Round Optimal Blind Signatures

Dominique Schröder
University of Maryland*

Dominique Unruh
Saarland University

May 25, 2011

Abstract. All known round optimal (i.e., two-move) blind signature schemes either need a common reference string, rely on random oracles, or assume the hardness of some interactive assumption. At Eurocrypt 2010, Fischlin and Schröder showed that a broad class of three-move blind signature scheme cannot be instantiated in the standard model based on any non-interactive assumption. This puts forward the question if round optimal blind signature schemes exist in the standard model. Here, we give a positive answer presenting the first round optimal blind signature scheme that is secure in the standard model without any setup assumptions. Our solution does not need interactive assumptions.

1 Introduction

Blind signature schemes [Cha83, Cha84] provide the functionality of a carbon copy envelope: The user (receiver), puts his message into this envelope and hands it over to the signer (sender). The signer in return signs the envelope and gives it back to the user who uses the signed enelope to recover the original message together with a signature on it. The notion of security in this context entails (1) that the signer remains oblivious about the message (blindness), but at the same time, (2) the receiver cannot forge signatures for fresh messages (unforgeability).

Blind signatures are an important primitive, whose classical applications include e-cash, e-voting, and anonymous credentials [Bra00, CG08, BP10]. Moreover, oblivious transfer can be built from *unique* blind signatures [CNS07, FS09]. The several known instantiations of blind signature schemes are based on security assumptions either in the random oracle model [PS00, Abe01, BNPS03, Bol03, AO09, Rüc10], or in the standard model [CKW04, Oka06, HK07, KZ08, AFG+10]. Constructions based on general assumptions are also known [JLO97, Fis06, HKKL07, FS09]. Recently, Katz, Schröder, and Yerukhimovich show that blind signature scheme cannot be build in a black-box way from one-way trapdoor permutations [KSY11].

Although many blind signature schemes are known, all round optimal solutions (the user sends a single message to the signer and gets a single response) rely either on the random oracle heuristic [Cha84, Bol03], or they require a common reference string [Fis06, AFG+10, GS10, MSF10], and some instantiations even prove their security under an interactive assumption [BNPS03, Bol03, GS10]. Recently, at Eurocrypt 2010, Fischlin and Schröder give a (partial) answer to the question why the construction of round optimal blind signatures without any setup assumption is very difficult [FS10]. In fact, the author show that three-move blind signature schemes with signature-derivation checks cannot be build from any non-interactive assumption in the standard model. A signature derivation-checks is a publicly verifiable test if the user is able to derive a valid signature or not. Interestingly, most of the round optimal blind signature schemes known today have

*Supported by a DAAD postdoctoral fellowshi.

this property [Cha84, Bol03, Fis06]. In particular, this means that there is no much hope to instantiate one of the known schemes under weaker assumptions.

Concurrently Secure Blind Signature Schemes Another reason why round optimal blind signature schemes are desirable is that a solution would be concurrently secure. Concurrently secure blind signature schemes, however, are difficult to obtain. Juels, Luby, and Ostrovsky [JLO97] explained why a straight forward approach does not work. The authors then present a solution that is, according to Hazay et al. [HKKL07], only secure in the sequential setting. The reason is that the solution seems to require a *concurrently secure* protocol for two-party computation. Such a protocol, however, is a mayor open problem in the standard model [HKKL07].

Obtaining a concurrently secure protocol under simulation-based definition via black-box proof is impossible as shown by Lindell [Lin03]. Previous protocols overcome this impossibility result by assuming a common reference string and by relying on game-based definitions. The only exception is the protocol of Hazay et al. [HKKL07] that does not need a CRS. The authors build a blind signature scheme that uses the concurrent zero-knowledge protocol of Prabhakaran, Rosen, and Sahai [PRS02] that has a logarithmically round complexity as a building block.

1.1 Our Contribution

Our main contribution is the first round optimal blind signature scheme in the standard. In contrast to prior schemes, our solution does not need any setup assumption such as a common reference string. Our construction is based on standard cryptographic assumptions and its security is not based on interactive assumption. Our solution can be considered interesting for at least the following reasons:

- Our construction is the first construction in the standard model that consists of only two moves.
- The scheme shows how to bypass the impossibility result of Fischlin and Schröder from Eurocrypt 2010 [FS10]. This is achieved by 1) building a scheme *without* signature-derivation checks and 2) using non black-box techniques.
- Our solution shades light onto build concurrently secure 2-party protocols. In particular, it shows that the known impossibility results for concurrently 2-party computation [Lin03, Lin04] can be bypassed by considering specific functionalities.

Our blind signature scheme is based on general assumption and can be instantiated under the assumption that exponential hard one-way functions, certified trapdoor permutations, exists and that the DDH assumption holds.

Notations. Before presenting our results we briefly recall some basic definitions. In what follows we denote by $\lambda \in \mathbb{N}$ the security parameter. We say that a function is *negligible* if it vanishes faster than the inverse of any polynomial. A function is non-negligible if it is not negligible. If S is a set, then $x \xleftarrow{\$} S$ indicates that x is chosen uniformly at random over S (which in particular assumes that S can be sampled efficiently). We write $A(x; X)$ to indicate that A is an algorithm that takes as input a value x and uses randomness X. In general, we use capital letters for the randomness. W.l.o.g. we assume that X has bit length λ.

2 Blind Signatures and Their Security

To define blind signatures formally we introduce the following notation for interactive executions between algorithms $\mathcal{X}$ and $\mathcal{Y}$. By $(a, b) \leftarrow \langle \mathcal{X}(x), \mathcal{Y}(y) \rangle$ we denote the joint execution of $\mathcal{X}$ and $\mathcal{Y}$, where x is the

private input of $\mathcal{X}$ and y defines the private input of $\mathcal{Y}$. The private output of $\mathcal{X}$ equals a and the private output o $\mathcal{Y}$ is b.

Definition 2.1 *A* blind signature scheme BS *consists of PPT algorithms* Gen, Vrfy *along with interactive PPT algorithms* $\mathcal{S}$,$\mathcal{U}$ *such that for any* $\lambda \in \mathbb{N}$*:*

- $\mathsf{Gen}(1^\lambda)$ *generates a key pair* (sk, vk).
- *The joint execution of* $\mathcal{S}(sk)$ *and* $\mathcal{U}(vk, m)$*, where* $m \in \{0,1\}^\lambda$*, generates an output* σ *for the user and no output for the signer. We write this as* $(\perp, \sigma) \leftarrow \langle \mathcal{S}(sk), \mathcal{U}(vk, m) \rangle$.
- *Algorithm* $\mathsf{Vrfy}(vk, m, \sigma)$ *outputs a bit* b.

We assume completeness *i.e., for any* $m \in \{0,1\}^\lambda$*, and for* $(sk, vk) \leftarrow \mathsf{Gen}(1^\lambda)$*, and* σ *output by* $\mathcal{U}$ *in the joint execution of* $\mathcal{S}(sk)$ *and* $\mathcal{U}(vk, m)$*, it holds that* $\mathsf{Vrfy}(vk, m, \sigma) = 1$ *with overwhelming probability in* $\lambda \in \mathbb{N}$.

Note that it is always possible to sign messages of arbitrary length by applying a collision-resistant hash function to the message prior to signing.

Blind signatures must satisfy two properties: unforgeability and blindness [JLO97, PS00]. For unforgeability we require that a user who runs k executions of the signature-issuing protocol should be unable to output $k+1$ valid signatures on $k+1$ distinct messages.

Definition 2.2 *Blind signature scheme* $\mathsf{BS} = (\mathsf{Gen}, \mathcal{S}, \mathcal{U}, \mathsf{Vrfy})$ *is* unforgeable *if for any polynomial* ℓ*, the success probability of any PPT algorithm* $\mathcal{U}^*$ *in the following game is negligible (in* λ*):*

- $\mathsf{Gen}(1^\lambda)$ *outputs* (ssk, svk)*, and* $\mathcal{U}^*$ *is given* svk.
- $\mathcal{U}^*(svk)$ *interacts concurrently with* ℓ *instances* $\mathcal{S}^1_{ssk}, \ldots, \mathcal{S}^\ell_{ssk}$.
- $\mathcal{U}^*$ *outputs* $(m_1, \sigma_1, \ldots, m_{\ell+1}, \sigma_{\ell+1})$.

$\mathcal{U}^*$ *succeeds if the* $\{m_i\}$ *are distinct and* $\mathsf{Vrfy}(svk, m_i, \sigma_i) = 1$ *for all* i.

The blindness condition says that it should be infeasible for any a malicious signer $\mathcal{S}^*$ to decide which of two messages m_0 and m_1 has been signed first in two executions with an honest user $\mathcal{U}$. This condition must hold, even if $\mathcal{S}^*$ is allowed to choose the public key maliciously [ANN06]. If one of these executions has returned $\perp$ then the signer is not informed about the other signature either.

Definition 2.3 *Blind signature scheme* $\mathsf{BS} = (\mathsf{Gen}, \mathcal{S}, \mathcal{U}, \mathsf{Vrfy})$ *satisfies* blindness *if the advantage for any PPT algorithm* $\mathcal{S}^*$ *in the following game is negligible (as a function of* λ*):*

1. $\mathcal{S}^*$ *outputs an arbitrary public key* svk *along with two messages* m_0, m_1.
2. *A random bit* b *is chosen, and* $\mathcal{S}^*$ *interacts concurrently with* $\mathcal{U}_b := \mathcal{U}(svk, m_b)$ *and* $\mathcal{U}_{\bar{b}} := \mathcal{U}(svk, m_{\bar{b}})$*. When* $\mathcal{U}_b, \mathcal{U}_{\bar{b}}$ *have completed their executions,* $\sigma_b, \sigma_{\bar{b}}$ *are defined as follows:*
   - *If either* $\mathcal{U}_b$ *or* $\mathcal{U}_{\bar{b}}$ *abort, then* $(\sigma_b, \sigma_{\bar{b}}) := (\perp, \perp)$.
   - *Otherwise, let* σ_0 *(resp.* σ_1*) be the output of* $\mathcal{U}_0$ *(resp.* $\mathcal{U}_1$*).*

   $\mathcal{S}^*$ *is given* (σ_0, σ_1).
3. *Finally,* $\mathcal{S}^*$ *outputs a bit* b'.

