature scheme for equivalence relation* $\mathcal{R}$ over $\mathbb{G}_i$ with $i \in \{1,2\}$ is a tuple $\mathsf{SPS\text{-}EQ}$ of the following PPT algorithms:

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

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)$ is a probabilistic algorithm which on input a bilinear group BG and a vector length $\ell > 1$ (in unary) outputs a key pair $(\mathsf{sk}, \mathsf{pk})$.

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

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

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

$\mathsf{VKey}_{\mathcal{R}}(\mathsf{sk}, \mathsf{pk})$ is a deterministic algorithm which given a secret key sk and a public key pk checks their consistency and returns 1 on success and 0 otherwise.

An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ defined on message-space $\mathbb{G}_i$ is *secure* if the DDH assumption holds in $\mathbb{G}_i$, if $\mathsf{SPS\text{-}EQ}$ is *correct*, *EUF-CMA secure* and if it *perfectly adapts signatures*.

Definition 6 (Correctness). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ over $\mathbb{G}_i$ with $i \in \{1, 2\}$ is *correct* if for all security parameters $\kappa \in \mathbb{N}$, for all $\ell > 1$, all bilinear groups $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P}) \in [\mathsf{BGGen}_{\mathcal{R}}(1^\kappa)]$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^\ell)]$, all messages $M \in (\mathbb{G}_i^*)^\ell$ and all scalars $\mu \in \mathbb{Z}_p^*$ we have:

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

In contrast to the standard unforgeability definition for signatures, EUF-CMA security for SPS-EQ is defined with respect to equivalence classes, i.e., a forgery is a signature on a message from an equivalence class from which the adversary has not asked any messages to be signed.

Definition 7 (EUF-CMA). An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ over $\mathbb{G}_i$ with $i \in \{1, 2\}$ is *existentially unforgeable under adaptive chosen-message attacks* if for all $\ell > 1$ and all PPT algorithms $\mathcal{A}$ having access to a signing oracle $\mathsf{Sign}_{\mathcal{R}}(\cdot, \mathsf{sk})$, there is a negligible function $\epsilon(\cdot)$ such that:

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

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

The next two definitions were introduced in [FHS15]. They formalize the notion that signatures output by $\mathsf{ChgRep}_{\mathcal{R}}$ are distributed like fresh signatures on the new representative.

Definition 8 (Signature adaptation). Let $\ell > 1$. An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ on $(\mathbb{G}_i^*)^\ell$ with $i \in \{1, 2\}$ *perfectly adapts signatures* if for all tuples $(\mathsf{sk}, \mathsf{pk}, M, \sigma, \mu)$ with

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

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

The following definition demands that this even holds for maliciously generated verification keys. As for such keys there might not even exist a corresponding secret key, we require that adapted signatures are random elements in the space of valid signatures.

Definition 9 (Signature adaptation under malicious keys). Let $\ell > 1$. An SPS-EQ scheme $\mathsf{SPS\text{-}EQ}$ on $(\mathbb{G}_i^*)^\ell$ with $i \in \{1, 2\}$ *perfectly adapts signatures under malicious keys* if for all tuples $(\mathsf{pk}, M, \sigma, \mu)$ with

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

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

In Figure 1, we restate the SPS-EQ construction from [FHS14]. It is EUF-CMA secure in the generic group model and satisfies Definitions 8 and 9.

$\underline{\mathsf{BGGen}_\mathcal{R}}(1^\kappa)$: On input a security parameter 1^κ, output $\mathsf{BG} \overset{R}{\leftarrow} \mathsf{BGGen}(1^\kappa)$.

$\underline{\mathsf{KeyGen}_\mathcal{R}}(\mathsf{BG}, 1^\ell)$: On input a bilinear-group description BG and vector length $\ell > 1$ (in unary), choose $(x_i)_{i\in[\ell]} \overset{R}{\leftarrow} (\mathbb{Z}_p^*)^\ell$, set secret key $\mathsf{sk} \leftarrow (x_i)_{i\in[\ell]}$, compute public key $\mathsf{pk} \leftarrow (\hat{X}_i)_{i\in[\ell]} = (x_i\hat{P})_{i\in[\ell]}$ and output $(\mathsf{sk}, \mathsf{pk})$.

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

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

$\underline{\mathsf{Verify}_\mathcal{R}}(M, \sigma, \mathsf{pk})$: On input a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of equivalence class $[M]_\mathcal{R}$, a signature $\sigma = (Z, Y, \hat{Y}) \in \mathbb{G}_1 \times \mathbb{G}_1^* \times \mathbb{G}_2^*$ and public key $\mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} \in (\mathbb{G}_2^*)^\ell$, check whether

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

and if this holds output 1 and 0 otherwise.

$\underline{\mathsf{ChgRep}_\mathcal{R}}(M, \sigma, \mu, \mathsf{pk})$: On input a representative $M = (M_i)_{i\in[\ell]} \in (\mathbb{G}_1^*)^\ell$ of equivalence class $[M]_\mathcal{R}$, a signature $\sigma = (Z, Y, \hat{Y})$, $\mu \in \mathbb{Z}_p^*$ and public key pk, return $\perp$ if $\mathsf{Verify}_\mathcal{R}(M, \sigma, \mathsf{pk}) = 0$. Otherwise pick $\psi \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and return $(\mu \cdot M, \sigma')$ with $\sigma' \leftarrow (\psi\mu Z, \frac{1}{\psi}Y, \frac{1}{\psi}\hat{Y})$.

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

Fig. 1: Scheme 1, an EUF-CMA secure SPS-EQ scheme

3 Blind Signatures

Before we discuss the construction from [FHS15] and then present our new blind signature construction, we give the abstract model and the security properties of blind signature schemes. These are correctness, unforgeability and blindness and were initially studied in [PS00, JLO97] and later on rigorously treated in [FS09, SU12].

Definition 10 (Blind signature scheme). A blind signature scheme BS consists of the following PPT algorithms:

$\mathsf{KeyGen}_\mathsf{BS}(1^\kappa)$, on input κ, returns a key pair $(\mathsf{sk}, \mathsf{pk})$. The security parameter κ is also an (implicit) input to the following algorithms.

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

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

A blind signature scheme BS is *secure* if it is *correct*, *unforgeable* and *blind.*

Definition 11 (Correctness). A blind signature scheme BS is *correct* if for all security parameters $\kappa \in \mathbb{N}$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KeyGen}_{\mathsf{BS}}(1^\kappa)]$, all messages m and all signatures $\sigma \in [(\mathcal{U}_{\mathsf{BS}}(m, \mathsf{pk}), \mathcal{S}_{\mathsf{BS}}(\mathsf{sk}))]$ it holds that $\mathsf{Verify}_{\mathsf{BS}}(m, \sigma, \mathsf{pk}) = 1$.

Definition 12 (Unforgeability). BS is *unforgeable* if for all PPT algorithms $\mathcal{A}$ having access to a signer oracle, there is a negligible function $\epsilon(\cdot)$ such that:

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

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

There are several different kinds of blindness, where the strongest (and arguably most natural) definition is blindness in the *malicious-key* model [ANN06, Oka06]. In this case, the public key is generated by the adversary, whereas in the weaker *honest-key* model the key pair is initially set up by the environment, i.e., it requires a trusted setup. We use the stronger notion to prove the blindness of our construction—as also done by other existing round-optimal standard-model constructions [GRS$^+$11, GG14, FHS15]:

Definition 13 (Blindness). A blind signature scheme BS is called *blind* in the malicious-key model if for all PPT algorithms $\mathcal{A}$ having one-time access to two user oracles, there is a negligible function $\epsilon(\cdot)$ such that:

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

3.1 The FHS Construction

The construction in [FHS15] uses unconditionally hiding commitments to the messages and SPS-EQ to sign these commitments. The latter allows for blinding and unblinding, as it implies the ability to derive a signature for arbitrary representatives of this class (without knowing the private signing key). The construction is unforgeable under the EUF-CMA security of the SPS-EQ and an asymmetric-group variant of the Diffie-Hellman inversion assumption. It is blind under an interactive DDH variant in the malicious-key model without requiring any trusted setup. Its design principle is as follows.

A signer public key consists of an SPS-EQ verification key pk and two elements $(Q = qP, \hat{Q} = q\hat{P})$ for some random $q \in \mathbb{Z}_p^*$. When asking for a signature on a message m, the user picks $r \xleftarrow{R} \mathbb{Z}_p^*$ and creates a Pedersen commitment $C = mP + rQ$ and forms a vector (C, P), which is a representative of equivalence class $[(C, P)]_{\mathcal{R}}$. Then she chooses a randomizer $s \xleftarrow{R} \mathbb{Z}_p^*$ and uses it to randomize (C, P) to another representative (sC, sP), thereby blinding the vector, and sends (sC, sP) to the signer. When the signer returns an SPS-EQ signature on (sC, sP), the user is able to derive a signature for the unblinded (original) message (C, P), using SPS-EQ's changing of representatives. Verification of the blind signature will only accept messages whose second component is P. Together with SPS-EQ unforgeability, this means that the only such message for which the user can derive a signature is (C, P).

The Pedersen commitment $C = mP + rQ$ has a tweaked opening, which is (m, rP) instead of (m, r), and which lets one check the well-formedness of C via the pairing equation $e(C - mP, \hat{P}) = e(rP, \hat{Q})$. This can be thought of as showing knowledge of the discrete logarithm r without revealing it (revealing r would lead to attacks against blindness). Under the co-DHI$_1^*$ assumption commitments with opening of this form are binding, meaning the user can open a commitment only to one message, which is required for blind-signature unforgeability. The user includes the values $T \leftarrow C - mP$ and $R \leftarrow rP$ in the blind signature to allow the verification of the opening.

Blindness intuitively follows from the fact that the message $(sC, sP) = (smP + srQ, sP)$ that the signer sees during issuing looks unrelated to the message m and the resulting blind signature (which contains rP): under DDH, given sP and rP, the element srP looks random. However, the blinding factor in the randomized commitment is not srP but srQ, with Q chosen by the signer. This is what forced FHS to introduce an interactive variant of DDH, where the adversary chooses Q and $\hat{Q}$ and then gets an instance rP, rQ, sP, tQ and needs to decide whether $t = rs$.

3.2 Construction

In previous round-optimal blind-signature schemes (using a related approach involving commitments) the commitment is done w.r.t. a commitment key contained in the CRS. Since we aim at constructing a scheme in the standard model where there is no CRS, we could add the commitment key to the signer's public key—as done in [FHS15]. In this case the commitment must be perfectly hiding and can thus only be computationally binding. (Binding protects the signer from a user generating signatures on more messages than signatures issued by the signer.) We choose a different approach, namely to let the user choose the commitment key. To prevent forgeries, the commitment now needs to be perfectly binding, which we achieve by using an encryption scheme. We then show that, together with the properties of the used SPS-EQ scheme, computational hiding of the commitment implies blindness of our construction.

In our signing protocol the user chooses a public key Q for ElGamal encryption and then commits to the message m by encrypting mP as $(C, R) = (mP + rQ, rP)$. The user then forms a vector (C, R, Q, P), consisting of the ciphertext, the public key and the group generator P. (Note that this vector uniquely defines m.) Next, to blind the message, the user transforms this tuple to a random element of the equivalence class $[(C, R, Q, P)]_{\mathcal{R}}$: she picks $s \overset{R}{\leftarrow} \mathbb{Z}_p^*$, computes $M \leftarrow (sC, sR, sQ, sP)$, and sends M to the signer. When the signer returns an SPS-EQ signature on (sC, sR, sQ, sP), the user derives a signature for the unblinded (original) message (C, R, Q, P). For unforgeability, this unblinding must be unambiguous, which is why verification only accepts tuples whose last component is P.

