A Short Paper on Blind Signatures from Knowledge Assumptions

Lucjan Hanzlik(✉) and Kamil Kluczniak

Faculty of Fundamental Problems of Technology,
Wrocław University of Technology, Wrocław, Poland
{lucjan.hanzlik,kamil.kluczniak}@pwr.edu.pl

Abstract. This paper concerns blind signature schemes. We focus on two moves constructions, which imply concurrent security. There are known efficient blind signature schemes based on the random oracle model and on the common reference string model. However, constructing two move blind signatures in the standard model is a challenging task, as shown by the impossibility results of Fischlin et al. The recent construction by Garg et al. (Eurocrypt'14) bypasses this result by using complexity leveraging, but it is impractical due to the signature size ($\approx$ 100 kB). Fuchsbauer et al. (Crypto'15) presented a more practical construction, but with a security argument based on interactive assumptions. We present a blind signature scheme that is two-move, setup-free and comparable in terms of efficiency with the results of Fuchsbauer et al. Its security is based on a knowledge assumption.

Keywords: Blind signature · Okamoto-Uchiyama cryptosystem · Knowledge assumption

1 Introduction

A blind signature scheme is a cryptographic primitive that allows a user to receive a signature under a message in such a way, that the signer does not learn anything about the signed message (*blindness*). In addition, if the user receives a number of signatures, he should not be able to create a signature under a different message (*unforgeability*).

The idea of blind signatures was first introduced by David Chaum in the paper [6]. He used blind signatures for protecting privacy of users in his e-cash system. Thanks to blind signatures the bank cannot trace the usage of a signed e-cash as the structure of a note is not known. From this point on, blind signatures have been used as building blocks in numerous cryptographic schemes, e.g. in e-voting and anonymous credential systems.

Solutions that are *provably secure* in the random oracle model are frequently accepted by researchers and the industry, and are of great value due to their efficiency. However, the random oracle model does not always yield a secure real world instantiation. In order to bypass the random oracle model, authors in [7,11,12]

J. Grossklags and B. Preneel (Eds.): FC 2016, LNCS 9603, pp. 535–543, 2017.
DOI: 10.1007/978-3-662-54970-4_31

used the common reference string model in their constructions of blind signatures. This model requires that the users perform a setup phase in which they receive the common reference string (CRS) that must be computed by a trusted third party in order to be useful and to ensure the security of the scheme.

Fischlin et al. have shown in [8] a negative result on the existence of three-move blind signature schemes with a black-box reduction in the standard model. Surprisingly, recent results [10,11] present constructions which circumvent the limitation from [8]. To be more specific, the authors present two-move blind signature schemes which are provably secure without ROM or CRS, however use a non-block-box technique called complexity leveraging. Both solutions are not really practical with signature size of hundreds of kB. A more practical solution was proposed by Fuchsbauer et al. in [9] at CRYPTO'15. The signature size of their construction is not greater than 1 kB. The security of the scheme is based on interactive assumptions. However, the interactive assumption is required so that blindness holds in the stronger *malicious-signer* model (where the signer's public key can be chosen in a malicious way). Blindness in the weaker *honest-signer* model (where the signer's public key is honestly generated), holds under the standard Decisional Diffie-Hellman assumption.

Our Contribution. We propose a different approach to bypass the impossibility results from [8]. We combine the partially homomorphic Okamoto-Uchiyama cryptosystem, Pedersen commitments and BB signatures in order to get an efficient two-move, setup-free blind signature scheme.

Blindness of our solution is based on the semantic security of the encryption scheme and unforgeability follows from the knowledge of factor assumption [1]. Under this assumption the Okamoto-Uchiyama cryptosystem is secret key aware. Note that this strong extraction assumption implies non-black-box reductions. Blindness of our scheme holds in the weaker *honest-signer* model. The proposed construction is comparable, in terms of signature size and communication size, with the one from [9]. However, since the security of our scheme is based on a different type of assumption, we feel that it is an interesting alternative.