$\mathcal{S}^*$ *succeeds (denoted* succ*) if* $b' = b$*. The advantage of* $\mathcal{S}^*$ *is* $|\operatorname{Prob}[\mathsf{succ}] - \frac{1}{2}|$.

A blind signature scheme is secure if it is unforgeable and blind.

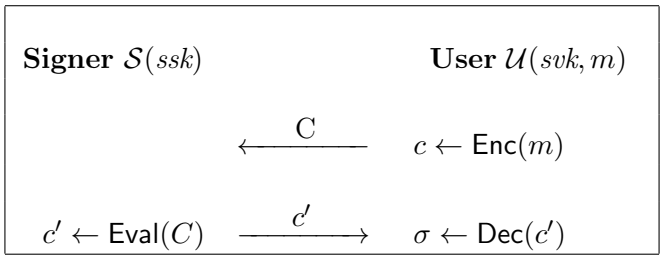

Figure 1: Underlying idea of the signature issue protocol.

3 Towards a Secure Construction

The high-level idea of our construction is as follows (Figure 1 shows a simplified version of the signature issue protocol). The user first encrypts the message using a fully homomorphic encryption scheme and sends the ciphertext to the signer. The signer, in return, evaluates the signing circuit on the ciphertext and sends the result back. To recover the signature, the user simply decrypts the ciphertext. The basic idea of the protocol follows the (well known) approach of building secure two-party computation from a fully homomorphic encryption scheme. The resulting protocol, however, is only secure in the semi-honest setting. In the context of blind signatures we are interested in stronger security guarantees and now we describe which additional steps are required to obtain a fully secure blind signature scheme.

Key Generation. The first observation is that the user must generate the keys for the fully homomorphic encryption scheme, or the scheme cannot be blind. But if the user generates the key, then the scheme might be forgeable. The reason is that the forger might generate fake keys that may leak some parts of the circuit and thus of the signer's private key. To handle this issue we let the user append a proof that the keys are generated honestly. This proof, however, must not reveal any information about the decryption key nor about the encrypted message. The obvious way to handle this problem would be a non-interactive zero-knowledge proof (NIZK). Yet, since NIZKs (except in the ROM) require a common reference string, they are not applicable in our setting. Instead we rely on two-round witness-indistinguishable proofs, called ZAPs. These proofs have the interesting property that the first message can be fixed once and for all and used for several proofs. This property helps us preserve the round complexity by storing the first move of the ZAP in the public key. ZAPs, however, are "only" witness indistinguishable and not zero-knowledge. Therefore, we include as a second witness a pre-image of a one-way function (the image is stored in the public key). The ZAP then proves that the user either generated the key honestly and encrypted the message honestly, or that it knows the a pre-image of a one-way function.

Signing. The signer then validates the proof and is supposed to run the evaluation algorithm honestly using the right private key, or blindness might be violated. In particular, consider an adversary that first uses ssk_0 and afterwards ssk_1 as a signing key and that otherwise follows the protocol honestly. The attacker would receive both signatures and could easily break blindness. In order to guarantee that the signer computes all steps honestly, we let the signer append a second ZAP. This ZAP then proves that it "signed" the contained message honestly using the right private key. Again, since the ZAP is only witness-indistinguishable, we use as a second witness a second pre-image of a one-way function. The first message of the ZAP and the image of the one-way function for this proof is part of the user's first protocol message. Again, the round complexity is preserved.

Achieving Unforgeability. To show that the protocol is unforgeable, several more modifications are necessary.

The overall idea is to reduce the unforgeability to the unforgeability of the underlying signature scheme. To do so, we construct an adversary $\mathcal{B}$ against the unforgeability of the signature scheme that simulates the protocol execution for the forger of the blind signature scheme. The difficulty in this proof is that $\mathcal{B}$ has to submit a "real" message to its external signing oracle and hence needs to find out which message is contained in the ciphertext sent by the user. Since ZAPs are only witness-indistinguishable (and no proof of knowledge) the extraction of the message from the ZAP is not possible. We solve this issue by applying a complexity leveraging argument. Loosely speaking, this technique says that some primitive A cannot be broken in polynomial time but can be broken in time $T(\lambda)$ for some super-polynomial function T, while a second primitive B cannot be broken in time $T(\lambda)$. Concretely, we assume that the signature scheme is unforgeable w.r.t. time T_2 and our attacker $\mathcal{B}$ runs in time $T_1 < T_2$. In the protocol, we let the user commit to the message (in addition to the encryption) using a commitment scheme that it extractable in time T_1. Our attacker $\mathcal{B}$ then extract the message from the commitment and sends it to the signing oracle and encrypts the obtained signature. In this step, we need an additional property of the fully homomorphic encryption scheme that is called circuit privacy. Roughly speaking, this property says that it is not possible to distinguish between a ciphertext that has been computed by applying the evaluation algorithm to the ciphertext, or by applying the circuit to the message and then encrypting the result.

Achieving Blindness. The above-mentioned modifications are not yet sufficient to achieve blindness. Recall that blindness means that the malicious signer cannot distinguish the order of two signature issue protocols. In order to formally prove blindness, we have to show that the transcript (i.e., the messages exchanged between the signer and the user) is computationally independent of the message to be signed. We achieve this in two main steps. First, we let the signer commit to its private key. Second, we apply another complexity leveraging argument to extract the private key and the pre-image out of the commitments. Recall that the ZAP from the user to the signer proves that he has encrypted the messages honestly, or that he know the pre-image of a one-way function. Since we now know the second witness, we let the user send an encryption of an all zero string to the malicious signer. Since the fully homomorphic encryption is IND-CPA it follows that this modification does not change the success probability of the adversary. In the last step of the proof, we let the user sign its message locally with the previously extracted private key. Since the transcript is now independent of the message, it follows that the scheme is blind.

4 Needed Primitives

Before presenting our generic construction, we review the required primitives.

One-Way Functions. The standard notion of one-wayness of functions is defined as follows. Let $\mathcal{A}$ be an adversary and define OW-advantage for a function $f : \{0,1\}^\lambda \mapsto \{0,1\}^\lambda$ as

$$\mathbf{Adv}^{ow}_{f,\mathcal{A}}(\lambda) = \Pr\left[\ f(z) = y : x \leftarrow \{0,1\}^\lambda\ ;\ y \leftarrow f(x)\ ;\ z \leftarrow \mathcal{A}(y)\ \right]\ .$$

Definition 4.1 *A function f is T-*one-way *if $\mathbf{Adv}^{ow}_{f,\mathcal{A}}$ is negligible for any PPT algorithm $\mathcal{A}$ running in time $T \cdot poly(\lambda)$.*

We need in our proofs that the function is invertible after a certain time.

Definition 4.2 *A function $f : \{0,1\}^\lambda \mapsto \{0,1\}^\lambda$ is* invertible *in time T, if there exists an algorithm $\mathcal{A}$ that gets as input an image $y \leftarrow f(x)$, with $x \in \{0,1\}^\lambda$, runs in time $T \cdot poly(\lambda)$, and outputs x' such that $x' = x$ with overwhelming probability.*

Moreover, we assume that f has efficiently decidable images. That is, for all values $y \in \{0,1\}^\lambda$ there exists a PPT algorithm $\mathcal{A}$ that outputs 1 iff y is an image of f with overwhelming probability. We write this as $y \in \mathsf{image}(f)$.

Pseudorandom Functions. Loosely speaking, a function f is pseudorandom if no PPT adversary can distinguish it from a random function. More precisely, a function $F_R : \{0,1\}^\lambda \mapsto \{0,1\}^\lambda$ is T-pseudorandom if for all adversaries $\mathcal{A}$ running in time $T \cdot poly(\lambda)$ there exists a negligible function $\mathsf{negl}(\lambda)$ such that

$$\left|\mathrm{Prob}\left[\mathcal{A}^{F_R(\cdot)}(1^\lambda) = 1\right] - \mathrm{Prob}\left[\mathcal{A}^{f(\cdot)}(1^\lambda) = 1\right]\right| = \mathsf{negl}(\lambda),$$

where $R \leftarrow \{0,1\}^\lambda$ is chosen uniformly at random and f is chosen uniformly at random from the set of functions mapping λ-bit strings to λ-bit strings.

Non-interactive Commitment Scheme. A commitment scheme consists of a pair of efficient algorithms $\mathcal{C} = (\mathsf{Com}, \mathsf{Open})$ where: Com takes as input $m \in \{0,1\}^\lambda$ and outputs $(\mathsf{decom}, \mathsf{com}) \leftarrow \mathsf{Com}(m)$, where decom and com are both of length $\{0,1\}^\lambda$; the algorithm $\mathsf{Open}(\mathsf{decom}, \mathsf{com})$ outputs a message m or $\perp$ if c is not a valid commitment to any message.