Finally, the user needs to "open" $(C, R, Q = qP)$ to the actual message m. This could be done by publishing $Z = rQ$ and $\hat{Q} = q\hat{P}$: then for a message m we could check whether the signature is valid on $(mP + Z, R, Q, P)$ and whether Z is of the correct form, by checking $e(Q, \hat{P}) = e(P, \hat{Q})$ and

$$e(Z, \hat{P}) = e(R, \hat{Q}) \ . \qquad (2)$$

This is basically the opening that FHS use (where $\hat{Q}$ is part of the commitment key). In their scheme R is only given in the final signature; here however, the signer also sees sR, which leads to the following attack: The signer can check whether $M = (sC, sR, sQ, sP)$ received during the signing protocol corresponds to a particular m, by testing $e(M_1 - mM_4, \hat{P}) = e(M_2, \hat{Q})$, since this corresponds to the pairing equation $e(srQ, \hat{P}) = e(srP, \hat{Q})$.

To prevent this attack, we "split" the logarithm of Q and define $Q = uvP$. Instead of publishing $\hat{Q}$, we publish $X = ruP$ and $\hat{V} = v\hat{P}$ and replace the RHS of (2) with $e(X, \hat{V}) = e(r \cdot uvP, \hat{P})$. Now we additionally need to enable a check that X and $\hat{V}$ are correctly formed, which we do by publishing $U = uP$ and $\hat{U} = u\hat{P}$. As in [FHS14, FHS15], we assume the bilinear group generation algorithm of the SPS-EQ scheme to be deterministic and to produce one bilinear group per security parameter. We then show that assuming ABDDH$^+$ for such a group generation algorithm, our scheme satisfies malicious-key blindness. Our blind-signature scheme is detailed in Figure 2.

$\underline{\mathsf{KeyGen}_{\mathsf{BS}}}(1^\kappa)$: Given a security parameter $\kappa > 0$ (in unary), compute $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$; compute $(\mathsf{sk}, \mathsf{pk}) \overset{R}{\leftarrow} \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, 1^4)$ and output $(\mathsf{sk}, \mathsf{pk})$.

$\underline{\mathcal{U}^{(1)}_{\mathsf{BS}}}(m, \mathsf{pk})$: Given pk and a message $m \in \mathbb{Z}_p$, compute $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$; choose $r, s, u, v \overset{R}{\leftarrow} \mathbb{Z}_p^*$ s.t. $m + ruv \neq 0$ and output

$$M \leftarrow (s(mP + ruvP), srP, suvP, sP) \qquad \mathsf{st} \leftarrow (\mathsf{pk}, M, r, s, u, v)$$

$\underline{\mathcal{S}_{\mathsf{BS}}}(M, \mathsf{sk})$: Given $M \in (\mathbb{G}_1^*)^4$ and a secret key sk, output $\pi \overset{R}{\leftarrow} \mathsf{Sign}_{\mathcal{R}}(M, \mathsf{sk})$.

$\underline{\mathcal{U}^{(2)}_{\mathsf{BS}}}(\mathsf{st}, \pi)$: Parse st as $(\mathsf{pk}, M, r, s, u, v)$. If $\mathsf{Verify}_{\mathcal{R}}(M, \pi, \mathsf{pk}) = 0$ then return $\perp$. Else run $((mP + ruvP, rP, uvP, P), \sigma) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M, \pi, \frac{1}{s}, \mathsf{pk})$; output $\tau \leftarrow (\sigma, Y = ruvP, Q = uvP, R = rP, U = uP, X = ruP, \hat{U} = u\hat{P}, \hat{V} = v\hat{P})$.

$\underline{\mathsf{Verify}_{\mathsf{BS}}}(m, \tau, \mathsf{pk})$: Given message $m \in \mathbb{Z}_p$, blind signature $\tau = (\sigma, Y, Q, R, U, X, \hat{U}, \hat{V})$ and public key pk, output 1 if the following holds and 0 otherwise.

$$\mathsf{Verify}_{\mathcal{R}}((mP + Y, R, Q, P), \sigma, \mathsf{pk}) = 1 \qquad e(Q, \hat{P}) = e(U, \hat{V}) \tag{3}$$

$$e(U, \hat{P}) = e(P, \hat{U}) \qquad e(X, \hat{P}) = e(R, \hat{U}) \qquad e(Y, \hat{P}) = e(X, \hat{V}) \tag{4}$$

Fig. 2: A Blind Signature Scheme from SPS-EQ.

3.3 Security

The correctness of the scheme in Figure 2 follows by inspection.

Theorem 1. *If the underlying SPS-EQ scheme is EUF-CMA secure, then the scheme in Figure 2 is unforgeable.*

Unforgeability of the SPS-EQ scheme guarantees that after k signing queries the adversary possesses only signatures on k tuples of the form (C_i, R_i, Q_i, P). (Since the last component fixes each equivalence class to one representative.) It remains to show that each such tuple can only be opened to one message m: let (C, R, Q, P) and σ be such a valid message-signature pair. Then we show that any choice of $(Y, U, X, \hat{U}, \hat{V})$ that satisfies verification together with (σ, Q, R) leads to the same m. Let u, v be such that $\hat{U} = u\hat{P}$ and $\hat{V} = v\hat{P}$. Then by (3.2), the 2nd equation in (3): $Q = uvP$; and (4.1) implies $U = uP$. With r s.t. $R = rP$, we have $X = ruP$ by (4.2) and $Y = ruv = rQ$ by (4.3). This means that R and Q uniquely determine Y, which together with $C = mP + Y$ uniquely determines m.

The formal proof is given in Appendix A. The reduction has a natural security loss determined by the number of signing queries by the adversary, since the reduction has to guess which of the $k + 1$ valid signatures is the forgery.

Blindness. In Lemma 2 in Appendix B, we first show that ABDDH$^+$ (Def. 4) implies that when given $rQ, Q, R, U, X, \hat{U}, \hat{V}$ (the elements which the signer sees in the final signature), the elements srQ (the blinding factor of the message in the issuing protocol), and sQ, srP and sP (the remaining components seen during issuing) are indistinguishable from random. This intuitively means that what the adversary sees during issuing looks unrelated to the derived blind signature.

We start with the basic idea to prove blindness. Given an instance of the decision problem just described $(\mathsf{BG}, R, S = sP, U = uP, X = uR, Q = uvP, Y = rQ, \hat{U} = u\hat{P}, \hat{V} = v\hat{P}, T, W, Z)$, where either (a) $T = sR$, $W = sQ$ and $Z = sY$ or (b) T, W and Z are random, in the blindness game the challenger could compute the message sent to the signer during issuing as

$$M \leftarrow (m \cdot S + Z, T, W, S) \ , \tag{5}$$

which is correctly distributed in case (a) but independent of m (and the resulting blind signature) in case (b). In the blindness game, the challenger next receives an SPS-EQ signature on M, which it needs to adapt to the unblinded message in order to construct a blind signature.

Overall, we distinguish two behaviors of blindness adversaries. Type I does not return correct SPS-EQ signatures during issuing. As in this case the adversary does not obtain blind signatures at the end, the above simulation already works and we are done.

However, if the adversary returns valid signatures (Type II) then the simulator, after embedding the instance when creating M as in (5), does not know the blinding factor s, meaning the simulator cannot adapt the SPS-EQ signature to the unblinded message. By perfect adaptation however, the distribution of an adapted signature is the same as that of a fresh signature on the unblinded message. In the honest-key model, where the simulator knows the signing key, it could therefore compute a signature σ on $(m \cdot P + Z, R, Q, P)$ and return the blind signature $(\sigma, Y, Q, R, U, X, \hat{U}, \hat{V})$. Blindness follows, since during issuing the signer obtained a random quadruple; thus the game is independent of bit b.

For blindness in the malicious-key model, we do not have access to the adversarially generated signing key, meaning we cannot recompute the signature on the unblinded message. Instead, we use the adversary $\mathcal{A}$ as a signing oracle by rewinding it. (This is similar to Coron's [Cor02] meta-reduction strategy, which was extended to randomizable signatures by Hofheinz et al. [HJK12].) The idea is to first run the adversary to obtain a signature on $(s'(mP + Y), s'R, s'Q, s'P)$ for a known s', which we can therefore transform into a signature on $(mP + Y, R, Q, P)$. We then rewind the adversary to the point after it output the public key and the messages, and then run it again (using a new random bit b), this time setting M as in (5), thus not knowing s. In the second run we are not able to transform the signature, but we can use the signature from the first run, which is distributed identically, thanks to the property of the SPS-EQ scheme.

Making this approach actually work turns out quite tricky. In the proof in [FHS15] it is argued that an adversary must always output two valid signatures, as otherwise the bit b is perfectly hidden due to the perfectly hiding commitments. For such adversaries if the original blindness game is won with some probability then the game that rewinds the adversary will yield valid signatures in the first run and in the second run the adversary wins with the same probability as in the original (non-rewinding) game.

This is not true anymore for our scheme, as an aborting adversary (one that returns invalid SPS-EQ signatures) can still win the game. In particular, we show that *rewinding once is not enough*: in Appendix B.1, we give an example of an adversary's coin distribution (before and after the point of rewinding) that leads to the original blindness game being won with non-negligible probability, while the game with rewinding (which outputs a random bit if it receives invalid signatures in the first run) is won with probability *less than one half.*

However, if we rewind more than once then it suffices to obtain valid signatures *in at least one* of the rewinds. We therefore consider a game where we rewind the adversary λ times and abort if all runs yield invalid signatures (outputting a random bit); otherwise, we run the adversary a final time and check if it wins or not.

In Claim 3 in Appendix B we show the following: suppose the adversary wins the blindness game with non-negligible advantage, that is, for some polynomial p and infinitely many security-parameter values κ, the probability of winning the blindness game is greater than $\frac{1}{2} + \frac{1}{p(\kappa)}$. Then if we rewind the adversary $\lambda = \kappa \cdot p(\kappa)$ times, the probability that at least one of the λ runs yields valid SPS-EQ signatures *and* the adversary wins the final run is greater than $\frac{1}{2} + \frac{1}{2 \cdot p(\kappa)}$ for infinitely many κ's. We make this formal in the following theorem, which is proved in Appendix B.

Theorem 2. *If the underlying SPS-EQ scheme has perfect adaptation of signatures under malicious keys and ABDDH$^+$ holds for* BGGen *then the scheme in Figure 2 satisfies blindness in the malicious-key model.*

Efficiency of the construction. When instantiating our blind signature construction with the SPS-EQ scheme from [FHS14], we obtain a public key size of $4\,\mathbb{G}_2$, a communication complexity of $6\,\mathbb{G}_1 + 1\,\mathbb{G}_2$ and a signature size of $7\,\mathbb{G}_1 + 3\,\mathbb{G}_2$ elements. We will now contrast this to the FHS construction [FHS15] and to the DLIN construction from [GG14].

Instantiating the FHS construction with the SPS-EQ scheme from [FHS14] yields a blind signature scheme having a public key size of $1\,\mathbb{G}_1{+}3\,\mathbb{G}_2$, a communication complexity of $4\,\mathbb{G}_1{+}1\,\mathbb{G}_2$ and a signature size of $4\,\mathbb{G}_1 + 1\,\mathbb{G}_2$ elements. While being more efficient, we recall that blindness of the FHS construction is based on an interactive and, thus, much stronger assumption.

Ignoring the increase of the security parameter due to complexity leveraging for the construction from [GG14], it has a public key size of $43\,\mathbb{G}_1$ elements, a communication complexity of $18\log_2 q\ +\ 41\,\mathbb{G}_1$ elements (where, for instance, we have $\log_2 q = 155$ when assuming that the adversary runs in at most 2^{80} steps) and a signature size of $183\,\mathbb{G}_1$ elements.

Extension to partially blind signatures. We note that analogously to the extension of the round-optimal blind signature construction in [FHS15], it is possible to derive a partially blind signature scheme from the scheme in Figure 2. To include a common information $\gamma \in \mathbb{Z}_p^*$, the underlying SPS-EQ scheme is set up for $\ell = 5$ (instead of $\ell = 4$) and the additional vector component is being used to include γ. In contrast to the blind signature scheme in Figure 2, the signer on receiving $M \leftarrow (s(mP + ruvP), srP, suvP, sP)$ computes an SPS-EQ signature for vector $(s(mP + ruvP), srP, suvP, \gamma(sP), sP)$. In the verification of the partially blind signature, the SPS-EQ signature is verified on $(mP + Y, R, Q, \gamma P, P)$.