2 Preliminaries

Definition 1 (Bilinear Groups). *Let us consider cyclic groups* $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$, $(\mathbb{G}_T, \cdot)$ *of prime order* q. *Let* P_1, P_2 *be generators of respectively* $\mathbb{G}_1$ *and* $\mathbb{G}_2$. *A mapping* $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ *is called a* bilinear map *(pairing), if it is efficiently computable and the following conditions hold:*

bilinearity: $\forall (S, T) \in \mathbb{G}_1 \times \mathbb{G}_2$, $\forall a, b \in \mathbb{Z}_q$, *we have* $e(aS, bT) = e(S, T)^{a \cdot b}$,
non-degeneracy: $e(P_1, P_2) \neq 1$ *is a generator of group* $\mathbb{G}_T$.

Definition 2 (Bilinear-group generator). *A bilinear-group generator is a polynomial-time algorithm* BGGen *that on input a security parameter* λ *returns a bilinear group* $\mathsf{BG} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2)$ *such that* $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$

and $\mathbb{G}_T$ are groups of order q with $\log_2 q = \lambda$ and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map. Similar to the authors of [9], we assume that BGGen *is deterministic (which is the case for BN-curves [2]).*

2.1 Okamoto-Uchiyama Cryptosystem

In our construction we use the Okamoto-Uchiyama cryptosystem [13].

Key Generation: Choose two large primes p, q ($|p| = |q| = k$), and let $n = p^2 q$. Choose $g \in \mathbb{Z}_n^*$ randomly such that the order of $g_p = g^{p-1} \mod p^2$ is p. Let $h = g^n \mod n$. The public key is the tuple $\mathsf{pk}_{\mathsf{Enc}} = (n, g, h)$. The secret key is the tuple $\mathsf{sk}_{\mathsf{Enc}} = (p, q)$.

Encryption: Let $m \in \mathbb{Z}_p$ be a plaintext. Select $r \xleftarrow{\$} \mathbb{Z}_n$ and output $C = g^m h^r \mod n$. We will simply use $\mathsf{Enc}(m)$ to denote a ciphertext of message m, and $\mathsf{Enc}(m, r)$ to additionally identify the randomness r used.

Decryption: Compute $C_p = C^{p-1} \mod p^2$, output message $m = \frac{L(C_p)}{L(g_p)} \mod p$, where $L(x) = \frac{x-1}{p}$.

The Okamoto-Uchiyama cryptosystem is semantically secure. In other words, indistinguishability under chosen plaintext attack (IND-CPA) holds for this scheme. It is partially homomorphic:

$$\mathsf{Enc}(m_1, r_1) \cdot \mathsf{Enc}(m_2, r_2)^{m_3} \mod n = \mathsf{Enc}(m_1 + m_2 \cdot m_3, r_1 + r_2 \cdot m_3).$$

Barbosa and Farshim [1] introduced a so-called *knowledge of factor assumption.* It is similar to the well-known knowledge of exponent assumptions [3]. However, it states that one can output an integer of the form $n = p^2 \cdot q$ only if one knows the primes p and q. It was shown by Barbosa and Farshim that under the knowledge of factor assumption the Okamoto-Uchiyama cryptosystem is secret-key-aware, i.e. it is possible to extract the secret key from an adversary that has generated the public key for such a cryptosystem.

2.2 BB Signatures

We now recall the short signature scheme proposed by Boneh and Boyen [4]. Their signature scheme consists of the following PPT algorithms:

$\mathsf{KeyGen}_{\mathsf{BB}}(1^\lambda)$: Select random generators $P_1 \in \mathbb{G}_1$ and $P_2 \in \mathbb{G}_2$, random integers $x, y \in \mathbb{Z}_p^*$. Compute $u = [x]P_2$ and $v = [y]P_2$. The public key is the tuple $\mathsf{pk}_{\mathsf{BB}} = (P_1, P_2, u, v)$. The secret key is the triple $\mathsf{sk}_{\mathsf{BB}} = (P_1, x, y)$.

$\mathsf{Sign}_{\mathsf{BB}}(m, \mathsf{sk}_{\mathsf{BB}})$: given the secret key $\mathsf{sk}_{\mathsf{BB}} = (P_1, x, y)$ and a message $m \in \mathbb{Z}_p$, pick $r \in \mathbb{Z}_p \backslash \{-\frac{x+m}{y}\}$ at random and compute $s = [\frac{1}{m+x+yr}]P_1$. Then $\sigma = (s, r)$ is a signature of m.