It is assumed that the commitment scheme is complete, i.e., for any message $m \in \{0,1\}^\lambda$ and $(\mathsf{decom}, \mathsf{com}) \leftarrow \mathsf{Com}(ck, m)$, we have $\mathsf{Open}(ck, \mathsf{decom}, \mathsf{Com}(ck, m)) = m$ with overwhelming probability in $\lambda \in \mathbb{N}$.

Commitment schemes must satisfy two properties: hiding and binding. Hinding means that no adversary can distinguish which of two messages are locked in the commitment. Let $\mathcal{A}$ be a non-uniform adversary against $\mathcal{C}$ and define its hiding-advantage as

$$\mathbf{Adv}^{\mathrm{hid}}_{\mathcal{C},\mathcal{A}}(\lambda) = 2 \cdot \Pr\left[b = b' \;\middle|\; \begin{array}{l}(m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}(1^\lambda); b \leftarrow \{0,1\}; \\ (\mathsf{decom}, \mathsf{com}) \leftarrow \mathsf{Com}(m_b); b' \leftarrow \mathcal{A}(\mathsf{com}, \mathsf{st})\end{array}\right] - 1\ .$$

Definition 4.3 *$\mathcal{C}$ is T-*hiding *if the advantage function $\mathbf{Adv}^{hid}_{\mathcal{C},\mathcal{A}}$ is a negligible function for all non-uniform adversaries $\mathcal{A}$ running in time $T \cdot poly(\lambda)$.*

Binding says that the adversary cannot open the commitment in two different ways. Here, we define the strongest variant known as perfectly binding.

Definition 4.4 *$\mathcal{C}$ is* perfectly binding *if there exist no values $(\mathsf{com}, m_0, m_1, \mathsf{decom}_0, \mathsf{decom}_1)$ with $m_0 \neq m_1$ such that $\mathsf{Open}(\mathsf{com}, \mathsf{decom}_0) = m_0$ and $\mathsf{Open}(\mathsf{com}, \mathsf{decom}_1) = m_1$.*

In addition to these requirements we assume that the commitment scheme is extractable in superpolynomial time T, i.e., there exists an algorithm that gets as input a commitment and outputs the contained message. More formally:

Definition 4.5 *A commitment scheme $\mathcal{C}$ is* extractable *in time T,if there exists an algorithm $\mathcal{A}$ running in time $T \cdot poly(\lambda)$ such that for any $\mathsf{com}, \mathsf{decom}$ with $\mathsf{Open}(\mathsf{com}, \mathsf{decom}) = m \neq \perp$, we have $\mathcal{A}(\mathsf{com}) = m$ with overwhelming probability.*

Signature Scheme. A signature scheme $\mathsf{Sig} = (\mathsf{SigGen}, \mathsf{Sign}, \mathsf{SigVrfy})$ is a tuple of algorithms: $\mathsf{SigGen}(1^\lambda)$ outputs a key-pair (ssk, svk); the algorithm $\mathsf{Sign}(ssk, m)$ takes as input a signing key ssk, a message $m \in \{0,1\}^\lambda$ and outputs signature σ; the verification algorithm $\mathsf{SigVrfy}(svk, m, \sigma)$ outputs 1 iff σ is a signature on m under svk. We assume completeness i.e., for any message $m \in \{0,1\}^\lambda$, and key pair $(ssk, svk) \leftarrow \mathsf{SigGen}(1^\lambda)$ and $\sigma \leftarrow \mathsf{Sign}(ssk, m)$ we have $\mathsf{SigVrfy}(svk, m, \sigma) = 1$ with overwhelming probability in $\lambda \in \mathbb{N}$. The security of signature schemes is proven against existential forgery under adaptive chosen message attacks (EU-CMA) [GMR88]. Let $\mathcal{A}$ be an adversary against Sig and define its $\mathsf{eu\text{-}cma}$-advantage as

$$\mathbf{Adv}^{cma}_{\mathsf{Sig},\mathcal{A}}(\lambda) = \Pr\left[\ \mathsf{SigVrfy}(svk, m^*, \sigma^*) = 1 : (ssk, svk) \leftarrow \mathsf{SigGen}(1^\lambda); (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(ssk,\cdot)}(svk)\ \right] .$$

The adversary $\mathcal{A}$ is not allowed to query $\mathsf{Sign}(ssk, \cdot)$ about m^*.

Definition 4.6 Sig *is* T-$\mathsf{eu\text{-}cma\text{-}secure}$ *if the advantage function* $\mathbf{Adv}^{cma}_{\mathsf{Sig},\mathcal{A}}$ *is a negligible function in* λ *for all adversaries* $\mathcal{A}$ *running in time* $T \cdot poly(\lambda)$.

ZAP. A ZAP is a 2-round witness-indistinguishable proof [DN07] (with negligible soundness error) with the useful property that the first round (a message from verifier $\mathcal{V}$ to prover $\mathcal{P}$) can be made universal for all executions and therefore be part of the public key of $\mathcal{V}$. More formally: Let $L_{p(\lambda)} := L \cap \{0,1\}^{\leq p(\lambda)}$ for some polynomial p. A ZAP is 2-round public coin witness-indistinguishable protocol for some $\mathcal{NP}$-language L with associated relation R_L. It consists of two efficient interactive algorithms $\mathcal{P}, \mathcal{V}$ such that:

- The verifier $\mathcal{V}(1^\lambda)$ outputs an initial message msg;
- The prover $\mathcal{P}(1^\lambda, \mathsf{msg}, w)$ gets as input msg, a statement $s \in L_{p(\lambda)}$, and a witness w such that $(s, w) \in R_L$; it outputs a proof π;
- The verifier $\mathcal{V}(\mathsf{msg}, s, \pi)$ outputs a decision bit b.

A ZAP is complete if for any $(s, w) \in R_L$, we have $\mathcal{V}(\mathsf{msg}, s, \mathcal{P}(\mathsf{msg}, s, w)) = 1$ with overwhelming probability. ZAPs must satisfy adaptive soundness and witness indistinguishability.

Definition 4.7 *A ZAP satisfies* $\mathsf{adaptive\ soundness}$ *if for any (unbounded) algorithm* $\mathcal{P}^*$ *the following is negligible:*

$$\Pr\left[\mathsf{msg} \leftarrow \mathcal{V}(1^\lambda); (s, \pi) \leftarrow \mathcal{P}^*(\mathsf{msg}) : \mathcal{V}(\mathsf{msg}, s, \pi) = 1 \bigwedge s \notin L\right]$$

Definition 4.8 *A ZAP is non-uniform computationally* $\mathsf{witness\ indistinguishable}$ *if the advantage of any non-uniform PPT adversary* $\mathcal{A}$ *in the following game is negligible:*

1. $\mathcal{A}(1^\lambda)$ *outputs a string* msg*, a sequence* $s_1, \ldots, s_\ell \in L_{p(\lambda)}$*, and two sequences* $w_1^0, \ldots, w_\ell^0$ *and* $w_1^1, \ldots, w_\ell^1$*. It is required that* $(s_i, w_i^0), (s_i, w_i^1) \in R_L$ *for all* i.
2. *A random bit* b *is chosen.*
3. *Compute* $\pi_i \leftarrow \mathcal{P}(1^\lambda, \mathsf{msg}, s_i, w_i^b)$ *for all* i*, and give these to* $\mathcal{A}$.
4. $\mathcal{A}$ *outputs a bit* b'*. The advantage of* $\mathcal{A}$ *is* $|\operatorname{Prob}[b = b'] - \frac{1}{2}|$.

Dwork and Naor showed that ZAPs can be build upon any certified trapdoor permutation [DN07].

Size-Dependent Homomorphic PKE. [BHHI10] Roughly speaking, a size-dependent homomorphic public-key encryption scheme is a fully homomorphic encryption scheme with the relaxation that the ciphertext may grow. More precisely, a size-dependent homomorphic public-key encryption scheme $\mathsf{PKE} = (\mathsf{EncGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ consists of a key generation algorithm $(ek, dk) \leftarrow \mathsf{EncGen}(1^\lambda)$; an encryption algorithm $c \leftarrow \mathsf{Enc}(ek, m)$ that, upon input a public key ek and a message m, outputs a ciphertext c; a decryption algorithm $m \leftarrow \mathsf{Dec}(dk, c)$ that, upon input the private key and a ciphertext c, returns the message m. The algorithm Eval takes as input a public key ek, a circuit C, and a ciphertext c and outputs another ciphertext c'.

The scheme $\mathsf{PKE} = (\mathsf{EncGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ is perfectly correct for a given circuit C if, for any plaintext m, and key-pair $(ek, dk) \leftarrow \mathsf{EncGen}(1^\lambda)$, and ciphertext c with $c \leftarrow \mathsf{Enc}(ek, m)$ it is the case that $\mathsf{Dec}(dk, \mathsf{Eval}(ek, C, c)) = C(m)$ with probability 1.

Now, we define weak function-privacy [BHHI10]. This property says that the adversary cannot distinguish which circuit has been used for the evaluation as long as the output of two circuits are the same (even if the adversary knows the private decryption key). More formally, we say that PKE is non-uniformly computationally weak function-private for all $m \in \{0,1\}^\lambda$, all circuits C_1, C_2 with $|C_1| = |C_2|$ and $C_1(m) = C_2(m)$, all (ek, dk) in the range of $\mathsf{EncGen}(1^\lambda)$, and all c in the range of $\mathsf{Enc}(ek, m)$, we have that $\mathsf{Eval}(ek, C_1, c)$ and $\mathsf{Eval}(ek, C_2, c)$ are non-uniformly computationally indistinguishable.[1]

We define CPA security as usual. Let $\mathcal{A}$ be an adversary against PKE and define its IND-CPA-advantage as

$$\mathbf{Adv}^{cpa}_{\mathsf{PKE},\mathcal{A}}(\lambda) = 2 \cdot \Pr\left[b = b' \;\middle|\; \begin{array}{l} (dk, ek) \leftarrow \mathsf{EncGen}(1^\lambda); b \leftarrow \{0,1\}; (m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}(ek); \\ c^* \leftarrow \mathsf{Enc}(ek, m_b); b' \leftarrow \mathcal{A}(c^*, \mathsf{st}) \end{array} \right] - 1 \,.$$

We require that $|m_0| = |m_1|$ and st is some arbitrary state information.