References

Abe01. Masayuki Abe. A secure three-move blind signature scheme for polynomially many signatures. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 136–151. Springer, Heidelberg, May 2001.

ACD$^+$12. Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24. Springer, Heidelberg, December 2012.

AFG$^+$10. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236. Springer, Heidelberg, August 2010.

AGHO11. Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666. Springer, Heidelberg, August 2011.

AGOT14a. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Structure-preserving signatures from type II pairings. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 390–407. Springer, Heidelberg, August 2014.

AGOT14b. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 688–712. Springer, Heidelberg, February 2014.

AHO10. Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. http://eprint.iacr.org/2010/133.

ANN06. Michel Abdalla, Chanathip Namprempre, and Gregory Neven. On the (im)possibility of blind message authentication codes. In David Pointcheval, editor, *Topics in Cryptology – CT-RSA 2006*, volume 3860 of *Lecture Notes in Computer Science*, pages 262–279. Springer, Heidelberg, February 2006.

BFF$^+$15. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In Jonathan Katz, editor, *PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography*, volume 9020 of *Lecture Notes in Computer Science*, pages 355–376. Springer, Heidelberg, March / April 2015.

BFPV11. Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011: 14th International Conference on Theory and Practice of Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 403–422. Springer, Heidelberg, March 2011.

BN06. Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005: 12th Annual International Workshop on Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, Heidelberg, August 2006.

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: 6th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer, Heidelberg, January 2003.

BPV12a. Olivier Blazy, David Pointcheval, and Damien Vergnaud. Compact round-optimal partially-blind signatures. In Ivan Visconti and Roberto De Prisco, editors, *SCN 12: 8th International Conference on Security in Communication Networks*, volume 7485 of *Lecture Notes in Computer Science*, pages 95–112. Springer, Heidelberg, September 2012.

BPV12b. Olivier Blazy, David Pointcheval, and Damien Vergnaud. Round-optimal privacy-preserving protocols with smooth projective hash functions. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 94–111. Springer, Heidelberg, March 2012.

Cha82. David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – CRYPTO'82*, pages 199–203. Plenum Press, New York, USA, 1982.

Cha83. David Chaum. Blind signature system. In David Chaum, editor, *Advances in Cryptology – CRYPTO'83*, page 153. Plenum Press, New York, USA, 1983.

CKW05. Jan Camenisch, Maciej Koprowski, and Bogdan Warinschi. Efficient blind signatures without random oracles. In Carlo Blundo and Stelvio Cimato, editors, *SCN 04: 4th International Conference on Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 134–148. Springer, Heidelberg, September 2005.

CM11. Sanjit Chatterjee and Alfred Menezes. On cryptographic protocols employing asymmetric pairings - the role of ψ revisited. *Discrete Applied Mathematics*, 159(13):1311–1322, 2011.

Cor02. Jean-Sébastien Coron. Optimal security proofs for PSS and other signature schemes. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 272–287. Springer, Heidelberg, April / May 2002.

FHS14. Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. Cryptology ePrint Archive, Report 2014/944, 2014. http://eprint.iacr.org/2014/944.

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, *Advances in Cryptology*

– *CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 233–253. Springer, Heidelberg, August 2015.

Fis06. Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 60–77. Springer, Heidelberg, August 2006.

FS09. Marc Fischlin and Dominique Schröder. Security of blind signatures under aborts. In Stanislaw Jarecki and Gene Tsudik, editors, *PKC 2009: 12th International Conference on Theory and Practice of Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 297–316. Springer, Heidelberg, March 2009.

FS10. Marc Fischlin and Dominique Schröder. On the impossibility of three-move blind signature schemes. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 197–215. Springer, Heidelberg, May 2010.

Fuc09. Georg Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009. http://eprint.iacr.org/2009/320.

GG14. Sanjam Garg and Divya Gupta. Efficient round optimal blind signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 477–495. Springer, Heidelberg, May 2014.

Gha16. Essam Ghadafi. Short structure-preserving signatures. In Kazue Sako, editor, *Topics in Cryptology – CT-RSA 2016*, volume 9610 of *Lecture Notes in Computer Science*, pages 305–321. Springer, Heidelberg, February / March 2016.

GRS$^+$11. Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh. Round optimal blind signatures. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 630–648. Springer, Heidelberg, August 2011.

GS08. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432. Springer, Heidelberg, April 2008.

GS12. Essam Ghadafi and Nigel P. Smart. Efficient two-move blind signatures in the common reference string model. In Dieter Gollmann and Felix C. Freiling, editors, *ISC 2012: 15th International Conference on Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 274–289. Springer, Heidelberg, September 2012.

HJK12. Dennis Hofheinz, Tibor Jager, and Edward Knapp. Waters signatures with optimal security reduction. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 66–83. Springer, Heidelberg, May 2012.

HK16. Lucjan Hanzlik and Kamil Kluczniak. A Short Paper on Blind Signatures from Knowledge Assumptions. In *Financial Cryptography and Data Security - FC 2016*, LNCS. Springer, 2016.

HS14. Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 491–511. Springer, Heidelberg, December 2014.

JLO97. Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures (extended abstract). In Burton S. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO'97*, volume 1294 of *Lecture Notes in Computer Science*, pages 150–164. Springer, Heidelberg, August 1997.

Jou00. Antoine Joux. A one round protocol for tripartite diffie-hellman. In Wieb Bosma, editor, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.

KPW15. Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 275–295. Springer, Heidelberg, August 2015.

Lin03. Yehuda Lindell. Bounded-concurrent secure two-party computation without setup assumptions. In *35th Annual ACM Symposium on Theory of Computing*, pages 683–692. ACM Press, June 2003.

LW14. Allison B. Lewko and Brent Waters. Why proving HIBE systems secure is difficult. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 58–76. Springer, Heidelberg, May 2014.

Oka93. Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, *Advances in Cryptology – CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer, Heidelberg, August 1993.

Oka06. Tatsuaki Okamoto. Efficient blind and partially blind signatures without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006: 3rd Theory of Cryptography Conference*, volume 3876 of *Lecture Notes in Computer Science*, pages 80–99. Springer, Heidelberg, March 2006.

OO98. Kazuo Ohta and Tatsuaki Okamoto. On concrete security treatment of signatures derived from identification. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 354–369. Springer, Heidelberg, August 1998.

PS00. David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

SC12. Jae Hong Seo and Jung Hee Cheon. Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In Ronald Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 133–150. Springer, Heidelberg, March 2012.

SU12. Dominique Schröder and Dominique Unruh. Security of blind signatures revisited. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 662–679. Springer, Heidelberg, May 2012.

A Proof of Theorem 1

Proof. We assume that there is an efficient adversary $\mathcal{A}$ winning the unforgeability game with non-negligible probability $\epsilon(\kappa)$ and construct an adversary $\mathcal{B}$ that uses $\mathcal{A}$ to break the EUF-CMA security of the underlying SPS-EQ scheme.

We are now going to describe the setup, the initialization of the environment, the reduction and the abort conditions.

$\mathcal{B}$ obtains pk of the SPS-EQ scheme with $\ell = 4$ from the challenger $\mathcal{C}$ of the EUF-CMA security game and runs $\mathcal{A}(\mathsf{pk})$. Whenever $\mathcal{A}$ queries the $(\cdot, \mathcal{S}_{\mathsf{BS}}(\cdot, \mathsf{sk}))$ oracle with message M, $\mathcal{B}$ queries the SPS-EQ signing oracle $\mathcal{O}(\cdot, \mathsf{sk})$ with identical message M and forwards its response to $\mathcal{A}$. If $\mathcal{A}$ outputs $((m_1, \tau_1), \ldots, (m_{k+1}, \tau_{k+1}))$ with $\tau_i = (\sigma_i, Y_i, Q_i, R_i, U_i, X_i, \hat{U}_i, \hat{V}_i)$ after k successful queries to $(\cdot, \mathcal{S}_{\mathsf{BS}}(\cdot, \mathsf{sk}))$ with $m_i \neq m_j \;\; \forall i, j \in [k+1], i \neq j$ and $\mathsf{Verify}_{\mathsf{BS}}(m_i, \tau_i, \mathsf{pk}) = 1$ $\forall i \in [k+1]$, then we have that $(C_i = m_i P + Y_i, R_i, Q_i, P) \neq (C_j = m_j P + Y_j, R_j, Q_j, P)$ for all $i, j \in [k+1], i \neq j$. This follows from the fact that any choice of $(Y, U, X, \hat{U}, \hat{V})$ satisfying verification together with (σ, Q, R) leads to the same m: Let u, v be such that $\hat{U} = u\hat{P}$ and $\hat{V} = v\hat{P}$. Then by $e(Q, \hat{P}) = e(U, \hat{V})$, the 2nd equation in (3): $Q = uvP$; and (4.1), that is $e(U, \hat{P}) = e(P, \hat{U})$, implies $U = uP$. With r s.t. $R = rP$, we have $X = ruP$ by $e(X, \hat{P}) = e(R, \hat{U})$ in (4.2) and $Y = ruv = rQ$ by $e(Y, \hat{P}) = e(X, \hat{V})$ in (4.3). This means that R and Q uniquely determine Y, which together with $C = mP + Y$ uniquely determines m.

$\mathcal{A}$ has made k valid signing queries, but $((m_i P + Y_i, R_i, Q_i, P), \sigma_i)_{i \in [k+1]}$ are valid message-signature pairs under the SPS-EQ scheme for *distinct* classes. Consequently, there exists $n \in [k+1]$ such that the message-signature pair $((m_n P + Y_n, R_n, Q_n, P), \sigma_n)$ represents a class that has not been queried to $\mathcal{C}$'s signing oracle. Hence, one of these $k+1$ message-signature pairs enables $\mathcal{B}$ to break the EUF-CMA security of the SPS-EQ scheme. Due to blindness, however, $\mathcal{B}$ is not able to link these message-signature pairs to the messages $M_i = (s_i(m_i P + Y_i), s_i R_i, s_i Q_i, s_i P)$ which $\mathcal{A}$ has queried to the $(\cdot, \mathcal{S}_{\mathsf{BS}}(\cdot, \mathsf{sk}))$ oracle. Thus, $\mathcal{B}$ has no efficient means to determine the correct index n of the output that lets $\mathcal{B}$ break the EUF-CMA security of the SPS-EQ scheme. Consequently, $\mathcal{B}$ guesses an index $n^* \in [k+1]$ and outputs $((m_{n^*} P + Y_{n^*}, R_{n^*}, Q_{n^*}, P), \sigma_{n^*})$ as a forgery to $\mathcal{C}$. If $\mathcal{A}$ wins the unforgeability game, then $\mathcal{B}$ breaks the EUF-CMA security of the underlying SPS-EQ scheme incurring a polynomial loss of $1/(k+1)$. □

B Proof of Theorem 2

We start with showing that under the assumption in Definition 4 two distributions are indistinguishable, which we will use in the proof of blindness:

Lemma 2. *If ABDDH$^+$ (Def. 4) holds for* BGGen *then the following two distributions are indistinguishable by all PPT adversaries:*

$$\begin{aligned}\mathcal{D}_1 :\equiv \big[&\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\kappa),\ r, s, u, v \xleftarrow{R} \mathbb{Z}_p : \\ &(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P},\ srP, suvP, sruvP)\big] \\ \mathcal{D}_2 :\equiv \big[&\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\kappa),\ r, s, u, v, t, w, z \xleftarrow{R} \mathbb{Z}_p : \\ &(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P},\ tP, wP, zP)\big]\end{aligned}$$

Proof. We first consider an intermediate distribution:

$$\begin{aligned}\mathcal{D}_3 :\equiv \big[&\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\kappa),\ r, s, u, v \xleftarrow{R} \mathbb{Z}_p : \\ &(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P},\ \underline{t}P, suvP, \underline{t}uvP)\big]\end{aligned}$$

Under DDH in $\mathbb{G}_1$ (which by Lemma 1 follows from ABDDH$^+$) it is indistinguishable from $\mathcal{D}_1$, since given a DDH instance (BG, R, S, T), we can choose $u, v \xleftarrow{R} \mathbb{Z}_p$ and compute $(\mathsf{BG}, S, R, uP, uR, uvP, uvR, u\hat{P}, v\hat{P}, T, uvS, uvT)$, which when given a DDH instance is distributed as $\mathcal{D}_1$, and when given a random instance is distributed as $\mathcal{D}_3$.