$\mathsf{Verify}_{\mathsf{BB}}(m, \sigma, \mathsf{pk}_{\mathsf{BB}})$: given the public key $\mathsf{pk}_{\mathsf{BB}} = (P_1, P_2, u, v)$, a message m, and a signature $\sigma = (s, r)$, check whether $e(s, u \cdot [m]P_2 \cdot [r]v) = e(P_1, P_2)$. If the equality holds, then output 1 and 0 otherwise.

Under the q-SDH assumption the above signature scheme is secure against strong existential forgery and an adaptive chosen message attack.

2.3 Pedersen Commitments

In contrary to the standard approach, where commitments are elements of groups, we require that the commitments are elements of a subset of $\mathbb{Z}_q$. In particular, one can easily transform Pedersen commitments defined over elliptic curves to have this property. Below we give a formal definition of this commitment scheme.

Definition 3 (Pedersen Commitment with Commitments in $\mathbb{Z}_q$). *Pedersen commitments consist of the following algorithms:*

$\mathsf{Setup_P}(1^\lambda, q)$*:*
Compute, using the security parameter 1^λ*, an ordinary elliptic curve* $\mathbb{G} = E(\mathbb{F}_p)$ *(where* $p < q$*) of a prime order* q_P*. Let* P *be the generator of* $\mathbb{G}$*. Choose* $z \xleftarrow{\$} \mathbb{Z}_q$*, compute* $Q = [z]P$ *and output the commitment key* $\mathsf{cpp} = (\mathbb{G}, P, Q, q_\mathsf{P})$ *(which is an implicit parameter to the below algorithms).*

$\mathsf{Commit_P}(m, r)$*:*
On input a message $m \in \mathbb{Z}_{q_\mathsf{P}}$ *and randomness* $r \in \mathbb{Z}_{q_\mathsf{P}}$*, compute* $Co = (Co_x, Co_y) = [m]P + [r]Q$*, output commitment* Co_x *and opening* $O = r$*.*

$\mathsf{Open_P}(Co_x, m, O)$*:*
On input a commitment $Co_x \in \mathbb{F}_p$*, message* m *and opening* O*, compute* $(Co_x^*, Co_y^*) = [m]P + [r]Q$ *and if* $Co_x = Co_x^*$ *output* m*, else output* $\perp$*.*

This modified Pedersen commitment scheme is still perfectly hiding and computationally binding under the DLP assumption in $\mathbb{G}$. Note that it may happen that an adversary breaks the binding property by returning (m_0, r_0) and (m_1, r_1) such that $(Co_x, Co_y) = [m_0]P + [r_0]Q$ and $(Co_x, -Co_y) = [m_1]P + [r_1]Q$. However, in such a case we can still compute the DLP of Q to base P because $m_0 + z \cdot r_0 = -(m_1 + z \cdot r_1)$, which yields $z = -(m_0 + m_1)/(r_0 + r_1)$.

3 Blind Signatures

In this section we recall the syntax and security of blind signature schemes.

Definition 4. *A blind signature scheme consists of the following PPT algorithms* $\mathsf{BS} = (\mathsf{KeyGen_{BS}}, \mathcal{U}_\mathsf{BS}, \mathcal{S}_\mathsf{BS}, \mathsf{Verify_{BS}})$ *defined as follows:*

$\mathsf{KeyGen_{BS}}(1^\lambda)$*: on input a security parameter, this algorithm outputs a pair of public/secret key* $(\mathsf{pk_{BS}}, \mathsf{sk_{BS}})$ *of the signer.*

$\langle \mathcal{U}_\mathsf{BS}(m, \mathsf{pk_{BS}}), \mathcal{S}_\mathsf{BS}(\mathsf{sk_{BS}}) \rangle$*: are executed by a user and a signer. On input the signer's secret key* $\mathsf{sk_{BS}}$ *algorithm* $\mathcal{S}_\mathsf{BS}$ *interacts with algorithm* $\mathcal{U}_\mathsf{BS}$*. On input a message* m*, from message space* $\mathcal{M}$*, and the signer public key* $\mathsf{pk_{BS}}$*, algorithm* $\mathcal{U}_\mathsf{BS}$ *outputs a signature* σ *on* m*, or* $\perp$*, if the interaction was not successful.*