Definition 4.9 (IND-CPA) PKE *is* IND-CPA secure *if the advantage function* $\mathcal{A}^{cpa}_{\mathsf{PKE},\mathcal{A}}$ *is a negligible function in* λ *for all non-uniform computational adversaries* $\mathcal{A}$.

Overview About the Primitives. Fix two superpolynomial functions T_1 and T_2 such that $T_2 > T_1$. In our construction, we assume two one-way functions f^s and f^u, a pseudorandom function F, two commitment schemes $\mathcal{C}^M, \mathcal{C}^R$, a signature scheme Sig, two ZAPs Z^s, Z^u, and a size-dependent encryption scheme Enc. We will assume that these schemes satisfy the following conditions:

Condition 1. For the correctness we assume that Sig is complete; Enc is correct; $\mathcal{C}^M$ and $\mathcal{C}^R$ are complete; Z^s and Z^u are complete.

Condition 2. For the proof of unforgeability we assume that

- f^s is T_2-one-way;
- f^u is invertible in time T_2 and has efficiently decidable images;
- F is a T_2-pseudorandom function;
- Enc is non-uniformly computationally weak function-private;
- Sig is T_2 unforgeable;
- $\mathcal{C}^M$ is non-uniformly hiding, perfectly binding, and extractable in time T_1;
- $\mathcal{C}^R$ is T_2-hiding, perfectly binding;
- ZAP Z^s is adaptively sound;

[1] Our definition deviates from that in [BHHI10]: First, our definition is computational while theirs is statistical. Second, we consider even maliciously constructed ciphertexts c as long as they are in the range of $\mathsf{Enc}(ek, m)$ while they consider honestly generated ciphertexts $c = \mathsf{Enc}(ek, m)$. (I.e., we consider the case where the randomness is chosen maliciously.)

- ZAP Z^u is non-uniformly computationally witness-indistinguishable.

Condition 3. For the proof of blindness we assume that

- f^s has efficiently decidable images;
- f^u is T_1-oneway;
- Enc is perfectly correct and non-uniformly IND-CPA secure;
- $\mathcal{C}^M$ is extractable in time T_1 and non-uniformly hiding;
- $\mathcal{C}^R$ is perfectly binding;
- ZAP Z^s is non-uniformly computationally witness-indistinguishable;
- ZAP Z^u is adaptively sound.

Instantiability. In what follows, we discuss which standard assumptions Condition 1,2, and 3 can be instantiated. Firstly, to instantiate f^s, f^u we need to assume that exponential hard one-way functions exist. The perfectly binding commitment schemes $\mathcal{C}^M, \mathcal{C}^R$ can be build from any one-way permutation. Signature scheme exist under the assumption that one-way function exist. The size-dependent homomorphic public-key encryption scheme can be instantiate under the DDH assumption [BHHI10]. We stress that this is a strictly weaker assumption than the existence of a fully homomorphic encryption scheme. ZAPs can be build from any certified trapdoor permutation [DN07].

5 Construction and Security Proofs

In this section, we define our construction and show that it is unforgeable and blind.

5.1 Construction

We define our blind signature scheme through the following algorithms:

Key Generation. $\mathsf{Gen}(1^\lambda)$ peforms the following steps:

- $R, S, T \leftarrow \{0,1\}^\lambda$
- $(ssk, svk) \leftarrow \mathsf{SigGen}(1^\lambda; S)$
- $x^s \leftarrow \{0,1\}^\lambda$, $y^s \leftarrow f^s(x^s)$
- $\mathsf{msg}^s \leftarrow \mathcal{V}^s(1^\lambda)$
- $\mathsf{com}^R \leftarrow \mathsf{Com}^R((R, ssk); T)$
- set $sk \leftarrow (svk, ssk, R, S, T)$ and $vk \leftarrow (svk, y^s, \mathsf{msg}^s, \mathsf{com}^R)$

Signing. The protocol for $\mathcal{U}$ to obtain a signature on message m is as follows:

- If $y^s \notin \mathsf{image}(f^s)$, $\mathcal{U}$ aborts.
- $\mathcal{U}$ picks four random values K, E, M, X^u each of bit length λ. It generates a key-pair of the encryption scheme $(ek, dk) \leftarrow \mathsf{EncGen}(1^\lambda; K)$, encrypts the message $c \leftarrow \mathsf{Enc}(ek, m; E)$, and commits to the message $\mathsf{com}^m \leftarrow \mathsf{Com}^M(m; M)$. It then computes $\mathsf{com}^{x^u} \leftarrow \mathsf{Com}^M(0^\lambda; X^u)$ and a proof π^s (with respect to msg^s) for the ZAP Z^s that $(y^s, ek, c, \mathsf{com}^m, \mathsf{com}^{x^u}) \in L^s$, where L^s contains tuples for which there exists either a witness $\omega_1^s = (K, E, M, m, dk)$ such that

$$(dk, ek) = \mathsf{EncGen}(1^\lambda; K) \bigwedge c = \mathsf{Enc}(ek, m; E) \bigwedge \mathsf{com}^m = \mathsf{Com}^M(m; M)$$

or there exists a witness $\omega_2^s = (x^s, X^u)$ such that

$$\mathsf{com}^{x^u} = \mathsf{Com}^M(x^s; X^u) \bigwedge f^s(x^s) = y^s.$$

Notice that in L^s, inside com^{x^u} we have the value x^s. This is due to the fact that com^{x^u} is the commitment produced by $\mathcal{U}$ which is supposed to show that $\mathcal{U}$ knows the value x^s produced by $\mathcal{S}$.

- $\mathcal{U}$ generates the challenge for the ZAP Z^u. It picks $x^u \leftarrow \{0,1\}^\lambda$ uniformly at random, sets $y^u \leftarrow f^u(x^u)$, and computes the first message of the ZAP Z^u as $\mathsf{msg}^u \leftarrow \mathcal{V}^u(1^\lambda)$. It then sends $(ek, c, \pi^s, \mathsf{com}^m, \mathsf{com}^{x^u}, \mathsf{msg}^u, y^u)$ to $\mathcal{S}$.
- $\mathcal{S}$ receives $(ek, c, \pi^s, \mathsf{com}^m, \mathsf{com}^{x^u}, \mathsf{msg}^u, y^u)$ from the user; it first verifies that π^s is a valid proof (with respect to msg^s) $(y^s, ek, c, \mathsf{com}^m, \mathsf{com}^{x^u}) \in L^s$ and that y^u is a valid image of f^u. If either of the checks fail, $\mathcal{S}$ aborts. Let $C := C_{ssk,R}(m)$ be the circuit computing $\mathsf{Sign}(ssk, m; F_R(m))$. Otherwise, if both condition hold, then $\mathcal{S}$ picks two random values V, X^s each of bit length λ and it signs the message contained in c by running $c' \leftarrow \mathsf{Eval}(ek, C, c; V)$ and computes the commitment $\mathsf{com}^{x^s} \leftarrow \mathsf{Com}^M(0^\lambda; X^s)$. It then computes a proof π^u (with respect to msg^u) for the statement $(svk, \mathsf{com}^R, c, c', ek, \mathsf{com}^{x^s}, y^u) \in L^u$, where L^u contains tuples for which there exists either a witness $\omega_1^u = (R, S, T, V, ssk)$ such that:

$$c' = \mathsf{Eval}(ek, C_R, c; V) \text{ with } C_{ssk,R} := \mathsf{Sign}(ssk, m; F_R(m)) \bigwedge$$
$$\mathsf{com}^R = \mathsf{Com}^R((R, ssk); T) \bigwedge (ssk, svk) = \mathsf{SigGen}(1^\lambda; S)$$

or there exists a witness $\omega_2^u = (x^u, X^s)$ such that

$$\mathsf{com}^{x^s} = \mathsf{Com}^M(x^u; X^s) \bigwedge f^u(x^u) = y^u.$$

$\mathcal{S}$ then sends $(c', \pi^u, \mathsf{com}^{x^s})$ to $\mathcal{U}$.

- $\mathcal{U}$ verifies that π^u is a valid proof (with respect to msg^u) w.r.t. the ZAP Z^u for the statement $(svk, \mathsf{com}^R, C, c, c', ek, \mathsf{com}^{x^s}, y^u) \in L^u$. If this proof fails, then $\mathcal{U}$ aborts. Otherwise, it computes the signature $\sigma \leftarrow \mathsf{Dec}(dk, c')$ and outputs σ.

Verification. $\mathsf{Vrfy}(vk, \sigma, m)$ returns $\mathsf{SigVrfy}(svk, \sigma, m)$.

5.2 Security Proofs

We show that the above defined construction is complete, unforgeable, and blind. Within all proofs, we assume that $T_1 < T_2$.

Proof of Unforgeability. The proof idea is the following. We start with a game that corresponds to the unforgeability game of blind signatures and we then gradually change this game such that at the end we can build an adversary against the unforgeability of the underlying signature scheme. The main steps of the proof are the following:

- We apply a complexity leveraging argument. This technique allows us to invert the one-way function f^u and also to extract the message m out of the second commitment com^m.
- We use the external signing oracle in the unforgeability game of the underlying signature scheme to sign the message m.