Next we consider another distribution and show that it is indistinguishable from $\mathcal{D}_3$ under ABDDH$^+$:

$$\begin{aligned}\mathcal{D}_4 :\equiv \big[&\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\kappa),\ r, s, u, v \xleftarrow{R} \mathbb{Z}_p : \\ &(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P},\ tP, \underline{w}P, tuvP)\big]\end{aligned}$$

Given an instance $(\mathsf{BG}, S = sP, U = uP, Q = uvP, \hat{U} = u\hat{P}, \hat{V} = v\hat{P}, W)$, where either $W = suvP$ or W is random, we can choose $r, t \xleftarrow{R} \mathbb{Z}_p$ and compute $(\mathsf{BG}, S, rP, U, rU, Q, rQ, \hat{U}, \hat{V}, tP, W, tQ)$, which, if $W = suvP$, is distributed as $\mathcal{D}_3$ and if W is random, it is distributed as $\mathcal{D}_4$.

Finally, $\mathcal{D}_4$ is indistinguishable from $\mathcal{D}_2$, again by ABDDH$^+$: Given an instance $(\mathsf{BG}, T = tP, U = uP, Q = uvP, \hat{U} = u\hat{P}, \hat{V} = v\hat{P}, Z)$, we can choose $r, s, w \xleftarrow{R} \mathbb{Z}_p$ and compute $(\mathsf{BG}, sP, rP, U, rU, Q, rQ, \hat{U}, \hat{V}, T, wP, Z)$, which if $Z = tuvP$ is distributed as $\mathcal{D}_4$ and if Z is random, it is distributed as $\mathcal{D}_2$. □

In the subsequent proof of blindness of our blind signature scheme, we will use the following implication of Definition 9:

Corollary 1. *Let* $\mathsf{SPS\text{-}EQ}$ *be an SPS-EQ scheme on* $(\mathbb{G}_i^*)^\ell$ *that satisfies Definition 9. If for a tuple* $(\mathsf{pk}, M, s_0, s_1, \sigma_0, \sigma_1)$ *we have* $\mathsf{Verify}_{\mathcal{R}}(s_0 M, \sigma_0, \mathsf{pk}) = 1$ *and* $\mathsf{Verify}_{\mathcal{R}}(s_1 M, \sigma_1, \mathsf{pk}) = 1$ *then* $\mathsf{ChgRep}_{\mathcal{R}}(s_0 M, \sigma_0, \frac{1}{s_0}, \mathsf{pk})$ *and* $\mathsf{ChgRep}_{\mathcal{R}}(s_1 M, \sigma_1, \frac{1}{s_1}, \mathsf{pk})$ *are identically distributed.*

Proof. The statement follows, since for $b = 0, 1$ the tuple $(\mathsf{pk}, s_b M, \sigma_b, \frac{1}{s_b})$ satisfies Equation (1), and for $(M, \sigma_b) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(s_b M, \sigma_b, \frac{1}{s_b}, \mathsf{pk})$, by Definition 9, σ_b is random conditioned on the fact that $\mathsf{Verify}_{\mathcal{R}}(M, \sigma_b, \mathsf{pk}) = 1$. Thus σ_0 and σ_1 are identically distributed. □

Proof (of Theorem 2). Consider the blindness game (with adversarially generated public keys) for the scheme in Figure 2 and a PPT adversary $\mathcal{A}$. W.l.o.g. we assume that $\mathcal{A}$ calls both its oracles. Written out, we have:

$\mathbf{Exp}^{\mathrm{blind}}_{\mathcal{A},\,\mathsf{BS}}(\kappa)$:

```
 1: $b \overset{R}{\leftarrow} \{0,1\}$
 2: $(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(1^\kappa)$
 3: $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$
 4: $r_0, s_0, u_0, v_0 \overset{R}{\leftarrow} \mathbb{Z}_p$
 5: $r_1, s_1, u_1, v_1 \overset{R}{\leftarrow} \mathbb{Z}_p$
 6: $M_0 \leftarrow (s_0(m_0P + r_0u_0v_0P), s_0r_0P, s_0u_0v_0P, s_0P)$
 7: $M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
 8: $(\pi_b, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
 9: $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
10: if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then $b^* \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, \perp, \perp)$
11: else
12:     $(N_0, \sigma_0) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_0, \pi_0, \frac{1}{s_0}, \mathsf{pk})$
13:     $(N_1, \sigma_1) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_1, \pi_1, \frac{1}{s_1}, \mathsf{pk})$
14:     $b^* \overset{R}{\leftarrow} \mathcal{A}\big(\mathsf{st}_{\mathcal{A}}, (\sigma_0, r_0u_0v_0P, u_0v_0P, r_0P, u_0P, r_0u_0P, u_0\hat{P}, v_0\hat{P}),$
                $(\sigma_1, r_1u_1v_1P, u_1v_1P, r_1P, u_1P, r_1u_1P, u_1\hat{P}, v_1\hat{P})\big)$
15: end if
16: return $(b^* = b)$
```

We have slightly modified the game, in that (for $i = 0, 1$) we allowed r_i, s_i, u_i, v_i to also take the value 0 and be such that $m_i + r_iu_iv_i = 0$. However, these events only happen with negligible probability (thus if the original game returned 1 with probability one half plus non-negligible then this is still the case in the above game). We now distinguish two cases, depending on whether the adversary returns an invalid π_0 or an invalid π_1, or whether they are both valid.

Case I: $\mathcal{A}$ Returns an Invalid Signature

Consider the following game, where if the adversary returns two valid signatures then the experiment outputs a random bit:

$\mathbf{Exp}^{\mathrm{blind\text{-}(I)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa)$:

```
 1: $b \overset{R}{\leftarrow} \{0,1\}$
 2: $(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(1^\kappa)$
 3: $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$
 4: $r_0, s_0, u_0, v_0 \overset{R}{\leftarrow} \mathbb{Z}_p$
 5: $r_1, s_1, u_1, v_1 \overset{R}{\leftarrow} \mathbb{Z}_p$
 6: $M_0 \leftarrow (s_0(m_0P + r_0u_0v_0P), s_0r_0P, s_0u_0v_0P, s_0P)$
 7: $M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
 8: $(\pi_b, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
 9: $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
10: if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then
11:     $b^* \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, \perp, \perp)$
12:     return $(b^* = b)$
13: else return $b' \overset{R}{\leftarrow} \{0,1\}$
14: end if
```

We now define another variant $\mathbf{Exp}^{\mathrm{blind\text{-}(I)\text{-}(0)}}$, where we replace line 6 in $\mathbf{Exp}^{\mathrm{blind\text{-}(I)}}$ with the following line:

$$t_0, w_0, z_0 \overset{R}{\leftarrow} \mathbb{Z}_p \;;\; M_0 \leftarrow (s_0m_0P + z_0P, t_0P, w_0P, s_0P) \;.$$

Claim 1. *If ABDDH$^+$ holds for* BGGen *then for all PPT* $\mathcal{A}$ *we have:* $\big|\Pr[\mathbf{Exp}^{\text{blind-(I)}}_{\mathcal{A},\mathsf{BS}} = 1] - \Pr[\mathbf{Exp}^{\text{blind-(I)-(0)}}_{\mathcal{A},\mathsf{BS}} = 1]\big|$ *is negligible.*

Proof. Assume that for some adversary $\mathcal{A}$, the probability of the two experiments outputting 1 is non-negligibly different. Then we can construct an adversary $\mathcal{B}$ that can distinguish $\mathcal{D}_1$ from $\mathcal{D}_2$ in Lemma 2, that is, decide whether $(T, W, Z) = (srP, suvP, sruvP)$ or whether it is random.

Reduction $\mathcal{B}\big(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P}, T, W, Z\big)$:

```
1:  $b \xleftarrow{R} \{0,1\}$
2:  $(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{BG})$
3:  $r_1, s_1, u_1, v_1 \xleftarrow{R} \mathbb{Z}_p$
4:  $M_0 \leftarrow (m_0(sP) + Z, T, W, (sP))$
5:  $M_1 \leftarrow (s_1(m_1 P + r_1 u_1 v_1 P), s_1 r_1 P, s_1 u_1 v_1 P, s_1 P)$
6:  $(\pi_b, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
7:  $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
8:  if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then
9:      $b^* \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, \perp, \perp)$
10:     return $(b^* = b)$
11: else return $b' \xleftarrow{R} \{0,1\}$
12: end if
```

It is immediate that if $(T, W, Z) = (srP, suvP, sruvP)$ then $\mathcal{B}$ simulates $\mathbf{Exp}^{\text{blind-(I)}}$, while if (T, W, Z) is random in $\mathbb{G}_1^3$ then $\mathcal{B}$ simulates $\mathbf{Exp}^{\text{blind-(I)-(0)}}$. □

We next define a further game $\mathbf{Exp}^{\text{blind-(I)-(1)}}$, where in $\mathbf{Exp}^{\text{blind-(I)}}$ we additionally replace line 7 by

$$t_1, w_1, z_1 \xleftarrow{R} \mathbb{Z}_p \ ; \ M_1 \leftarrow (s_1 m_1 P + z_1 P, t_1 P, w_1 P, s_1 P) \ .$$

By an argument analogous to the proof of Claim 1, we have:

Claim 2. *If ABDDH$^+$ holds for* BGGen *then for all PPT* $\mathcal{A}$ *we have:* $\big|\Pr[\mathbf{Exp}^{\textit{blind-(I)-(0)}}_{\mathcal{A},\mathsf{BS}} = 1] - \Pr[\mathbf{Exp}^{\textit{blind-(I)-(1)}}_{\mathcal{A},\mathsf{BS}} = 1]\big|$ *is negligible.*

Now in $\mathbf{Exp}^{\text{blind-(I)-(1)}}$ the elements z_0 and z_1 perfectly hide m_0 and m_1, meaning the bit b is information-theoretically hidden from $\mathcal{A}$; thus $\Pr[\mathbf{Exp}^{\text{blind-(I)-(1)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1] = \frac{1}{2}$. Lemma 2, Claims 1 and 2 together yield: If ABDDH$^+$ holds then for all PPT $\mathcal{A}$:

$$\Pr[\mathbf{Exp}^{\text{blind-(I)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1] \leq \tfrac{1}{2} + \nu^{(\mathrm{I})}(\kappa) \quad \text{for some negligible } \nu^{(\mathrm{I})}(\cdot) \ . \tag{6}$$

Case II: $\mathcal{A}$ Returns Two Valid Signatures

We now consider the "dual" game of $\mathbf{Exp}^{\text{blind-(I)}}$, where we output a random bit if the adversary does not return two valid signatures (see below). We show that if $\mathcal{D}_1$ and $\mathcal{D}_2$ from Lemma 2 are indistinguishable then game $\mathbf{Exp}^{\text{blind-(II)}}$ cannot be won with a non-negligible advantage. To do so, we define a series of intermediate games $\mathbf{Exp}^{\text{blind-(II)-(i)}}_{\mathcal{A},\,\mathsf{BS}}$ for $i = 0, 1, 2, 3$. These intermediate games involve multiple rewindings of the adversary $\mathcal{A}$.