$\mathsf{Verify_{BS}}(m, \sigma, \mathsf{pk_{BS}})$*: on input a message* m*, signature* σ *and the signer's public key* $\mathsf{pk_{BS}}$*, this algorithm outputs* 1*, if* σ *is a valid signature and* 0 *otherwise.*

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

Unforgeability. A blind signature scheme BS is *strongly unforgeable*, if for all PPT algorithms $\mathcal{A}$ having access to a signer oracle, we have:

$$\Pr\Big[(\mathsf{pk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda), (m_i^*, \sigma_i^*)_{i=1}^{k+1} \leftarrow \mathcal{A}(\mathsf{pk}_{\mathsf{BS}})^{\langle \cdot\ , \mathcal{S}_{\mathsf{BS}}(\mathsf{sk}_{\mathsf{BS}})\rangle} : \\ (m_i^*, \sigma_i^*) \neq (m_j^*, \sigma_j^*) \quad \text{for } i, j \in \{1, \ldots, k+1\}, i \neq j \qquad \text{and} \\ \mathsf{Verify}_{\mathsf{BS}}(m_i^*, \sigma_i^*, \mathsf{pk}_{\mathsf{BS}}) = 1 \quad \text{for } i \in \{1, \ldots, k+1\}\Big] \leq \epsilon(\lambda),$$

where k is the number of oracle queries.

Blindness. A blind signature scheme BS is *blind* in the *honest-signer* model, if for all PPT algorithms $\mathcal{A}$ with one-time access to two user oracles, we have:

$$\Pr\Big[b \xleftarrow{\$} \{0,1\}, (\mathsf{pk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}}) \leftarrow \mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda), (\mathsf{St}_1, m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}_{\mathsf{BS}}, \mathsf{sk}_{\mathsf{BS}}), \\ (\mathsf{St}_2) \leftarrow \mathcal{A}(\mathsf{St}_1)^{\langle \mathcal{U}_{\mathsf{BS}}(m_b, \mathsf{pk}_{\mathsf{BS}}),\ \cdot\rangle^{(1)}, \langle \mathcal{U}_{\mathsf{BS}}(m_{1-b}, \mathsf{pk}_{\mathsf{BS}}),\ \cdot\rangle^{(1)}}, \\ \text{Let } \sigma_b \text{ and } \sigma_{1-b} \text{ be the resp. outputs of } \mathcal{U}_{\mathsf{BS}}, \\ \text{If } \sigma_0 = \bot \text{ or } \sigma_1 = \bot \text{ then } (\sigma_0, \sigma_1) = (\bot, \bot), \\ b^* \leftarrow \mathcal{A}(\mathsf{St}_2, \sigma_0, \sigma_1) : b = b^*\Big] - \tfrac{1}{2} \leq \epsilon(\lambda).$$

4 Construction

The core idea of our construction is to use the partially homomorphic properties of the Okamoto-Uchiyama cryptosystem to perform certain parts of the signing algorithm of BB signatures. However, for correctness the message space of the encryption scheme must be large, so that the computations are performed in $\mathbb{Z}$. To ensure blindness the signed value is not the actual message m, but a perfectly-hiding commitment (Definition 3) to m. Thus, the message space of the scheme is the same as for the commitment scheme, i.e. $\mathcal{M} = \mathbb{Z}_{q_{\mathsf{P}}}$. Finally, the signed commitment and the opening information are given as part of the blind signature. The details of our construction are given in Scheme 1.