Figure 2: Issue protocol of the two move blind signature scheme.

- Instead of applying the evaluation algorithm Eval, we directly encrypt the obtained signature using the size-dependent homomorphic encryption scheme. These modifications do not change the success probability of the adversary (against the unforgeability of the blind signature scheme) because:
  - the size-dependent homomorphic encryption scheme is weakly function-private and thus, the attacker cannot tell the difference;
  - the ZAP remains valid as it now uses the previously computed preimage x^u of f^u as a witness.

Theorem 5.1 *Suppose that f^s, f^u, and F are function, $\mathcal{C}^M, \mathcal{C}^R$ two commitment schemes, Sig a signature scheme, Z^s, Z^u two ZAPs, and Enc size-dependent encryption scheme such that all primitives satisfy Condition 1. Then the blind signature scheme as defined in Section 5.1 is unforgeable.*

Proof. Assume towards contradiction that the above construction is not unforgeable. Then, there exists a PPT algorithm $\mathcal{U}^*$ that outputs $(\ell+1)$ message/signature pairs (m_i, σ_i) after ℓ executions of the signature issue protocols. This adversary wins if all messages are distinct and all signatures verify. Now, consider the following sequence of games, where the first game $\mathsf{Game}\ 0$ is the unforgeability game in which we run the game with the forger $\mathcal{U}^*$. Within all games, the first line number is the number of the game (i.e., line 107 in $\mathsf{Game}\ 1$ corresponds to 007 in $\mathsf{Game}\ 0$).

$\mathsf{Game}\ 0$

000 $x^s, R, S, T, V_i, X_i^s \leftarrow \{0,1\}^\lambda$
001 $(ssk, svk) \leftarrow \mathsf{SigGen}(1^\lambda; S), \mathsf{msg}^s \leftarrow \mathcal{V}^s(1^\lambda), y^s \leftarrow f(x^s), \mathsf{com}^R \leftarrow \mathsf{Com}^R(R, ssk; T)$
002 $vk \leftarrow (svk, y^s, \mathsf{msg}^s, \mathsf{com}^R)$
003 $\mathsf{st}_0 \leftarrow \mathcal{U}^*(vk)$
004 for $i = 1, \ldots, \ell$
005 $(ek_i, c_i, \pi_i^s, \mathsf{com}_i^m, \mathsf{com}_i^{x^u}, \mathsf{msg}_i^u, y_i^u, \mathsf{st}_i) \leftarrow \mathcal{U}^*(\mathsf{st}_{i-1})$
006 $s_i^s := (y^s, ek_i, c_i, \mathsf{com}_i^m, \mathsf{com}_i^{x^u})$
007 if $y_i^u \in \mathsf{image}(f^u)$ and $\mathcal{V}^s(\mathsf{msg}_i^s, s_i^s, \pi_i^s) = 1$ then
008 $c_i' \leftarrow \mathsf{Eval}(ek_i, C_{ssk,R}, c_i; V_i)$
009 $\mathsf{com}_i^{x^s} \leftarrow \mathsf{Com}^M(0^\lambda; X_i^s)$
010 $s_i^u := (svk, \mathsf{com}^R, C_{ssk,R}, c_i, c_i', ek_i, \mathsf{com}_i^{x^s}, y_i^u)$
011 $w_i^u := (R, S, T, V_i, ssk)$
012 $\pi_i^u \leftarrow \mathcal{P}^u(\mathsf{msg}^u, s_i^u, w_i^u)$
013 else
014 $c_i', \mathsf{com}_i^{x^s}, \pi_i^u \leftarrow \perp$
015 $\mathsf{st}_i \leftarrow \mathcal{U}^*(c_i', \mathsf{com}_i^{x^s}, \pi_i^u, \mathsf{st}_i)$
016 end for
017 $(m_1, \sigma_1, \ldots, m_{\ell+1}, \sigma_{\ell+1}) \leftarrow \mathcal{U}^*(\mathsf{st}_\ell)$
018 Return 1 iff $\mathsf{SigVrfy}(svk, m_i, \sigma_i) = 1$ for all $i = 1, \ldots, \ell$ and $m_i \neq m_j$ for all $i \neq j$

$\mathsf{Game}\ 0 \Rightarrow \mathsf{Game}\ 1$**.** We now modify the above game by letting the signer (after step 005) invert the one-way function f^u and extract the message m_i from the commitment com_i^m. By $\mathsf{Com}_i^{M^{-1}}(\mathsf{com}_i^m)$ we denote the function that extract the committed value according to Definition 4.5. Analogously, $f_i^{u^{-1}}(y^s)$ is the algorithm that inverts the one-way function f^u according to Definition 4.2. Both algorithm are running in time T_1. To show that the adversary's success probability in both games is the same (except for a negligible fraction) we have exploit the non-uniform hiding property of the commitment. The difficulty is that step 106a cannot be computed efficiently. Nevertheless, we solve this issue applying the following (standard) technique. The idea is to consider an attacker against the commitment scheme that is computationally unbounded, as long as it

Game 1	
106	$s_i^s := (y^s, ek_i, c_i, \mathsf{com}_i^m, \mathsf{com}_i^{x^u})$
106a	$\boldsymbol{x_i^u \leftarrow f_i^{u^{-1}}(y_i^u), m_i \leftarrow \mathsf{Com}_i^{M^{-1}}(\mathsf{com}_i^m)}$
109	$\mathsf{com}_i^{x^s} \leftarrow \mathsf{Com}^M(\boldsymbol{x_i^u}; X_i^s)$

has not received the commitment. Once the attacker has obtained the commitment, it runs in polynomial time. More precisely is the following lemma:

Lemma 5.2 *Let $\mathcal{C}$ be a non-uniformly hiding commitment scheme and $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary such that $\mathcal{A}_1$ is computationally unbounded and $\mathcal{A}_2$ runs in polynomial time. Then, the probability that $\mathcal{A}$ wins the following game is negligible:*

$$2 \cdot \Pr\left[b = b' \;\middle|\; \begin{array}{l} (m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}_1(1^\lambda)\ ;\ b \leftarrow \{0,1\}\ ; \\ (\mathsf{decom}, \mathsf{com}) \leftarrow \mathsf{Com}(m_b)\ ;\ b' \leftarrow \mathcal{A}_2(\mathsf{com}) \end{array} \right] - 1\ .$$

Proof. Suppose to the contrary that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is an adversary that wins the above game with non-negligible probability. Then there exists a worst-case random tape for $\mathcal{A}$ (for any security parameter) such that $\mathcal{A}$ with that random tape wins the game with non-negligible probability. We now apply an averaging argument. Let m_0, m_1 be the messages that $\mathcal{A}_1$ returns given this random tape and denote by st the returned state. Now, let $\mathcal{A}_2$ be the second adversary that has this state hardcoded into its circuit. Note that $\mathcal{A}_2$ is a non-uniform adversary that runs in polynomial-time. Now, $\mathcal{A}_2$ can clearly predict the bit b and thus wins the game with non-negligible probability. This, however, contradicts the assumption that $\mathcal{C}$ is non-uniformly hiding. □

Lemma 5.2 allows us to perform a computation that is not feasible in polynomial time *before* seeing the commitment. During this step, we extract the message out of the commitment $m_i \leftarrow \mathsf{Com}_i^{M^{-1}}(\mathsf{com}_i^m)$ and we invert the one-way function $x_i^u \leftarrow f_i^{u^{-1}}(y_i^u)$. preimage with overwhelming probability. Then, we commit to x_i^u (instead of 0^λ). Note that this is only possible because step 119 happens after step 116. This, however, is not quite true because this step happens in a loop. Thus, at some point step 119 happens before step 116. To handle this issue, we refine our argument as follows: let Game $\tilde{1}_i$ be the game where we made the substitution during the first i runs but not in iterations $i+1, \ldots, \ell$. Now, the same argument as above shows that Game $\tilde{1}_i$ and Game $\tilde{1}_{i+1}$ are indistinguishable for any i (even if i depends on the security parameter). This, however, also implies that Game $\tilde{1}_0$ and Game $\tilde{1}_\ell$ are indistinguishable. Furthermore Game $\tilde{1}_0$ = Game 0 and Game $\tilde{1}_\ell$ = Game 1, hence Game 0 $\approx$ Game 1 where $\approx$ indicates that the probability that both games output 1 is the same (except for a negligible amount).

Game 1 $\Rightarrow$ Game 2 $\Rightarrow$ Game 3. In the next game, Game 2, we first change the witness of the ZAP Z^u. That is, we use as a witness the pre-image x_i^u of the one-way function f^u that we have inverted in the previous step. Afterwards, in Game 3, we sign the message that was extracted in Game 1, we run the evaluation algorithm on the circuit C_{σ_i} that outputs the constant value σ_i. C_{σ_i} can be assumed to have the same size as $C_{ssk,R}$ by padding.