$\mathbf{Exp}^{\text{blind-(II)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa)$

```
$\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^{\kappa})$
$(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{BG})$
$r_0, u_0, v_0 \xleftarrow{R} \mathbb{Z}_p,\ r_1, u_1, v_1 \xleftarrow{R} \mathbb{Z}_p$
$(\star)\ s_0, s_1 \xleftarrow{R} \mathbb{Z}_p\ ;\ b \xleftarrow{R} \{0,1\}$
$M_0 \leftarrow (s_0(m_0P + r_0u_0v_0P), s_0r_0P, s_0u_0v_0P, s_0P)$
$M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
$(\pi_b, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
$(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then return $b' \xleftarrow{R} \{0,1\}$        ▷ Aborting run
else
    $(N_0, \sigma_0) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_0, \pi_0, \frac{1}{s_0}, \mathsf{pk})$
    $(N_1, \sigma_1) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_1, \pi_1, \frac{1}{s_1}, \mathsf{pk})$
    $b^* \xleftarrow{R} \mathcal{A}\big(\mathsf{st}_{\mathcal{A}}, (\sigma_0, r_0u_0v_0P, u_0v_0P, r_0P, u_0P, r_0u_0P, u_0\hat{P}, v_0\hat{P}),$
                                   $(\sigma_1, r_1u_1v_1P, u_1v_1P, r_1P, u_1P, r_1u_1P, u_1\hat{P}, v_1\hat{P})\big)$
    return $(b^* = b)$
end if
```

Game $\mathbf{Exp}^{\textbf{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}$. The description of this game is given below; it consists of $\lambda + 1$ runs of the adversary $\mathcal{A}$ forked from the point $(\star)$ in $\mathbf{Exp}^{\text{blind-(II)}}$. A particular run is considered to be "non-aborting" if both the signatures that $\mathcal{A}$ generates (viz., (M_i, π_i) for $i = 0, 1$) are valid. If there exists a non-aborting run among the first λ runs, we run the adversary for one final time. We relate the probability of success of the forking to that of the underlying experiment $\mathbf{Exp}^{\text{blind-(II)}}$.

$\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa, \lambda)$

```
$\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^{\kappa})$
$(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{BG})$
$r_0, u_0, v_0 \xleftarrow{R} \mathbb{Z}_p,\ r_1, u_1, v_1 \xleftarrow{R} \mathbb{Z}_p$
for $j = 1, \ldots, \lambda$: do                                                    ▷ Run $\lambda$ times from $\star$
    $s_0^{(j)}, s_1^{(j)} \xleftarrow{R} \mathbb{Z}_p\ ;\ b^{(j)} \xleftarrow{R} \{0,1\}$
    $M_0^{(j)} \leftarrow (s_0^{(j)}(m_0P + r_0u_0v_0P), s_0^{(j)}r_0P, s_0^{(j)}u_0v_0P, s_0^{(j)}P)$
    $M_1^{(j)} \leftarrow (s_1^{(j)}(m_1P + r_1u_1v_1P), s_1^{(j)}r_1P, s_1^{(j)}u_1v_1P, s_1^{(j)}P)$
    $(\pi^{(j)}_{b^{(j)}}, \mathsf{st}^{(j)}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M^{(j)}_{b^{(j)}})$;   $(\pi^{(j)}_{1-b^{(j)}}, \mathsf{st}^{(j)}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}^{(j)}_{\mathcal{A}}, M^{(j)}_{1-b^{(j)}})$
    if $\mathsf{Verify}_{\mathcal{R}}(M_0^{(j)}, \pi_0^{(j)}, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1^{(j)}, \pi_1^{(j)}, \mathsf{pk}) = 0$ then $a^{(j)} \leftarrow \perp$        ▷ Event $A_t$
    end if
end for
if $\exists j \in [\lambda] : (a^{(j)} \neq \perp)$ then                                ▷ Event $\neg(A_1 \wedge \ldots \wedge A_\lambda)$
    $s_0, s_1 \xleftarrow{R} \mathbb{Z}_p\ ;\ b\ \xleftarrow{R} \{0,1\}$                                      ▷ Final run
    $M_0 \leftarrow (s_0(m_0P + r_0u_0v_0P), s_0r_0P, s_0u_0v_0P, s_0P)$
    $M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
    $(\pi_b, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$;   $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
    if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then return $b' \xleftarrow{R} \{0,1\}$        ▷ Event $A$
    else
        $(N_0, \sigma_0) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_0, \pi_0, \frac{1}{s_0}, \mathsf{pk})$
        $(N_1, \sigma_1) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_1, \pi_1, \frac{1}{s_1}, \mathsf{pk})$
        $b^* \xleftarrow{R} \mathcal{A}\big(\mathsf{st}_{\mathcal{A}}, (\sigma_0, r_0u_0v_0P, u_0v_0P, r_0P, u_0P, r_0u_0P, u_0\hat{P}, v_0\hat{P}),$
                                   $(\sigma_1, r_1u_1v_1P, u_1v_1P, r_1P, u_1P, r_1u_1P, u_1\hat{P}, v_1\hat{P})\big)$
        $b' \leftarrow (b^* = b)$
    end if
else return $b' \xleftarrow{R} \{0,1\}$                                          ▷ Event $A_1 \wedge \ldots \wedge A_\lambda$
end if
```

We now relate the probability that this game outputs 1 to the probability that the game without rewinding outputs 1.

Claim 3. *There exists a function λ such that the following holds. If* $\Pr[\mathbf{Exp}^{\text{blind-(II)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1] \geq \frac{1}{2} + \varphi(\kappa)$ *for a non-negligible function* $\varphi(\cdot)$ *then* $\Pr[\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa, \lambda(\kappa)) = 1] \geq \frac{1}{2} + \psi(\kappa)$ *for a non-negligible function* $\psi(\cdot)$*. Moreover, if* $\mathbf{Exp}^{\text{blind-(II)}}_{\mathcal{A},\,\mathsf{BS}}(\cdot)$ *is polynomial-time then so is* $\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}(\cdot, \lambda(\cdot))$*.*

Proof. Consider the random coins used in the experiment $\mathbf{Exp}^{\text{blind-(II)}}_{\mathcal{A},\,\mathsf{BS}}$. Let X denote the coins it uses before the point $(\star)$; that is, X consists of the internal coins of $\mathcal{A}$ (before $(\star)$) and $((r_0, u_0, v_0), (r_1, u_1, v_1))$. Similarly, Y denotes the coins used after $(\star)$: the internal coins of $\mathcal{A}$ (after $(\star)$), coins used in $\mathsf{ChgRep}_{\mathcal{R}}$ and $(s_0, s_1), b$. Moreover, let A (for "abort") be the set of coins (X, Y) which lead to π_0 or π_1 being invalid and let W ("winning") be the set of coins where π_0 and π_1 are valid and $b^* = b$, that is, the final output is 1. Let $\mathcal{X}$ and $\mathcal{Y}$ be the (efficient) sampling algorithms for X and Y. $\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}$ can be abstracted to the following forking experiment:

```
$\mathbf{Exp}^{\text{fork}}(\mathcal{X}, \mathcal{Y}, \kappa, \lambda)$
  $X \xleftarrow{R} \mathcal{X}$, $Y, Y_1 \ldots Y_\lambda \xleftarrow{R} \mathcal{Y}$
  if $\forall i : (X, Y_i) \in A$ then return $b \xleftarrow{R} \{0,1\}$          ▷ Event $A_1 \wedge \ldots \wedge A_\lambda$
  else
      if $(X, Y) \in A$ then return $b \xleftarrow{R} \{0,1\}$                    ▷ Event $A$
      else if $(X, Y) \in W$ then return 1                                        ▷ Event $W$
      else return 0
      end if
  end if
```

From the assumption made in the claim, we have

$$\frac{1}{2}\Pr[A] + \Pr[W] \geq \frac{1}{2} + \varphi \ , \tag{7}$$

Since by assumption φ is non-negligible, there exists a polynomial p such that for infinitely many κ:

$$\varphi(\kappa) \geq \frac{1}{p(\kappa)} \ , \tag{8}$$

Let $1/2 + \psi$ denote the probability with which 1 is output in experiment $\mathbf{Exp}^{\text{fork}}$—and hence in $\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}$. Our goal is to show that ψ is a non-negligible function of φ—to be precise, we show that $\psi \geq \varphi/2$ up to a negligible term. From the definition of $\mathbf{Exp}^{\text{fork}}$ we have

$$\begin{aligned}
\frac{1}{2} + \psi &= \frac{1}{2}\underbrace{\Pr[A_1 \wedge \ldots \wedge A_\lambda]}_{= \Pr[(A_1 \wedge \ldots \wedge A_\lambda) \wedge A] + \Pr[(A_1 \wedge \ldots \wedge A_\lambda) \wedge \bar{A}]} + \frac{1}{2}\Pr[\neg(A_1 \wedge \ldots \wedge A_\lambda) \wedge A] + \Pr[\neg(A_1 \wedge \ldots \wedge A_\lambda) \wedge W] \\
&= \frac{1}{2}\Pr[A] + \frac{1}{2}\Pr[\bar{A} \wedge (A_1 \wedge \ldots \wedge A_\lambda)] + \Pr[W \wedge \neg(A_1 \wedge \ldots \wedge A_\lambda)] \\
&\geq \frac{1}{2}\Pr[A] + \Pr[W \wedge \neg(A_1 \wedge \ldots \wedge A_\lambda)] \ .
\end{aligned} \tag{9}$$

Next, we follow the line of argument similar to that in [LW14]. Let $U \subseteq W$ denote the subset of winning coins for which the probability of aborting when rewinding is below some threshold ρ, which we set later; that is

$$U := \{(X,Y) \in W : \Pr_{Y' \overset{R}{\leftarrow} \mathcal{Y}}[(X,Y') \in A] < \rho\} \ . \tag{10}$$

It is possible to upper bound the size of the set $W \setminus U$, in a similar vein to the heavy-row lemma [OO98].

Claim. $\Pr[W \setminus U] < \rho$.

Proof. Let $P(X) := \Pr[(X,Y) \in \bar{A}]$, where the probability is over the choice of $Y \overset{R}{\leftarrow} \mathcal{Y}$. Similarly, let $P'(X) := \Pr[(X,Y) \in W]$; note that $P'(X) \leq P(X)$ since $W \subseteq \bar{A}$. By definition,

$$\Pr[W \setminus U] = \sum_{X:P'(X)<\rho} \Pr[X] \cdot P'(X) \leq \sum_{X:P(X)<\rho} \Pr[X] \cdot P(X) \leq \rho \cdot \sum_{X:P(X)<\rho} \Pr[X] < \rho \qquad \square$$

Now, we re-write (9) in terms of U:

$$\begin{aligned}
\frac{1}{2} + \psi &\geq \frac{1}{2}\Pr[A] + \Pr[U \wedge \neg(A_1 \wedge \ldots \wedge A_\lambda)] && \text{(As } U \subseteq W\text{)}\\
&= \frac{1}{2}\Pr[A] + \Pr[U] \cdot (1 - \Pr[A_1 \wedge \ldots \wedge A_\lambda | U])\\
&= \frac{1}{2}\Pr[A] + \Pr[U] \cdot (1 - \varPi_{i \in [\lambda]} \Pr[A_i | U]) && \text{(By independence of } A_i\text{'s on fixing } X\text{)}\\
&\geq \frac{1}{2}\Pr[A] + \Pr[U] - \Pr[U] \cdot (1-\rho)^\lambda && \text{(By definition of } U\text{; see (10))}\\
&= \frac{1}{2}\Pr[A] + \Pr[W] - \Pr[W \setminus U] - \Pr[U] \cdot (1-\rho)^\lambda\\
&\geq \frac{1}{2} + \varphi - \rho - (1-\rho)^\lambda . && \text{(By (7) and the bounds } \Pr[W \setminus U] < \rho, \Pr[U] \leq 1\text{)} \quad (11)
\end{aligned}$$

For the rest of the analysis, let κ be an arbitrary value (of infinitely many) that satisfies (8). We thus have

$$\psi(\kappa) \geq \frac{1}{p(\kappa)} - \rho - (1-\rho)^\lambda \ .$$

Setting $\rho = \frac{1}{4p(\kappa)}$ and $\lambda = \kappa \cdot p(\kappa)$, we have

$$\psi(\kappa) \geq \frac{3}{4p(\kappa)} - \left(1 - \frac{1}{4p(\kappa)}\right)^{\kappa \cdot p(\kappa)} = \frac{3}{4p(\kappa)} - \Bigg(\underbrace{\left(1 - \frac{1}{4p(\kappa)}\right)^{4p(\kappa)}}_{\leq 1/e}\Bigg)^{\kappa/4} \geq \frac{3}{4p(\kappa)} - \frac{1}{e^{\kappa/4}} \ ,$$

where the last term is greater than $\frac{1}{2p(\kappa)}$ for infinitely many κ. This shows that $\psi(\cdot)$ is a non-negligible function, which proves the first statement of the claim. The second statement is also satisfied, as $\lambda(\kappa) = \kappa \cdot p(\kappa)$ is a polynomial, and thus $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(0)}}(\cdot, \lambda(\cdot))$ runs in polynomial time if $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)}}(\cdot)$ does. $\square$

We move now to the next intermediate game.