Theorem 1 (Correctness). *Scheme 1 is correct.*

Proof. Let m be the message requested by the user, Co the commitment to it and $\mathsf{pk}_{\mathsf{Enc}} = (n, g_n, h_n)$ the public key of the Okamoto-Uchiyama cryptosystem. In order to answer the request of the user, the signer chooses random $b, r_S \xleftarrow{\$} \mathbb{Z}_q$ and uses the homomorphic property of the cryptosystem to compute the ciphertext $c_\sigma = (c_m \cdot c_r^y \cdot \mathsf{Enc}((x + (r_S \cdot y)) \mod q))^b \mod n$. The ciphertext c_σ, r_S and $[b]P_1$ are send to the user. The user deciphers c_σ and receives: $t = b \cdot (Co + r_S \cdot y + ((x + (r_S \cdot y)) \mod q)) \mod p_n$. However, since the Okamoto-Uchiyama

$\mathsf{KeyGen}_{\mathsf{BS}}(1^\lambda)$: Generate bilinear group parameters $\mathsf{BG} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q_1, Q_2) \leftarrow \mathsf{BGGen}(1^\lambda)$ and the commitment key $\mathsf{cpp} = (\mathbb{G}, P, Q, q_{\mathsf{P}}) \leftarrow \mathsf{Setup}_{\mathsf{P}}(1^\lambda, q)$. Use parameters BG to compute random elements $P_1 \xleftarrow{\$} \mathbb{G}_1$, $P_2 \xleftarrow{\$} \mathbb{G}_2$, $x \xleftarrow{\$} \mathbb{Z}_q$ $y \xleftarrow{\$} \mathbb{Z}_q$, the secret key $\mathsf{sk}_{\mathsf{BB}} = (P_1, x, y)$ and the public key $\mathsf{pk}_{\mathsf{BB}} = (P_1, P_2, u = [x]P_2, v = [y]P_2)$ for the BB signature scheme. Return $\mathsf{pk}_{\mathsf{BS}} = (1^\lambda, \mathsf{cpp}, \mathsf{pk}_{\mathsf{BB}})$ and $\mathsf{sk}_{\mathsf{BS}} = (\mathsf{sk}_{\mathsf{BB}})$.

$\mathcal{U}^{(1)}_{\mathsf{BS}}(m, \mathsf{pk}_{\mathsf{BS}})$: generate the parameters $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$. Compute the commitment $(Co, o_{Co}) = \mathsf{Commit}_{\mathsf{P}}(m, r_{Co})$ for a random $r_{Co} \in \mathbb{Z}_{q_{\mathsf{P}}}$. Generate the Okamoto-Uchiyama cryptosystem with public key $\mathsf{pk}_{\mathsf{Enc}} = (n, g_n, h_n)$ and secret key $\mathsf{sk}_{\mathsf{Enc}} = (p_n, q_n)$ (where $p_n > 3 \cdot q^2$). Compute $c_m = \mathsf{Enc}(Co)$, choose random $r_U \xleftarrow{\$} \mathbb{Z}_q$ and compute $c_r = \mathsf{Enc}(r_U)$. Set $\rho = (\mathsf{pk}_{\mathsf{Enc}}, c_m, c_r)$ and $\mathsf{St}_{\mathsf{BS}} = (\rho, (Co, o_{Co}, r_U), \mathsf{sk}_{\mathsf{Enc}})$. Send ρ to the signer.

$\mathcal{S}_{\mathsf{BS}}(\rho, \mathsf{sk}_{\mathsf{BS}})$: Compute $b \xleftarrow{\$} \mathbb{Z}_q$, $c_\sigma = (c_m \cdot c_r^y \cdot \mathsf{Enc}((x + (r_S \cdot y)) \mod q))^b \mod n$, for random $r_S \xleftarrow{\$} \mathbb{Z}_q$ and send $\beta = (c_\sigma, r_S, [b]P_1)$ to the user.

$\mathcal{U}^{(2)}_{\mathsf{BS}}(\beta, \mathsf{St}_{\mathsf{BS}}, \mathsf{pk}_{\mathsf{BS}})$: Decrypt ciphertext c_σ receiving integer $t = b \cdot (Co + r_S \cdot y + ((x + (r_S \cdot y)) \mod q))$, compute $s = ([t^{-1}]([b]P_1)$ (so $s = [\frac{1}{Co+x+(r_S+r_U)\cdot y}]P_1$), $r = r_S + r_U$ and set $\sigma_{\mathsf{BB}} = (s, r)$. Return $\perp$ if $\mathsf{Verify}_{\mathsf{BB}}(Co, \sigma_{\mathsf{BB}}, \mathsf{pk}_{\mathsf{BB}}) = 0$; otherwise return $\sigma = (Co, o_{Co}, \sigma_{\mathsf{BB}})$.