Game 2	
210	$s_i^u := (svk, \mathsf{com}^R, C_{ssk,R}, c_i, c_i', ek_i, \mathsf{com}_i^{x^s}, y_i^u)$
211	$w_i^u := \boldsymbol{(x_i^s, X_i^u)}$
212	$\pi_i^u \leftarrow \mathcal{P}^u(\mathsf{msg}^u, s_i^u, \boldsymbol{w_i^u})$

Game 3	
308	$\boldsymbol{\sigma_i \leftarrow \mathsf{Sign}(ssk, m_i; F_R(m_i))}$
308a	$c_i' \leftarrow \mathsf{Eval}(ek_i, \boldsymbol{C_{\sigma_i}}, c_i; V_i)$

Now, we argue that both modifications do not change the success probability of the adversary $\mathcal{U}^*$ by more than a negligible amount and therefore, Game 0 $\approx$ Game 3. This should follow from the following two observations

- The one-way function f^u has efficiently decidable images and the signer checks if y_i^u is a valid image under f^u in step 007. Thus, according to our construction the witness x^u is a valid. Note that according to our construction the witness $w_i^u := (R, S, T, V_i, ssk)$ used in Game 1 is also valid. Since both witnesses are a valid witness and because we have assumed that the ZAP Z^u is non-uniformly witness-indistinguishable, it follows that the success probability of $\mathcal{U}^*$ in both games is the same (except for a negligible amount).

- The size-dependent homomorphic encryption scheme is non-uniformly weakly function-private. Thus, the adversary $\mathcal{U}^*$ does not notice the difference in the computation of c_i'.

Unfortunately, we cannot apply both arguments directly. The reason is that these arguments are only applicable as long as the games run in polynomial time. In the previous step, however, we have inverted the one-way function and we have extracted the message from the commitment. Both steps, however, are not computable in polynomial time. We handle this issue by carefully applying a hybrid argument.

The second difficulty results from the fact that the ciphertext may not contain the message that we have extracted from the commitment. In this case, the success probability of the adversary $\mathcal{U}^*$ would change as it would notice the difference after receiving the encrypted signature. We handle this problem by derving a contradiction to the soundness of the ZAP and the one-wayness of the function f^s. Firstly, we prove that the message in the commitment and the encryption are the same. Then, we apply the hybrid argument.

We now apply carefully a hybrid argument over all three games:

Game 1_i**:** Perform the following modifications:

- For all iterations $< i$ apply all changes from Game $1, 2$, and 3.
- In iterations i on apply the modification from Game 1.
- For all iterations $> i$ apply no changes (thus, it corresponds to Game 0).

Game 2_i Apply the following changes:

- For all iterations $< i$ apply all changes from Game $1, 2$, and 3.
- In iterations i on apply the modification from Game 1 and 2.
- For all iterations $> i$ apply no changes (thus, it corresponds to Game 0).

Game 3_i Do the following modifications:

- For all iterations $< i$ apply all changes from Game $1, 2$, and 3.
- In iterations i on apply the modification from Game $1, 2$, and 3.
- For all iterations $> i$ apply no changes (thus, it corresponds to Game 0).

Now we argue that

Game $3_{(i-1)} \approx$ Game 1_i**:** Follows as the only difference between both games are the modifications in Game 1 during the first execution.

Game $1_i \approx$ Game 2_i**:** Follows from our assumption that the ZAP Z^u is non-uniformly witness indistinguishable.

Game $2_i \approx$ Game 3_i**:** The difference between Game 2_i and Game 3_i is that in the i-th iteration, in Game 3_i we replace $c_i' \leftarrow \mathsf{Eval}(ek_i, C_{ssk,R}, c_i; V_i)$ (line 208) by $\sigma_i \leftarrow \mathsf{Sign}(ssk, m_i; F_R(m_i))$, $c_i' \leftarrow \mathsf{Eval}(ek_i, C_{\sigma_i}, c_i; V_i)$ (lines 308, 308a). Assume for the moment that the following fact $(*)$ holds with overwhelming probability: If line 208 is reached, then there exists a dk_i such that (ek_i, dk_i) is in the range of $\mathsf{EncGen}(1^\lambda)$ and

c_i is in the range of $\mathsf{Enc}(ek_i, m_i)$. Notice further that $C_{ssk,R}(m_i) = \sigma_i = C_{\sigma_i}(m_i)$ by construction. Then non-uniform weak circuit privacy implies that $\mathsf{Eval}(ek_i, C_{ssk,R}, c_i; V_i)$ and $\mathsf{Eval}(ek_i, C_{\sigma_i}, c_i; V_i)$ are non-uniformly computationally indistinguishable. Since in Game 2_i and Game 3_i, after line 208 and 308, respectively, only polynomial-time computations occur, this implies that Game $2_i \approx$ Game 3_i.[2]

It is left to show that $(*)$ holds with overwhelming probability. Observe that line 208 is only reached when $\mathcal{V}^s(\mathsf{msg}_i^s, s_i^s, \pi_i^s) = 1$. Thus from the adaptive soundness of Z^s it follows that $s_i^s \in L^s$ with overwhelming probability when line 208 is reached. Assume that s_i^s has a witness of the form (x^s, X^u) with non-negligible probability. Then with non-negligible probability, there are x', X' such that $\mathsf{com}^{x^u} = \mathsf{Com}^M(x'; X')$ and $f^s(x') = y^s$. This leads to a contradiction: From Game 2_i we can construct a non-uniform adversary that breaks the non-uniform T_2-one-wayness of f^s as follows: Upon input of a challenge y, it simulates Game 2_i, using y for y^s (instead of $x \leftarrow f(x^s)$). Then the adversary extract x' from com^{x^u}. With non-negligible probability $f(x') = y_2 = y$. Extracting x' takes time $T_1 \cdot poly(\lambda)$ since $\mathcal{C}^M$ is extractable in time T_1. Similarly, the operations introduced in line 106a take time $T_2 \cdot poly(\lambda)$ since f^u is invertible in time T_2 and $\mathcal{C}^M$ is extractable in time T_1. Thus we have constructed an adversary that runs in time $T_2 \cdot poly(\lambda)$ and breaks the one-wayness of f^s. This contradicts the T_2-one-wayness of f^s. Thus a witness (x^s, X^u) for s_i^s exists only with negligible probability. Since with overwhelming probability, when line 208 is reached, $s_i^s \in L^s$. By definition of L^s, this implies that there is a witness of the form (K, E, M, m, dk) for s_i^s. Hence $(dk, ek_i) = \mathsf{EncGen}(1^\lambda; K)$ and $c = \mathsf{Enc}(ek_i, m; E)$ and $\mathsf{com}_i^m = \mathsf{Com}^M(m; M)$ for some K, E, M, m, dk. Since $\mathcal{C}$ is perfectly binding and since m_i was extracted from com_i^m we have $m = m_i$. Hence $(*)$ holds with overwhelming probability.

Thus Game $2_i \approx$ Game 3_i.

Thus, Game $3_{(i-1)} \approx$ Game 3_i and therefore Game $3_0 \approx$ Game 3_ℓ. Since Game $0 =$ Game 3_0 and because Game $3_\ell =$ Game 3, it follows that Game $0 \approx$ Game 3_ℓ.

Game 3 $\Rightarrow$ Game 4. This game is identical to the prior one, but instead of committing to R and ssk, we commit to an all zero string. Since the commitment scheme $\mathcal{C}^R$ is T_2 hiding, this modification changes the success

Game 4	
401	$\mathsf{com}^R \leftarrow \mathsf{Com}^R(\mathbf{0^\lambda}; T)$

probability of $\mathcal{U}^*$ only by a negligible amount and thus, Game $3 \approx$ Game 4 and therefore Game $0 \approx$ Game 4.

Game 4 $\Rightarrow$ Game 5. In this game, we do not generate the sining key locally, but we build a forger $\mathcal{B}$ against the signature scheme Sig. The difference to the above described games is that it uses its external signing oracle in order to obtain the signature σ_i on the message m_i. Here $\widehat{\mathsf{SigGen}}$ and $\widehat{\mathsf{Sign}}$ constitute a signing oracle.

Game 5	
500	$x, T, V_i, X_i^s \leftarrow \{0,1\}^\lambda$ **(removed R, S)**
501	$\boldsymbol{svk \leftarrow \widehat{\mathsf{SigGen}}(1^\lambda)}, \mathsf{msg}^s \leftarrow \mathcal{V}^s(1^\lambda), y^s \leftarrow f(x^s), \mathsf{com}^R \leftarrow \mathsf{Com}^R(R, ssk; T)$
508	$\boldsymbol{\sigma_i \leftarrow \widehat{\mathsf{Sign}}(m_i)}$

$\widehat{\mathsf{SigGen}}$ produces a verification key and $\widehat{\mathsf{Sign}}$ signs messages, but whenever a message is submitted that was already signed, $\widehat{\mathsf{Sign}}$ returns the previously produced signature again.

[2] This is analogously to the proof of Lemma 5.2.

Since F is a T_2-pseudorandom function, and since R and S are used in Game 4 only in the arguments of SigGen and Sign, it follows that Game 4 $\approx$ Game 5 and thus Game 0 $\approx$ Game 5.

Now, assume that the adversary $\mathcal{U}^*$ wins the unforgeability game with non-negligible probability. Then, since Game 0 $\approx$ Game 5, $\mathcal{U}^*$ also wins with non-negligible in Game 5.

Then it returns $\ell + 1$ pairs (m_i, σ_i) such that $m_i \neq m_j$ for all $i \neq j$ and $\mathsf{SigVrfy}(vk, m_i, \sigma_i) = 1$ for all $i = 1, \ldots, \ell + 1$. We denote by $Q = (m_1, \ldots, m_\ell)$ the set of messages that have been asked to the external signing oracle $\widehat{\mathsf{Sign}}$. Since all messages are distinct there exists at least one message $m_j \notin Q$. The forger $\mathcal{B}$ outputs (m_j, σ_j). Since $\mathsf{SigVrfy}(vk, m_i, \sigma_i) = 1$ for all i, we have in particular that the pair (m_j, σ_j) verifies and thus $\mathcal{B}$ succeeds with non-negligible probability. Since $\mathcal{B}$ runs in time $T_2 \cdot poly(\lambda)$, this contradicts the assumption that Sig is T_2-unforgeable. This concludes the proof. □

Proof of Blindness. We sketch the main idea of the blindness proof and give a formal proof afterwards. The starting point of our proof is a game that corresponds to the blindness game. We then change the step by step such that at the entire transcript is independent of the message. The main steps in the proof are the following:

- We apply a complexity leveraging argument. This technique allows us to invert the one-way function f^s and also to extract the (R, ssk) from the commitment com^R.
- We then send the encryption of an all zero string to the signer and we sign the message locally using ssk.