Game $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\textbf{blind-(II)-(1)}}$. We now modify lines 19 and 20 in game $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(0)}}$ to the following:

$$(N_0, \sigma_0) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_0^{(j^*)}, \pi_0^{(j^*)}, \tfrac{1}{s_0^{(j^*)}}, \mathsf{pk})$$
$$(N_1, \sigma_1) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_1^{(j^*)}, \pi_1^{(j^*)}, \tfrac{1}{s_1^{(j^*)}}, \mathsf{pk}) \ .$$

That is, we use the signatures $\pi_0^{(j^*)}, \pi_1^{(j^*)}$ from one of the (arbitrarily chosen) non-aborting runs j^*, adapt them to signatures on N_i and give them to $\mathcal{A}$ as part of our blind signatures in the final run. We now argue that the probability of games $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(0)}}$ and $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(1)}}$ outputting 1 is the same. For $i = 0, 1$ we have the following. Since

$$\mathsf{Verify}_{\mathcal{R}}\big(s_i^{(j^*)} \cdot (m_iP + r_iu_iv_iP, r_iP, u_iv_iP, P), \pi_i^{(j^*)}, \mathsf{pk}\big) = 1 \quad \text{and}$$
$$\mathsf{Verify}_{\mathcal{R}}\big(s_i \cdot (m_iP + r_iu_iv_iP, r_iP, u_iv_iP, P), \pi_i, \mathsf{pk}\big) = 1 \ ,$$

the tuple $\big(\mathsf{pk}, (m_iP + r_iu_iv_iP, r_iP, u_iv_iP, P), s_i^{(j^*)}, s_i, \pi_i^{(j^*)}, \pi_i\big)$ satisfies the premise of Corollary 1 and therefore the outputs $\sigma_i^{(j^*)}$ of $\mathsf{ChgRep}_{\mathcal{R}}(M_i^{(j^*)}, \pi_i^{(j^*)}, \frac{1}{s_i^{(j^*)}}, \mathsf{pk})$ and σ_i of $\mathsf{ChgRep}_{\mathcal{R}}(M_i, \pi_i, \frac{1}{s_i}, \mathsf{pk})$ are identically distributed—hence so are $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(0)}}$ and $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(1)}}$. Let us write down $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(1)}}$:

$\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(1)}}(\kappa, \lambda)$

```
 1: $\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$
 2: $(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{BG})$
 3: $r_0, u_0, v_0 \xleftarrow{R} \mathbb{Z}_p,\ r_1, u_1, v_1 \xleftarrow{R} \mathbb{Z}_p$
 4: for $j = 1, \ldots, \lambda$: do                                          ▷ Run $\lambda$ times from $\star$
 5:     $s_0^{(j)}, s_1^{(j)} \xleftarrow{R} \mathbb{Z}_p$ ; $b^{(j)} \xleftarrow{R} \{0,1\}$
 6:     $M_0^{(j)} \leftarrow (s_0^{(j)}(m_0P + r_0u_0v_0P), s_0^{(j)}r_0P, s_0^{(j)}u_0v_0P, s_0^{(j)}P)$
 7:     $M_1^{(j)} \leftarrow (s_1^{(j)}(m_1P + r_1u_1v_1P), s_1^{(j)}r_1P, s_1^{(j)}u_1v_1P, s_1^{(j)}P)$
 8:     $(\pi_{b^{(j)}}^{(j)}, \mathsf{st}_{\mathcal{A}}^{(j)}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{b^{(j)}}^{(j)})$
 9:     $(\pi_{1-b^{(j)}}^{(j)}, \mathsf{st}_{\mathcal{A}}^{(j)}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}^{(j)}, M_{1-b^{(j)}}^{(j)})$
10:     if $\mathsf{Verify}_{\mathcal{R}}(M_0^{(j)}, \pi_0^{(j)}, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1^{(j)}, \pi_1^{(j)}, \mathsf{pk}) = 0$ then $a^{(j)} \leftarrow \perp$     ▷ Event $A_t$
11:     end if
12: end for
13: if $\exists j \in [\lambda] : (a^{(j)} \neq \perp)$ then                        ▷ Event $\neg(A_1 \wedge \ldots \wedge A_\lambda)$
14:     Pick (arbitrarily) $j^* \in [\lambda]$ such that $a^{(j^*)} \neq \perp$
15:     $s_0, s_1 \xleftarrow{R} \mathbb{Z}_p$ ; $b \ \xleftarrow{R} \{0,1\}$                                    ▷ Final run
16:     $M_0 \leftarrow (s_0(m_0P + r_0u_0v_0P), s_0r_0P, s_0u_0v_0P, s_0P)$
17:     $M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
18:     $(\pi_b, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
19:     $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
20:     if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then return $b' \xleftarrow{R} \{0,1\}$     ▷ Event $A$
21:     else
22:         $(N_0, \sigma_0) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_0^{(j^*)}, \pi_0^{(j^*)}, \frac{1}{s_0^{(j^*)}}, \mathsf{pk})$
23:         $(N_1, \sigma_1) \xleftarrow{R} \mathsf{ChgRep}_{\mathcal{R}}(M_1^{(j^*)}, \pi_1^{(j^*)}, \frac{1}{s_1^{(j^*)}}, \mathsf{pk})$
24:         $b^* \xleftarrow{R} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, (\sigma_0, r_0u_0v_0P, u_0v_0P, r_0P, u_0P, r_0u_0P, u_0\hat{P}, v_0\hat{P}),$
                                    $(\sigma_1, r_1u_1v_1P, u_1v_1P, r_1P, u_1P, r_1u_1P, u_1\hat{P}, v_1\hat{P}))$
25:         $b' \leftarrow (b^* = b)$
26:     end if
27: else return $b' \xleftarrow{R} \{0,1\}$                                      ▷ Event $A_1 \wedge \ldots \wedge A_\lambda$
28: end if
```

Game $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(2)}}$. We define the next intermediate game by replacing line 16 in experiment $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(1)}}$ with the following

$$t_0, w_0, z_0 \xleftarrow{R} \mathbb{Z}_p \ ; \ M_0 \leftarrow (s_0m_0P + z_0P, t_0P, w_0P, s_0P) \tag{12}$$

That is, in the definition of M_0 we replaced the values $s_0r_0u_0v_0$ as well as $s_0u_0v_0$ and s_0r_0 with a random elements z_0, w_0 and t_0.

Claim 4. *If ABDDH$^+$ holds for* BGGen *then* $\boldsymbol{Exp}^{blind\text{-}(II)\text{-}(1)}$ *and* $\boldsymbol{Exp}^{blind\text{-}(II)\text{-}(2)}$ *are indistinguishable.*

Proof. Assume that the probability that $(b^* = b)$ is noticeably different in games $\mathbf{Exp}^{\text{blind-(II)-(1)}}_{\mathcal{A},\mathsf{BS}}$ and $\mathbf{Exp}^{\text{blind-(II)-(2)}}_{\mathcal{A},\mathsf{BS}}$. Then we construct an adversary $\mathcal{B}$ that can distinguish $\mathcal{D}_1$ from $\mathcal{D}_2$ in Lemma 2, which is impossible under ABDDH$^+$. Given an instance with randomness (r, s, u, v) and challenge (T, W, Z), $\mathcal{B}$ implicitly sets $r_0 \leftarrow r$, $u_0 \leftarrow u$, $v_0 \leftarrow v$ and $s_0 \leftarrow s$ and simulates $\mathbf{Exp}^{\text{blind-(II)-(1)}}_{\mathcal{A},\mathsf{BS}}$ setting $s_0r_0u_0v_0P \leftarrow Z$ and $s_0u_0v_0P \leftarrow W$ and $s_0r_0P \leftarrow T$.

Reduction $\mathcal{B}\big(\mathsf{BG}, sP, rP, uP, ruP, uvP, ruvP, u\hat{P}, v\hat{P}, T, W, Z\big)$

```
$(\mathsf{pk}, m_0, m_1, \mathsf{st}_\mathcal{A}) \xleftarrow{R} \mathcal{A}(\mathsf{BG})$
$r_0 \leftarrow r, u_0 \leftarrow u, v_0 \leftarrow v$ (implicitly), $r_1, u_1, v_1 \xleftarrow{R} \mathbb{Z}_p$
for $j = 1, \ldots, \lambda$: do                                                    ▷ Run $\lambda$ times from $\star$
    $s_0^{(j)}, s_1^{(j)} \xleftarrow{R} \mathbb{Z}_p$ ; $b^{(j)} \xleftarrow{R} \{0,1\}$
    $M_0^{(j)} \leftarrow (s_0^{(j)}(m_0P + r_0u_0v_0P), s_0^{(j)}r_0P, s_0^{(j)}u_0v_0P, s_0^{(j)}P)$
    $M_1^{(j)} \leftarrow (s_1^{(j)}(m_1P + r_1u_1v_1P), s_1^{(j)}r_1P, s_1^{(j)}u_1v_1P, s_1^{(j)}P)$
    $(\pi_{b^{(j)}}^{(j)}, \mathsf{st}_\mathcal{A}^{(j)}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_\mathcal{A}, M_{b^{(j)}}^{(j)})$
    $(\pi_{1-b^{(j)}}^{(j)}, \mathsf{st}_\mathcal{A}^{(j)}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_\mathcal{A}^{(j)}, M_{1-b^{(j)}}^{(j)})$
    if $\mathsf{Verify}_\mathcal{R}(M_0^{(j)}, \pi_0^{(j)}, \mathsf{pk}) = 0$ or $\mathsf{Verify}_\mathcal{R}(M_1^{(j)}, \pi_1^{(j)}, \mathsf{pk}) = 0$ then $a^{(j)} \leftarrow \perp$      ▷ Event $A_t$
    end if
end for
if $\exists j \in [\lambda] : (a^{(j)} \neq \perp)$ then                                   ▷ Event $\neg(A_1 \wedge \ldots \wedge A_\lambda)$
    Pick (arbitrarily) $j^* \in [\lambda]$ such that $a^{(j^*)} \neq \perp$
    $s_0 \leftarrow s$ (implicitly), $s_1 \xleftarrow{R} \mathbb{Z}_p$ ; $b \xleftarrow{R} \{0,1\}$                  ▷ Final run
    $M_0 \leftarrow (m_0(s_0P) + Z, T, W, s_0P)$
    $M_1 \leftarrow (s_1(m_1P + r_1u_1v_1P), s_1r_1P, s_1u_1v_1P, s_1P)$
    $(\pi_b, \mathsf{st}_\mathcal{A}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_\mathcal{A}, M_b)$
    $(\pi_{1-b}, \mathsf{st}_\mathcal{A}) \xleftarrow{R} \mathcal{A}(\mathsf{st}_\mathcal{A}, M_{1-b})$
    if $\mathsf{Verify}_\mathcal{R}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_\mathcal{R}(M_1, \pi_1, \mathsf{pk}) = 0$ then return $b' \xleftarrow{R} \{0,1\}$   ▷ Event $A$
    else
        $(N_0, \sigma_0) \xleftarrow{R} \mathsf{ChgRep}_\mathcal{R}(M_0^{(j^*)}, \pi_0^{(j^*)}, \frac{1}{s_0^{(j^*)}}, \mathsf{pk})$
        $(N_1, \sigma_1) \xleftarrow{R} \mathsf{ChgRep}_\mathcal{R}(M_1^{(j^*)}, \pi_1^{(j^*)}, \frac{1}{s_1^{(j^*)}}, \mathsf{pk})$
        $b^* \xleftarrow{R} \mathcal{A}\big(\mathsf{st}_\mathcal{A}, (\sigma_0, r_0u_0v_0P, u_0v_0P, r_0P, u_0P, r_0u_0P, u_0\hat{P}, v_0\hat{P}),$
                                    $(\sigma_1, r_1u_1v_1P, u_1v_1P, r_1P, u_1P, r_1u_1P, u_1\hat{P}, v_1\hat{P})\big)$
        $b' \leftarrow (b^* = b)$
    end if
else return $b' \xleftarrow{R} \{0,1\}$                                              ▷ Event $A_1 \wedge \ldots \wedge A_\lambda$
end if
```