$\mathsf{Verify}_{\mathsf{BS}}(m, \sigma, \mathsf{pk}_{\mathsf{BS}})$: return 1 iff $\mathsf{Verify}_{\mathsf{BB}}(Co, \sigma_{\mathsf{BB}}, \mathsf{pk}_{\mathsf{BB}}) = 1$ and $m = \mathsf{Open}_{\mathsf{P}}(Co, m, o_{Co})$.

Scheme 1: Our Blind Signature Scheme

cryptosystem was generated in such a way that $p_n > 3 \cdot q^2$, we have that $t = b \cdot (Co + r_S \cdot y + ((x + (r_S \cdot y)) \mod q))$ over $\mathbb{Z}$ and $t = b \cdot (Co + r_S \cdot y + ((x + (r_S \cdot y))$ in $\mathbb{Z}_q$. Thus, by computing $([t^{-1}]([b]P_1)$, the user receives $s = [\frac{1}{Co+x+(r_S+r_U)\cdot y}]P_1)$. It follows, that $\sigma_{\mathsf{BB}} = (s, r)$ (where $r = r_S + r_U$) is a valid BB signature on Co and $\mathsf{Verify}_{\mathsf{BB}}(Co, \sigma_{\mathsf{BB}}, \mathsf{pk}_{\mathsf{BB}}) = 1$. It remains to show that $m = \mathsf{Open}_{\mathsf{P}}(Co, m, o_{Co})$ but this follows from the correctness of Pedersen commitments.

Theorem 2 (Unforgeability). *If BB signatures are secure against strong existential forgery under an adaptive chosen message attack, Pedersen commitments from Definition 3 are computationally binding and the knowledge of factor assumption holds, then Scheme 1 is strongly unforgeable.*

Proof (Sketch). Let $\mathcal{A}$ be a PPT adversary that breaks the strong unforgeability of Scheme 1. We now show that we can construct a reduction $\mathcal{R}$ that, using $\mathcal{A}$ as a procedure, either breaks the strong existential unforgeability of the BB signature scheme or computational binding of the Pedersen commitment scheme. To break strong unforgeability the adversary $\mathcal{A}$ will return $k+1$ pairs $(m_i^*, \sigma_i^*)_{i=1}^{k+1} = (m_i^*, (Co_i^*, o_{Co_i}^*, \sigma_{\mathsf{BB},i}^*))_{i=1}^{k+1}$, where k is the number of queries made to the signing oracle. We now distinguish two cases leading to two different strategies followed by $\mathcal{R}$ and a different target of the attack:

Case 1: all commitments $Co_1^*, \ldots, Co_{k+1}^*$ are distinct,
Case 2: there exist $i, j \in \{1, \ldots, k+1\}$, $i \neq j$ for which $Co_i^* = Co_j^*$.

In the first option $\mathcal{R}$ aims to break the unforgeability of the BB signature scheme hoping that all commitments created by $\mathcal{A}$ will be different (if it turns to be false, then the attack fails). $\mathcal{R}$ interacts with $\mathcal{A}$ simulating the environment for the blind signature scheme; at the same time $\mathcal{R}$ uses a BB signing oracle. First, $\mathcal{R}$ computes the commitment key $\mathsf{cpp} \leftarrow \mathsf{Setup_P}(1^\lambda, q)$ but uses the public key $\mathsf{pk_{BB}} = (P_1, P_2, u = [x]P_2, v = [y]P_2)$ from the unforgeability game. It outputs $\mathsf{pk_{BS}} = (1^\lambda, \mathsf{cpp}, \mathsf{pk_{BB}})$ as its public key for the blind signature scheme. To perfectly simulate the signing queries for this public key, $\mathcal{R}$ extracts Co and r_U from the queries of $\mathcal{A}$. Note that under the knowledge of factor assumption $\mathcal{R}$ can extract the secret key and decrypt those values from c_m and c_r, respectively. Then $\mathcal{R}$ queries Co to its signing oracle, receiving a BB signature (s, r) on Co, where $s = [\frac{1}{Co+x+r \cdot y}]P_1$. The reduction computes $r_S = r - r_U$, chooses $t \xleftarrow{\$} \mathbb{Z}_{3 \cdot q^2}$, computes $s' = [t]s$ and $c_\sigma = \mathsf{Enc}(t)$. $\mathcal{R}$ answers the query by returning (c_σ, r_S, s'). Note that $\mathcal{A}$ will receive a valid signature under Co. Finally, $\mathcal{R}$ returns $(Co_i^*, \sigma_{\mathsf{BB},i}^*)_{i=1}^{k+1}$ and breaks the strong existential unforgeability of BB signatures.