We show that the success probability of the adversary against the blindness remains the same (except for a negligible amount) because:

- the ZAP Z^s remains valid as it now uses the previously computed preimage x^s of f^s as a witness.
- the size-dependent homomorphic encryption scheme is CPA secure and thus, the attacker cannot tell the difference;

Our modifications, however, result in a protocol where the transcript is independent of the message. This implies that the success probability of the adversary is only negligible bigger than 1/2.

Theorem 5.3 *Suppose that f^s, f^u, and F are functions, $\mathcal{C}^M, \mathcal{C}^R$ two commitment schemes,* Sig *a signature scheme, Z^s, Z^u two ZAPs, and* Enc *size-dependent homomorphic encryption scheme such that all primitives satisfy Condition 3. Then the blind signature scheme as defined in Section 5.1 is blind.*

Proof. We prove this theorem via a sequence of games. It is understood that the adversary $\mathcal{S}^*$ keeps some state during the blindness experiment. The first game Game 0 corresponds to the blindness game.

Game 0

000	$K_0, K_1, X_0^u, X_1^u, M_0, M_1, E_0, E_1, x_0^u, x_1^u \leftarrow \{0,1\}^\lambda, b \leftarrow \{0,1\}$	
001	$(vk, m_0, m_1) \leftarrow \mathcal{S}^*(1^\lambda)$ with $vk = (svk, y^s, \mathsf{msg}^s, \mathsf{com}^R)$; if $y^s \notin \mathsf{image}(f^s)$ then abort	
002	$(ek_0, dk_0) \leftarrow \mathsf{EncGen}(1^\lambda; K_0)$	$(ek_1, dk_1) \leftarrow \mathsf{EncGen}(1^\lambda; K_1)$
003	$\mathsf{com}_0^{x^u} \leftarrow \mathsf{Com}^M(0^\lambda; X_0^u)$	$\mathsf{com}_1^{x^u} \leftarrow \mathsf{Com}^M(0^\lambda; X_1^u)$
004	$\mathsf{com}_0^m \leftarrow \mathsf{Com}^M(m_0; M_0)$	$\mathsf{com}_1^m \leftarrow \mathsf{Com}^M(m_1; M_1)$
005	$c_0 \leftarrow \mathsf{Enc}(ek_0, m_0; E_0)$	$c_1 \leftarrow \mathsf{Enc}(ek_1, m_1; E_1)$
006	$s_0^s := (y^s, ek_0, c_0, \mathsf{com}_0^m, \mathsf{com}_0^{x^u})$	$s_1^s := (y^s, ek_1, c_1, \mathsf{com}_1^m, \mathsf{com}_1^{x^u})$
007	$w_0^s := (K_0, E_0, M_0, m_0, dk_0)$	$w_1^s := (K_1, E_1, M_1, m_1, dk_1)$
008	$\pi_0^s \leftarrow \mathcal{P}^s(\mathsf{msg}^s, s_0^s, w_0^s)$	$\pi_1^s \leftarrow \mathcal{P}^s(\mathsf{msg}^s, s_1^s, w_1^s)$
009	$y_1^u \leftarrow f^u(x_0^u)$	$y_1^u \leftarrow f^u(x_1^u)$
010	$\mathsf{msg}_0^u \leftarrow \mathcal{V}^u(1^\lambda)$	$\mathsf{msg}_1^u \leftarrow \mathcal{V}^u(1^\lambda)$
011	$((c'_b, \pi_b^u, \mathsf{com}_b^{x^s}), (c'_{\bar{b}}, \pi_{\bar{b}}^u, \mathsf{com}_{\bar{b}}^{x^s})) \leftarrow \mathcal{S}^*((ek_b, c_b, \pi_b^s, \mathsf{com}_b^m, \mathsf{com}_b^{x^u}, \mathsf{msg}_b^u, y_b^u), (ek_{\bar{b}}, c_{\bar{b}}, \pi_{\bar{b}}^s, \mathsf{com}_{\bar{b}}^m, \mathsf{com}_{\bar{b}}^{x^u}, \mathsf{msg}_{\bar{b}}^u, y_{\bar{b}}^u))$	
012	$s_0^{u'} := (svk, \mathsf{com}^R, c_0, c'_0, ek_0, \mathsf{com}_0^{x^s}, y_0^u)$	$s_1^{u'} := (svk, \mathsf{com}^R, c_1, c'_1, ek_1, \mathsf{com}_1^{x^s}, y_1^u)$
013	if $\mathcal{V}^u(\mathsf{msg}_0^u, s_0^{u'}, \pi_0^u) = 1$ then	if $\mathcal{V}^u(\mathsf{msg}_0^u, s_1^{u'}, \pi_1^u) = 1$ then
014	$\sigma_0 \leftarrow \mathsf{Dec}(dk_0, c'_0)$ else $\sigma_0 \leftarrow \perp$	$\sigma_1 \leftarrow \mathsf{Dec}(dk_1, c'_1)$ else $\sigma_1 \leftarrow \perp$
015	if $\mathsf{SigVrfy}(vk, m_i, \sigma_i) \neq 1$ for $i = 0, 1$ set $\sigma_0 \leftarrow \perp$ and $\sigma_1 \leftarrow \perp$	
016	$b' \leftarrow \mathcal{S}^*(\sigma_0, \sigma_1)$	
017	Return 1 iff $b = b'$	

Game 0 $\Rightarrow$ Game 1. Game 1 is identical to Game 0 except for the following modifications. In Step 101a we invert the one-way function f^s and we then commit to the preimage x^s (instead of 0^λ). Obviously, the

Game 1

101	$(vk, m_0, m_1) \leftarrow \mathcal{S}^*(1^\lambda)$ with $vk = (svk, y^s, \mathsf{msg}^s, \mathsf{com}^R)$; if $y^s \notin \mathsf{image}(f^s)$ then abort	
101a	$\boldsymbol{x^{s'} \leftarrow f^{s^{-1}}(y^s)}$	
103	$\mathsf{com}_0^{x^{s'}} \leftarrow \mathsf{Com}^M(\boldsymbol{x^{s'}}; X_0^u)$	$\mathsf{com}_1^{x^s} \leftarrow \mathsf{Com}^M(\boldsymbol{x^{s'}}; X_1^u)$

inversion of the one-way function f^s cannot be done efficiently. This operation, however, is possible applying Lemma 5.2 and the fact that the commitment scheme $\mathcal{C}^M$ is non-uniformly hiding. Recall that Lemma 5.2 shows that every non-uniform hiding commitment scheme preserves this property even is the adversary may perform an unbounded computation *before* receiving the commitment. Observe that the game aborts if the y^s is not a valid image and assume in the following that y^s is a valid image of f^s. But if y^s is a valid image, then we obtain a valid preimage $x^{s'}$. Since $\mathcal{C}^M$ is non-uniformly hiding, it follows that Game 0 $\approx$ Game 1.

Game 1 $\Rightarrow$ Game 2. Game 2 differs from Game 1 in the step where the user computes the proof π^s of the ZAP Z^s. In this game, we use the previously extracted preimage x^s of the one-way function f^s as a witness. It follows from our construction that both witnesses w_i^s are valid in game Game 1. Moreover, as discussed in the previous game, the value x^s is a valid preimage of y^s and thus it is an alternative witness for the ZAP Z^s. Since the ZAP Z^s is non-uniformly witness-indistinguishable it follows that the success probability of the adversary $\mathcal{S}^*$ remains the same (except for a negligible amount). Thus, Game 2 $\approx$ Game 3.

Game 2 $\Rightarrow$ Game 3. In this game, we modify the way we compute the commitment com^m. That is, instead of committing to the message m_i, we commit to 0^λ. According to our assumption that the commitment

Game 2		
206	$s_0^s := (y^s, ek_0, c_0, \mathsf{com}_0^m, \mathsf{com}_0^{x^u})$	$s_0^s := (y^s, ek_1, c_1, \mathsf{com}_1^m, \mathsf{com}_1^{x^u})$
207	$w_0^s := \boldsymbol{(x^{s'}, X_0^u)}$	$w_1^s := \boldsymbol{(x^{s'}, X_1^u)}$
208	$\pi_0^s \leftarrow \mathcal{P}^s(\mathsf{msg}^s, s_0^s, w_0^s)$	$\pi_1^s \leftarrow \mathcal{P}^s(\mathsf{msg}^s, s_1^s, w_1^s)$

Game 3		
304	$\mathsf{com}_0^m \leftarrow \mathsf{Com}^M(\mathbf{0^\lambda}; M_0)$	$\mathsf{com}_1^m \leftarrow \mathsf{Com}^M(\mathbf{0^\lambda}; M_1)$

scheme is non-uniformly hiding, it follows this modification changes the success probability of $\mathcal{S}^*$ only by a negligible amount, and thus, Game 2 $\approx$ Game 3.