The probability that $\mathcal{B}$ outputs 1 when $T = rsP$, $W = suvP$ and $Z = rsuvP$ is the probability that $\mathbf{Exp}^{\text{blind-(II)-(1)}}_{\mathcal{A},\mathsf{BS}}$ outputs 1; and the probability that $\mathcal{B}$ outputs 1 when given random T, W, and Z is the probability that $\mathbf{Exp}^{\text{blind-(II)-(2)}}_{\mathcal{A},\mathsf{BS}}$ outputs 1. □

Game $\mathbf{Exp}^{\text{blind-(II)-(3)}}_{\mathcal{A},\mathsf{BS}}$. In the final game, we replace line 17 of $\mathbf{Exp}^{\text{blind-(II)-(1)}}_{\mathcal{A},\mathsf{BS}}$ with random values as well: $s_1r_1u_1v_1$, $s_1u_1v_1$ and s_1r_1 in the definition of M_1 are replaced with z_1, w_1 and t_1.

$$\begin{aligned} t_0, w_0, z_0 \xleftarrow{R} \mathbb{Z}_p \ ; \ M_0 \leftarrow (s_0m_0P + z_0P, t_0P, w_0P, s_0P) \\ t_1, w_1, z_1 \xleftarrow{R} \mathbb{Z}_p \ ; \ M_1 \leftarrow (s_1m_1P + z_1P, t_1P, w_1P, s_1P) \end{aligned} \tag{13}$$

Claim 5. *If ABDDH$^+$ holds for* BGGen *then* $\boldsymbol{Exp}_{\mathcal{A},\mathsf{BS}}^{\textit{blind-(II)-(2)}}$ *and* $\boldsymbol{Exp}_{\mathcal{A},\mathsf{BS}}^{\textit{blind-(II)-(3)}}$ *are indistinguishable.*

The proof to the claim is analogous to that of Claim 4: we construct an adversary $\mathcal{B}$ which implicitly sets s_1, r_1, u_1, v_1 to the values from a challenge. We omit the details.

Perfect hiding. Finally, let us consider $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(3)}}$ (detailed below). We now see that for $i = 0, 1$, since s_i, t_i, w_i and z_i are uniformly random and used nowhere other than in the definition of M_i, the latter is a uniform random element from $\mathbb{G}_1^4$. Since b is only used to determine the order in which M_0 and M_1 (which are both random elements) are sent to $\mathcal{A}$, the bit b is information-theoretically hidden. We thus have that the probability that $(b^* = b)$ in the game is exactly $\frac{1}{2}$. Combining this with Claims 3, 4 and 5, we have that if ABDDH$^+$ holds for BGGen then for all PPT $\mathcal{A}$:

$$\Pr[\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)}}(\kappa) = 1] \le \tfrac{1}{2} + \nu^{(\text{II})}(\kappa) \quad \text{for some negligible } \nu^{(\text{II})}(\cdot)\ . \tag{14}$$

$\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind-(II)-(3)}}(\kappa, \lambda)$

```
$\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(1^\kappa)$
$(\mathsf{pk}, m_0, m_1, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{BG})$
$r_0, u_0, v_0 \overset{R}{\leftarrow} \mathbb{Z}_p$, $r_1, u_1, v_1 \overset{R}{\leftarrow} \mathbb{Z}_p$
for $j = 1, \ldots, \lambda$: do                                              $\triangleright$ Run $\lambda$ times from $\star$
    $s_0^{(j)}, s_1^{(j)} \overset{R}{\leftarrow} \mathbb{Z}_p$ ; $b^{(j)} \overset{R}{\leftarrow} \{0,1\}$
    $M_0^{(j)} \leftarrow (s_0^{(j)}(m_0 P + r_0 u_0 v_0 P), s_0^{(j)} r_0 P, s_0^{(j)} u_0 v_0 P, s_0^{(j)} P)$
    $M_1^{(j)} \leftarrow (s_1^{(j)}(m_1 P + r_1 u_1 v_1 P), s_1^{(j)} r_1 P, s_1^{(j)} u_1 v_1 P, s_1^{(j)} P)$
    $(\pi_{b^{(j)}}^{(j)}, \mathsf{st}_{\mathcal{A}}^{(j)}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{b^{(j)}}^{(j)})$
    $(\pi_{1-b^{(j)}}^{(j)}, \mathsf{st}_{\mathcal{A}}^{(j)}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}^{(j)}, M_{1-b^{(j)}}^{(j)})$
    if $\mathsf{Verify}_{\mathcal{R}}(M_0^{(j)}, \pi_0^{(j)}, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1^{(j)}, \pi_1^{(j)}, \mathsf{pk}) = 0$ then $a^{(j)} \leftarrow \perp$      $\triangleright$ Event $A_t$
    end if
end for
if $\exists j \in [\lambda] : (a^{(j)} \ne \perp)$ then                              $\triangleright$ Event $\neg(A_1 \wedge \ldots \wedge A_\lambda)$
    Pick (arbitrarily) $j^* \in [\lambda]$ such that $a^{(j^*)} \ne \perp$
    $s_0, s_1 \overset{R}{\leftarrow} \mathbb{Z}_p$ ; $b \overset{R}{\leftarrow} \{0,1\}$                                   $\triangleright$ Final run
    $t_0, w_0, z_0 \overset{R}{\leftarrow} \mathbb{Z}_p$, $M_0 \leftarrow (s_0 m_0 P + z_0 P, t_0 P, w_0 P, s_0 P)$
    $t_1, w_1, z_1 \overset{R}{\leftarrow} \mathbb{Z}_p$, $M_1 \leftarrow (s_1 m_1 P + z_1 P, t_1 P, w_1 P, s_1 P)$
    $(\pi_b, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_b)$
    $(\pi_{1-b}, \mathsf{st}_{\mathcal{A}}) \overset{R}{\leftarrow} \mathcal{A}(\mathsf{st}_{\mathcal{A}}, M_{1-b})$
    if $\mathsf{Verify}_{\mathcal{R}}(M_0, \pi_0, \mathsf{pk}) = 0$ or $\mathsf{Verify}_{\mathcal{R}}(M_1, \pi_1, \mathsf{pk}) = 0$ then return $b' \overset{R}{\leftarrow} \{0,1\}$      $\triangleright$ Event $A$
    else
        $(N_0, \sigma_0) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_0^{(j^*)}, \pi_0^{(j^*)}, \frac{1}{s_0^{(j^*)}}, \mathsf{pk})$
        $(N_1, \sigma_1) \overset{R}{\leftarrow} \mathsf{ChgRep}_{\mathcal{R}}(M_1^{(j^*)}, \pi_1^{(j^*)}, \frac{1}{s_1^{(j^*)}}, \mathsf{pk})$
        $b^* \overset{R}{\leftarrow} \mathcal{A}\big(\mathsf{st}_{\mathcal{A}}, (\sigma_0, r_0 u_0 v_0 P, u_0 v_0 P, r_0 P, u_0 P, r_0 u_0 P, u_0 \hat{P}, v_0 \hat{P}),$
                                   $(\sigma_1, r_1 u_1 v_1 P, u_1 v_1 P, r_1 P, u_1 P, r_1 u_1 P, u_1 \hat{P}, v_1 \hat{P})\big)$
        $b' \leftarrow (b^* = b)$
    end if
else return $b' \overset{R}{\leftarrow} \{0,1\}$                                     $\triangleright$ Event $A_1 \wedge \ldots \wedge A_\lambda$
end if
```

Bringing It All Together

Consider an adversary $\mathcal{A}$ in the original blindness game $\mathbf{Exp}_{\mathcal{A},\mathsf{BS}}^{\text{blind}}$. We let $\mathbf{E}^{(\text{I})}$ denote the event that $\mathcal{A}$ outputs at least one invalid signature and $\mathbf{E}^{(\text{II})}$ denote its complement, that is, both π_0

and π_1 are valid. By (6) we have

$$\tfrac{1}{2} + \nu^{(\mathrm{I})}(\kappa) \geq \Pr[\mathbf{Exp}^{\text{blind-(I)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1] = \Pr[\mathbf{E}^{(\mathrm{I})}]\Pr[\mathbf{Exp}^{\text{blind-(I)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1 \mid \mathbf{E}^{(\mathrm{I})}] \\ + \Pr[\mathbf{E}^{(\mathrm{II})}]\Pr[\mathbf{Exp}^{\text{blind-(I)}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1 \mid \mathbf{E}^{(\mathrm{II})}] \ .$$

Conditioned on $\mathbf{E}^{(\mathrm{I})}$, $\mathbf{Exp}^{\text{blind-(I)}}$ is the same as $\mathbf{Exp}^{\text{blind}}$, and conditioned on $\mathbf{E}^{(\mathrm{II})}$, the probability that $\mathbf{Exp}^{\text{blind-(I)}}$ outputs 1 is $\frac{1}{2}$. We therefore get:

$$\Pr[\mathbf{E}^{(\mathrm{I})}]\Pr[\mathbf{Exp}^{\text{blind}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1 \mid \mathbf{E}^{(\mathrm{I})}] \leq \tfrac{1}{2} - \tfrac{1}{2}\Pr[\mathbf{E}^{(\mathrm{II})}] + \nu^{(\mathrm{I})}(\kappa) \ . \tag{15}$$

Completely analogously we get from (14):

$$\Pr[\mathbf{E}^{(\mathrm{II})}]\Pr[\mathbf{Exp}^{\text{blind}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1 \mid \mathbf{E}^{(\mathrm{II})}] \leq \tfrac{1}{2} - \tfrac{1}{2}\Pr[\mathbf{E}^{(\mathrm{I})}] + \nu^{(\mathrm{II})}(\kappa) \ . \tag{16}$$

Adding Equations (15) and (16), we obtain

$$\begin{aligned}\Pr[\mathbf{Exp}^{\text{blind}}_{\mathcal{A},\,\mathsf{BS}}(\kappa) = 1] &\leq 1 - \tfrac{1}{2}\big(\Pr[\mathbf{E}^{(\mathrm{I})}] + \Pr[\mathbf{E}^{(\mathrm{II})}]\big) + \nu^{(\mathrm{I})}(\kappa) + \nu^{(\mathrm{II})}(\kappa) \\ &= \tfrac{1}{2} + \nu(\kappa) \ ,\end{aligned}$$

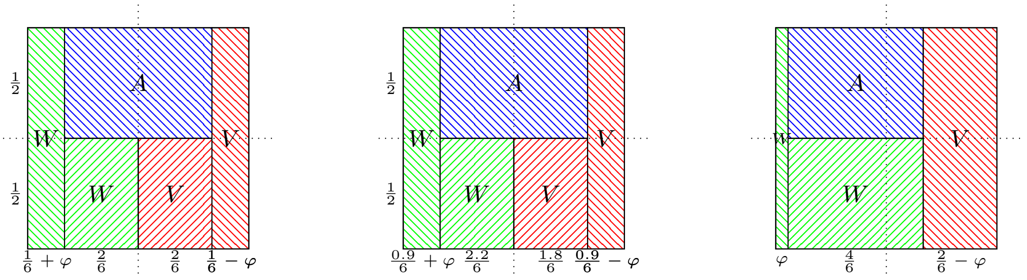
where $\nu(\kappa) \leftarrow \nu^{(\mathrm{I})}(\kappa) + \nu^{(\mathrm{II})}(\kappa)$ is a negligible function. We have thus proved that BS satisfies blindness. □

B.1 On the value of λ

We show that the value of λ cannot be 1 in Claim 3 (as was the case in the proof of the FHS scheme [FHS15]). In this case, the probability of success of the forking experiment $\mathbf{Exp}^{\text{blind-(II)-(0)}}_{\mathcal{A},\,\mathsf{BS}}$ is

$$\frac{1}{2}\Pr[A_1] + \frac{1}{2}\Pr[\neg A_1 \wedge A] + \Pr[\neg A_1 \wedge W].$$

Now consider experiment carried out on the probability spaces described in Figure 3. Figure 3a shows a probability space for which the lower bound just about holds; tipping this probability space by a bit yields a counter-example: Figure 3b; Figure 3c shows the worst counter-example that we could come up with (using the same approach). Amplification, using rewinding and repeated executions, was a *means* for bypassing these counter-examples. The calculations of the success probability are detailed below.