On the other hand, in order to perform an attack in Case 2, $\mathcal{R}$ breaks the binding property of the Pedersen commitment scheme. The reduction uses the commitment key $\mathsf{cpp} = (\mathbb{G}, P, Q, q_\mathsf{P})$ from the binding game but computes the BB signature public key $\mathsf{pk_{BB}}$ according to the protocol. Note that this time the signing key is known to $\mathcal{R}$ and all signing queries of $\mathcal{A}$ can be answered according to the protocol. However, at the end $\mathcal{A}$ outputs the above $k+1$ pairs. If Case 2 occurs, then there exist $i, j \in \{1, \ldots, k+1\}$, $i \neq j$ for which $Co_i^* = Co_j^*$. It follows, that by returning $(m_i^*, o_{Co_i}^*), (m_j^*, o_{Co_j}^*)$ the reduction $\mathcal{R}$ breaks the computational binding of the Pedersen commitment scheme.

Theorem 3 (Blindness). *If the Okamoto-Uchiyama cryptosystem is indistinguishable under chosen plaintext attack and the Pedersen commitment is perfectly-hiding, then Scheme 1 is blind in the honest-signer model.*

Proof (Sketch). We commence with the observation that if the adversary receives $(\perp, \perp)$, then due to perfect hiding property of Pedersen commitments the adversaries advantage in the blindness experiment is 0. To have a non-negligible advantage, the adversary must receive valid signatures (σ_0, σ_1). Thus, we assume that the adversary always receives valid signatures in the blindness experiment. We will show that advantage of adversary $\mathcal{A}$ in winning the blindness experiment cannot be greater than the advantage of any adversary against CPA security of the Okamoto-Uchiyama cryptosystem. The idea is that we construct a reduction $\mathcal{R}$ that plays the semantic security experiment and wins it with the same probability as $\mathcal{A}$ wins the blindness experiment. The steps of $\mathcal{R}$ are the following. First, it returns the bits 0 and 1 as the messages to be encrypted in the CPA experiment. As a result, $\mathcal{R}$ receives the public key $\mathsf{pk_{Enc}} = (n, g_n, h_n)$ and a ciphertext $C_b = \mathsf{Enc}(b)$, for an unknown bit b. The adversary $\mathcal{A}$ returns m_0, m_1. Using those values, the reduction computes two commitments $(Co_0, o_{Co_0}) = \mathsf{Commit}_{\mathsf{P}}(m_0, r_{Co_0})$, $(Co_1, o_{Co_1}) = \mathsf{Commit}_{\mathsf{P}}(m_1, r_{Co_1})$ and two ciphertexts: $C_0 = \mathsf{Enc}(Co_0 \cdot (1-b) + Co_1 \cdot b)$ and $C_1 = \mathsf{Enc}(Co_0 \cdot b + Co_1 \cdot (1-b))$. Note that using the partially homomorphic property of the cryptosystem, $\mathcal{R}$ can compute both values. Now depending on the bit b we have $C_0 = \mathsf{Enc}(Co_0), C_1 = \mathsf{Enc}(Co_1)$ if $b = 0$ and $C_0 = \mathsf{Enc}(Co_1), C_1 = \mathsf{Enc}(Co_0)$ if $b = 1$. The reduction then uses C_0 as a ciphertext of the message c_m in the first and C_1 in the second interaction. However, instead of using the values ρ_0 and ρ_1 returned by $\mathcal{A}$, the reduction computes the signatures (on Co_0 and Co_1) itself as it knows the signing key. Finally, $\mathcal{R}$ returns the bit outputted by $\mathcal{A}$.