Game 3 $\Rightarrow$ Game 4. This game is identical to the prior one, but in this game we extract the values R and ssk from the commitment com_R. Since R and ssk are never used and $\mathsf{Com}^{R^{-1}}$ has no side-effects,

Game 4	
401b	$\boldsymbol{(R, ssk) \leftarrow \mathsf{Com}^{R^{-1}}(\mathsf{com}^R)}$

Game 3 = Game 4.

Game 4 $\Rightarrow$ Game 5. In this game, instead of decrypting c_i' to get the signature σ_i, we instead just sign the extracted message m_i.

Assume for the moment that the following fact $(*)$ holds with overwhelming probability: If the assignment $\sigma_i \leftarrow \mathsf{Sign}(ssk, m_i; F_R(m_i))$ in line 514 is reached, then there exist values R_i, ssk_i such that (svk, ssk_i) is the range $\mathsf{SigGen}(1^\lambda)$ and c_i' is the range of $\mathsf{Eval}(ek_i, C_{R,ssk}, c_i)$ and com^R in the range of $\mathsf{Com}^R((R_i, ssk_i))$. Then, since $\mathcal{C}^R$ is perfectly binding, $\mathsf{Com}^{R^{-1}}(\mathsf{com}^R)$ returns $(R, ssk) = (R_i, ssk_i)$. By the perfect correctness of Enc and the definition of $C_{R,ssk}$, this implies that computing $\mathsf{Dec}(dk_i, c_i')$ and $\mathsf{Sign}(ssk, m_i; F_R(m_i))$ yields the same result. Thus, if $(*)$ holds with overwhelming probability, Game 4 $\approx$ Game 5.

It is left to show that $(*)$ holds with overwhelming probability. Observe that the assignment $\sigma_i \leftarrow \mathsf{Sign}(ssk, m_i; F_R(m_i))$ is only reached when $\mathcal{V}^u(\mathsf{msg}^u, s^{u'}, \pi_i^u) = 1$. Thus, from the adaptive soundness of Z^u it follows that $s_i^u \in L^u$ with overwhelming probability. Assume that s_i^u has a witness of the form (x^u, X^s) with non-negligible probability. Then with non-negligible probability, there are x', X' such that $\mathsf{com}^{x^s} = \mathsf{Com}^M(x'; X')$ and $f^u(x') = y_i^u$. This leads to a contradiction: From Game 5 we can construct a non-uniform adversary that breaks the non-uniform T_2-one-wayness of f^u as follows: Upon input of a challenge y, it simulates Game 5, using y for y_i^u (instead of $y_i^u \leftarrow f(x_i^u)$). Then the adversary extracts x' from com^{x^s} such that with non-negligible probability $f^u(x') = y_i^u$. Extracting x' takes time $T_1 \cdot poly(\lambda)$ since $\mathcal{C}^M$ is extractable in time T_1. Notice, however, that the steps introduced in lines 101a and 401b may take exponential time. However, these steps occur before the $y = y_i^u$ is first accessed. Thus we have constructed an adversary that first runs an unbounded amount of time, then inputs the challenge y, and then runs in time $T_1 \cdot poly(\lambda)$ and finds a preimage of y under f^u with non-negligible probability. Since the result of the unbounded precomputation can be hardcoded into a non-uniform adversary (analogous to Lemma 5.2), such an adversary breaks the T_1-one-wayness of f^u. Thus $(*)$ holds with overwhelming probability.

It follows Game 4 $\approx$ Game 5.

Game 5	
514	$\sigma_0 \leftarrow \mathsf{Sign}(ssk, \boldsymbol{m_0; F_R(m_0)})$ else $\sigma_0 \leftarrow \perp$ $\mid$ $\sigma_1 \leftarrow \mathsf{Sign}(ssk, \boldsymbol{m_1; F_R(m_1)})$ else $\sigma_1 \leftarrow \perp$

Game 5 $\Rightarrow$ Game 6. In this game, instead of sending an encryption of m_i, we send an encryption of 0^λ. Since after line 605, only polynomial-time computations occur, and since dk_0, dk_1 are never used, from the

Game 6	
605	$c_0 \leftarrow \mathsf{Enc}(ek_0, \boldsymbol{0^\lambda}; E_0)$ $\mid$ $c_1 \leftarrow \mathsf{Enc}(ek_1, \boldsymbol{0^\lambda}; E_1)$

non-uniform IND-CPA security of Enc it follows that Game 5 $\approx$ Game 6.

It follows Game 0 $\approx$ Game 6.

It is easy to see that in Game 6, the view of $\mathcal{S}^*$ is independent of b. (The signatures σ_i do not depend on the values sent by $\mathcal{S}^*$.) Thus in Game 6, the probability that $\mathcal{S}^*$ guesses $b' = b$ is $\frac{1}{2}$. Hence in Game 6, that probability is negligibly close to $\frac{1}{2}$. Thus our blind signature scheme satisfies blindness. □

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, Innsbruck, Austria, May 6–10, 2001. Springer, Berlin, Germany.

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In *Advances in Cryptology – CRYPTO 2010*, Lecture Notes in Computer Science, pages 209–236, Santa Barbara, CA, USA, August 2010. Springer, Berlin, Germany.

[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, San Jose, CA, USA, February 13–17, 2006. Springer, Berlin, Germany.

[AO09] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 435–450, Tokyo, Japan, December 6–10, 2009. Springer, Berlin, Germany.

[BHHI10] Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai. Bounded key-dependent message security. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 423–444, French Riviera, May 30 – June 3, 2010. Springer, Berlin, Germany.

[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, Miami, USA, January 6–8, 2003. Springer, Berlin, Germany.

[BP10] Stefan Brands and Christian Paquin. U-prove cryptographic specification v1.0. `http://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953`, March 2010.

[Bra00] Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, MA, USA, 2000.

[CG08] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 08: 15th Conference on Computer and Communications Security*, pages 345–356, Alexandria, Virginia, USA, October 27–31, 2008. ACM Press.

[Cha83] 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, Santa Barbara, CA, USA, 1983. Plenum Press, New York, USA.

[Cha84] David Chaum. Blind signature system. In David Chaum, editor, *Advances in Cryptology – CRYPTO'83*, page 153, Santa Barbara, CA, USA, 1984. Plenum Press, New York, USA.

[CKW04] 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, Amalfi, Italy, September 8–10, 2004. Springer, Berlin, Germany.

[CNS07] Jan Camenisch, Gregory Neven, and Abhi Shelat. Simulatable adaptive oblivious transfer. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 573–590, Barcelona, Spain, May 20–24, 2007. Springer, Berlin, Germany.

[DN07] Cynthia Dwork and Moni Naor. Zaps and their applications. *SIAM J. Comput.*, 36(6):1513–1543, 2007.

[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, Santa Barbara, CA, USA, August 20–24, 2006. Springer, Berlin, Germany.

[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, Irvine, CA, USA, March 18–20, 2009. Springer, Berlin, Germany.

[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, French Riviera, May 30 – June 3, 2010. Springer, Berlin, Germany.

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988.

[GS10] E. Ghadafi and N.P. Smart. Efficient two-move blind signatures in the common reference string model. Cryptology ePrint Archive, Report 2010/568, 2010. `http://eprint.iacr.org/`.

[HK07] Omer Horvitz and Jonathan Katz. Universally-composable two-party computation in two rounds. In Alfred Menezes, editor, *Advances in Cryptology – CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 111–129, Santa Barbara, CA, USA, August 19–23, 2007. Springer, Berlin, Germany.

[HKKL07] Carmit Hazay, Jonathan Katz, Chiu-Yuen Koo, and Yehuda Lindell. Concurrently-secure blind signatures without random oracles or setup assumptions. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 323–341, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Berlin, Germany.

[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, Santa Barbara, CA, USA, August 17–21, 1997. Springer, Berlin, Germany.

[KSY11] Jonathan Katz, Dominique Schröder, and Arkady Yerukhimovich. Impossibility of blind signature from one-way permutation. In *TCC 2011: 8th Theory of Cryptography Conference*, Lecture Notes in Computer Science. Springer, Berlin, Germany, 2011. To appear, available at `http://www.cs.umd.edu/~jkatz/`.

[KZ08] Aggelos Kiayias and Hong-Sheng Zhou. Equivocal blind signatures and adaptive UC-security. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 340–355, San Francisco, CA, USA, March 19–21, 2008. Springer, Berlin, Germany.

[Lin03] Yehuda Lindell. Bounded-concurrent secure two-party computation without setup assumptions. In *35th Annual ACM Symposium on Theory of Computing*, pages 683–692, San Diego, California, USA, June 9–11, 2003. ACM Press.

[Lin04] Yehuda Lindell. Lower bounds for concurrent self composition. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 203–222, Cambridge, MA, USA, February 19–21, 2004. Springer, Berlin, Germany.

[MSF10] Sarah Meiklejohn, Hovav Shacham, and David Mandell Freeman. Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures. In *Advances in Cryptology – ASIACRYPT 2010*, Lecture Notes in Computer Science, pages 519–538. Springer, Berlin, Germany, December 2010.

[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, New York, NY, USA, March 4–7, 2006. Springer, Berlin, Germany.

[PRS02] Manoj Prabhakaran, Alon Rosen, and Amit Sahai. Concurrent zero knowledge with logarithmic round-complexity. In *43rd Annual Symposium on Foundations of Computer Science*, pages 366–375, Vancouver, British Columbia, Canada, November 16–19, 2002. IEEE Computer Society Press.

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

[Rüc10] Markus Rückert. Lattice-based blind signatures. In *Advances in Cryptology – ASIACRYPT 2010*, Lecture Notes in Computer Science, pages 413–430. Springer, Berlin, Germany, December 2010.