(a) The tipping point

(b) A counter-example

(c) The worst case

Fig. 3: The structure of the probability space for counter-examples for $\lambda = 1$. The x and y axes represent the measures of the spaces $\mathcal{X}$ and $\mathcal{Y}$, respectively. The set of winning coins (W) is shaded in green, the aborting ones (A) in blue, whereas the rest (V) is in red.

1. **The tipping point:** $\frac{1}{2}\cdot\frac{1}{3}+\frac{1}{2}\cdot 2\cdot(\frac{2}{6}\cdot\frac{1}{2}\cdot\frac{1}{2})+(\frac{2}{6}\cdot\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{6}+\varphi)=\frac{6}{12}+\varphi$
2. **A counter example:** $\frac{1}{2}\cdot\frac{1}{3}+\frac{1}{2}\cdot(\frac{2.2}{6}\cdot\frac{1}{2}\cdot\frac{1}{2}+\frac{1.8}{6}\cdot\frac{1}{2}\cdot\frac{1}{2})+(\frac{2.2}{6}\cdot\frac{1}{2}\cdot\frac{1}{2}+\frac{0.9}{6}+\varphi)=\frac{5.9}{12}+\varphi$
3. **The worst case:** $\frac{1}{2}\cdot\frac{1}{3}+\frac{1}{2}\cdot(\frac{4}{6}\cdot\frac{1}{2}\cdot\frac{1}{2})+(\varphi+\frac{4}{6}\cdot\frac{1}{2}\cdot\frac{1}{2})=\frac{5}{12}+\varphi.$

C Proof of Assumption 4

Proof. Let $\mathcal{A}$ be a generic PPT adversary and let $\sigma\colon \mathbb{G}_1 \to \{0,1\}^{m_1}$, $\hat{\sigma}\colon \mathbb{G}_2 \to \{0,1\}^{m_2}$ and $\tau\colon \mathbb{G}_T \to \{0,1\}^{m_T}$ be random encoding functions with w.l.o.g. $m_1 < m_2 < m_T$. $\mathcal{A}$ cannot work directly with group elements, but is forced to work with their image under $\sigma, \hat{\sigma}$ and τ. Furthermore, $\mathcal{A}$ is given oracle access to perform generic bilinear group operations (operations in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ and pairings). Since $\mathcal{A}$ is given access to the group element encodings, it can perform equality checks on its own through string equality tests. At last, we require that $\mathcal{A}$ can only submit already queried encodings to the group oracles. (Note that we can enforce this by choosing m_1, m_2 and m_T large enough making the probability of guessing bitstrings in the image of $\sigma, \hat{\sigma}$ and τ, respectively, negligible.)

Now, let $\mathcal{B}$ be an algorithm interacting with $\mathcal{A}$ as follows. $\mathcal{B}$ picks a random bit b, picks $\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4 \xleftarrow{R} \{0,1\}^{m_1}$ as encodings of $\mathbb{G}_1$ elements and assigns them to the polynomials $1, R, U, UV, (1-b)T + b\cdot RUV$. Likewise, $\mathcal{B}$ picks $\hat{\sigma}_0, \hat{\sigma}_2, \hat{\sigma}_5 \xleftarrow{R} \{0,1\}^{m_2}$ as encodings of $\mathbb{G}_2$ elements and assigns them to the polynomials $1, U, V$.

$\mathcal{B}$ stores $(1, \sigma_0), (R, \sigma_1), (U, \sigma_2), (UV, \sigma_3), ((1-b)T + b\cdot RUV, \sigma_4)$ in a list L_1 and $(1, \hat{\sigma}_0), (U, \hat{\sigma}_2), (V, \hat{\sigma}_5)$ in a list L_2 and gives the respective encodings to $\mathcal{A}$. Furthermore, it initializes a list L_T to manage elements of $\mathbb{G}_T$.

Then, $\mathcal{B}$ simulates the group oracles as follows.

Group action in $\mathbb{G}_1$: Given two bitstrings σ, σ' representing elements in $\mathbb{G}_1$, $\mathcal{B}$ recovers the corresponding polynomials $f, f' \in \mathbb{Z}_p[R,T,U,V]$ and computes $f + f'$. In case L_1 already contains $f + f'$, $\mathcal{B}$ returns its associated bitstring. Otherwise, $\mathcal{B}$ chooses $\sigma \xleftarrow{R} \{0,1\}^{m_1}$, returns σ and stores $(f + f', \sigma)$ in L_1.

Inversion in $\mathbb{G}_1$: Given a bitstring σ representing an element in $\mathbb{G}_1$, $\mathcal{B}$ recovers the corresponding values $f \in \mathbb{Z}_p[R,T,U,V]$ and computes $-f$. In case L_1 already contains $-f$, $\mathcal{B}$ returns its associated bitstring. Otherwise, $\mathcal{B}$ chooses $\sigma' \xleftarrow{R} \{0,1\}^{m_1}$, returns σ' and stores $(-f, \sigma')$ in L_1.

Group action in $\mathbb{G}_2$: Given two bitstrings $\hat{\sigma}, \hat{\sigma}'$ representing elements in $\mathbb{G}_2$, $\mathcal{B}$ recovers the corresponding values $\hat{f}, \hat{f}' \in \mathbb{Z}_p[U,V]$ and computes $\hat{f} + \hat{f}'$. In case L_2 already contains $\hat{f} + \hat{f}'$, $\mathcal{B}$ returns its associated bitstring $\hat{\sigma}$. Otherwise, $\mathcal{B}$ chooses $\hat{\sigma} \xleftarrow{R} \{0,1\}^{m_2}$, returns $\hat{\sigma}$ and stores $(\hat{f} + \hat{f}', \hat{\sigma})$ in L_2.

Inversion in $\mathbb{G}_2$: Given a bitstring $\hat{\sigma}$ representing an element in $\mathbb{G}_2$, $\mathcal{B}$ recovers the corresponding values $\hat{f} \in \mathbb{Z}_p[U,V]$ and computes $-\hat{f}$. In case L_2 already contains $-\hat{f}$, $\mathcal{B}$ returns its associated bitstring $\hat{\sigma}'$. Otherwise, $\mathcal{B}$ chooses $\hat{\sigma}' \xleftarrow{R} \{0,1\}^{m_2}$, returns $\hat{\sigma}'$ and stores $(-\hat{f}, \hat{\sigma}')$ in L_2.

Pairing: Given two bitstrings $\sigma, \hat{\sigma}$ representing elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, $\mathcal{B}$ recovers the corresponding values $f \in \mathbb{Z}_p[R,T,U,V]$ from L_1 and $\hat{f} \in \mathbb{Z}_p[U,V]$ from L_2. In case L_T already contains $f \cdot \hat{f} \in \mathbb{Z}_p[R,T,U,V]$, $\mathcal{B}$ returns its associated bitstring τ. Otherwise, $\mathcal{B}$ chooses $\tau \xleftarrow{R} \{0,1\}^{m_T}$, returns τ and stores $(f \cdot \hat{f}, \tau)$ in L_T.

The group action and inversion oracles for $\mathbb{G}_T$ are simulated analogously to those for $\mathbb{G}_1$ and $\mathbb{G}_2$. Observe that the simulation of all oracles is consistent and thus perfect.

When $\mathcal{A}$ has finished querying the group oracles, $\mathcal{A}$ outputs a bit b^*. Then, $\mathcal{B}$ chooses $r, t, u, v \xleftarrow{R} \mathbb{Z}_p$ and substitutes the formal variables by setting $R \leftarrow r, T \leftarrow t, U \leftarrow u, V \leftarrow v$.

We now prove the following: (1) if the simulation before the substitution was consistent, no information about b was revealed and hence $\mathcal{A}$ can only guess b with probability $1/2$ and (2) the probability for the simulation to be inconsistent after the substitution (i.e., if two distinct polynomials in L_1, L_2 or L_T evaluate to the same value after choosing concrete values for R, T, U, V) is negligible.

For (1) we need to prove that such a collision in L_1, L_2 and L_T cannot be caused by $\mathcal{A}$ itself:

The polynomials contained in L_1 consist of terms in $1, R, U, UV$ and, additionally, of

- terms in T iff $b = 0$;
- terms in RUV iff $b = 1$.

The $\mathbb{G}_1$ group oracles do not change the degree of input polynomials and, thus, do not allow $\mathcal{A}$ to form polynomials containing term RUV out of lower-degree polynomials. Therefore, $\mathcal{A}$ cannot purposely produce collisions in L_1 that reveal bit b.

The substitutions in the formal variables in list L_2 are independent and moreover independent of the choice of b and so $\mathcal{A}$ cannot purposely produce collisions in L_2 that reveal bit b.

The polynomials contained in L_T arise from the multiplication of polynomials in L_1 (having terms in $1, R, U, UV, (1-b)T + bRUV$) and L_2 (having terms in $1, U, V$) using the pairing oracle. The substitutions in the formal variables in list L_T give polynomials having terms in $1, U, V, R, RU, RV, U^2, UV, U^2V, UV^2$ and, additionally having terms in

- T (using $T \in L_1$ and $1 \in L_2$), TU (using $T \in L_1$ and $U \in L_2$) and TV (using $T \in L_1$ and $V \in L_2$) – only if $b = 0$;
- (i) RUV (using $RUV \in L_1$ and $1 \in L_2$),
  (ii) $RU^2V = RUV \cdot U$ (using $RUV \in L_1$ and $U \in L_2$), and
  (iii) $RUV^2 = RUV \cdot V$ (using $RUV \in L_1$ and $V \in L_2$),
  – only if $b = 1$.

As in the other cases, the $\mathbb{G}_T$ group oracles do not allow any further increase of polynomial degrees and the pairing oracle does not allow any further multiplicative combination of terms. Thus, $\mathcal{A}$ cannot purposely produce collisions in L_T that reveal b, i.e., forming polynomials in RUV out of lower-degree terms other than described in (i); polynomials in RU^2V out of lower-degree terms other than described in (ii); and polynomials in RUV^2 out of lower-degree terms other than described in (iii).

What remains to be shown is (2) that the probability of a collision due to the concrete choice of values r, s, t, u is negligible, i.e., that two distinct polynomials in L_1, L_2 and L_T accidentally evaluate to the same value after the substitution (or alternatively that their difference polynomial evaluates to 0). Suppose that $\mathcal{A}$ has issued q queries to the group oracles. Let $|L_1| = O(q)$, $|L_2| = O(q)$ and $|L_T| = O(q)$, then there are $O(\binom{q}{2})$ possibilities of colliding polynomials. Then, by the Schwartz-Zippel lemma and the collision argument, the probability of such an error in the simulation of the generic bilinear group is $O(\frac{q^2}{p})$ and is therefore negligible in the security parameter. □