Remark 1. Note that if we would sign the actual message m, instead of a commitment to it, then there exists an adversary that can win the blindness game with non-negligible advantage. The adversary guesses the correct bit b and computes (β_0, β_1) in such a way that procedure $\mathcal{U}^{(2)}_{\mathsf{BS}}$ aborts (with the adversary receiving $(\perp, \perp)$) if the b is guessed wrong and returns a valid signature if bit b was correct. Due to space reasons we omit the details of this oracle attack and describe it in more detail in the full version of this article.

On the other hand, Scheme 1 prevents such an attack using perfectly-hiding commitments. In particular, if the adversary does not receive the openings to the commitments, then its advantage cannot be greater then 0 (as both events are equally probable). This idea is used in the first paragraph of the sketch of the proof. Note that this idea also applies in case of blindness with selective-failure attacks [5], where the adversary is given $(\epsilon, \perp)$ (or $(\perp, \epsilon)$) in case one of the execution succeeded and the second one failed.

5 Conclusions

We have proposed a fairly practical two-move blind signature without random oracles and a common reference string. It is efficient in terms of signature size and communication complexity. For a future work we plan to extend blindness to the malicious-signer model, where the adversary generates the signing key. One promising approach is to use the knowledge of exponent assumption to extract the signer's secret key as it only consists of one public value P_1 and two discrete logarithms of the public values X and Y to the base P_2. Moreover, we plan to extend our construction to partially blind signatures, where the signer and the user share some information (e.g. expiration date of the document) and this information is included in the signature.

Acknowledgments. We would like to thank prof. Mirosław Kutyłowski and the anonymous reviewers of FC for their valuable comments on this short paper. This research was supported by the National Science Centre (Poland) based on decision no. 2014/15/N/ST6/04577.

References

1. Barbosa, M., Farshim, P.: Strong knowledge extractors for public-key encryption schemes. In: Steinfeld, R., Hawkes, P. (eds.) ACISP 2010. LNCS, vol. 6168, pp. 164–181. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14081-5_11. http://dblp.uni-trier.de/db/conf/acisp/acisp2010.html#BarbosaF10a
2. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006). doi:10.1007/11693383_22. http://dblp.uni-trier.de/db/conf/sacrypt/sacrypt2005.html#BarretoN05
3. Bellare, M., Palacio, A.: The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 273–289. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_17. http://www.iacr.org/cryptodb/archive/2004/CRYPTO/961/961.pdf
4. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol. **21**(2), 149–177 (2008). http://dblp.uni-trier.de/db/journals/joc/joc21.html#BonehB08
5. Camenisch, J., Neven, G., Shelat, A.: Simulatable adaptive oblivious transfer. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 573–590. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72540-4_33
6. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) CRYPTO 1982, pp. 199–203. Springer, Heidelberg (1982)
7. Fischlin, M.: Round-optimal composable blind signatures in the common reference string model. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 60–77. Springer, Heidelberg (2006). doi:10.1007/11818175_4
8. Fischlin, M., Schröder, D.: On the impossibility of three-move blind signature schemes. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 197–215. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_10
9. Fuchsbauer, G., Hanser, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model. Cryptology ePrint Archive, Report 2015/626 (2015). http://eprint.iacr.org/
10. Garg, S., Gupta, D.: Efficient round optimal blind signatures. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 477–495. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_27
11. Garg, S., Rao, V., Sahai, A., Schröder, D., Unruh, D.: Round optimal blind signatures. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 630–648. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22792-9_36
12. Meiklejohn, S., Shacham, H., Freeman, D.M.: Limitations on transformations from composite-order to prime-order groups: the case of round-optimal blind signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 519–538. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_30
13. Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 308–318. Springer, Heidelberg (1998). doi:10.1007/BFb0054135