Partially blind Boneh-Boyen signatures

Sietse Ringers[1], Wouter Lueks[2], and Jaap-Henk Hoepman[2]

[1] Johann Bernoulli Institute for Mathematics and Computer Science, University of Groningen, The Netherlands
s.ringers@rug.nl
[2] Radboud University, Nijmegen, The Netherlands
{jhh,e.verheul}@cs.ru.nl

Abstract. In a partially blind signature scheme, one part of the message being signed is hidden from the signer, together with the resulting signature, while another part of the message is visible to the signer. In this paper we present a partially blind scheme for a signature scheme that is closely related to Boneh-Boyen signatures. As an application, we introduce a single-show attribute-based credential scheme with short signatures.

1 Introduction

A blind signature scheme is a signature scheme together with an issuing protocol, which is such that the signer learns neither the message that it signs nor the resulting signature. First introduced by Chaum [Cha83], blind signatures are used in, for example, electronic cash schemes (e.g., [CFN90]), electronic voting (e.g., [JC97]), and unlinkable credentials (e.g., [Cha90; Bra00]).

It can, however, be a problem that the signer has no knowledge or control whatsoever over the message that he signs; for example, there is no way in which it could impose an expiry date. In these cases one could use a *partially* blind signature scheme [AO00], in which one part of the message remains hidden but another part is visible to the signer. The known part of the message, called *common information*, can then be used for common information that the signer and signer agree upon in advance.

In this paper we present and give a full security proof of a partially blind issuing protocol for a signature scheme that is closely related to the Boneh-Boyen signature scheme [BB08] (which, if no common information is included, reduces to a blind signature scheme for actual Boneh-Boyen signatures). The Boneh-Boyen signature scheme produces very short signatures, and their security does not rely on the Random Oracle model (ROM). They have found applications in, for example, attribute-based signatures [MPR11], group signatures [Gro07], and verifiable random functions [DY05]. We expect that the ability to hide (part of) the message and the resulting signature from the issuer will allow many more applications, especially within privacy-sensitive areas such as the ones mentioned earlier, or in which the issuer is not fully trusted. As an example

of this, in the final section we briefly describe a single-show attribute-based credential scheme [Bra00], that has short signatures, provable unforgeability that does not rely on the Random Oracle Model, an efficient showing protocol, and single-show issuer unlinkability.

We define our scheme and its signing protocol in Section 4, after having fixed notations and discussed some preliminaries in Section 2, and the Boneh-Boyen signature scheme itself in Section 3. In Section 5, we prove that our scheme is indeed partially blind and unforgeable. Next, in Section 6 we discuss how our scheme relates to the Boneh-Boyen scheme, and how it can be generalized to allow multiple pieces of common information. Finally, in the same section we describe as an example of our scheme a single-show attribute-based credential scheme.

2 Preliminaries

First we fix some notation. We denote algorithms with calligraphic letters such as $\mathcal{A}$ and $\mathcal{B}$. By $y \leftarrow \mathcal{A}(x)$ we denote that y was obtained by running $\mathcal{A}$ on input x. If $\mathcal{A}$ is a deterministic algorithm then y is unique; if $\mathcal{A}$ is probabilistic then y is a random variable. If $\mathcal{A}$ and $\mathcal{B}$ are interactive algorithms, we write $a \leftarrow \mathcal{A}(\cdot) \leftrightarrow \mathcal{B}(\cdot) \rightarrow b$ when $\mathcal{A}$ and $\mathcal{B}$ interact and afterwards output a and b, respectively. Finally, $|x|$ denotes the length of x in bits. For example, if x is an integer then $|x| = \lceil \log_2 x \rceil$.

For zero-knowledge proofs we will use the Camenisch-Stadler notation [CS97]: for example,

$$\mathrm{PK}\big\{(k_1, k_2) \colon K = P_1^{k_1} P_2^{k_2}\big\}$$

denotes a zero-knowledge proof of knowledge of the numbers k_1, k_2 that satisfy the relation $K = P_1^{k_1} P_2^{k_2}$. (We will, however, not switch to Greek letters to denote the variables of which knowledge is proved.)

2.1 Partially blind signature schemes

A partially blind signature scheme is made up of three algorithms: KeyGen, Sign, and Verify, for generating keys, signing, and verifying signatures, respectively. For a fixed security parameter k, these algorithms work as follows:

KeyGen(1^k) outputs a random key pair (SK, PK).

Sign This is an interactive protocol between the signer $\mathcal{S}$ and a user $\mathcal{U}$ that results in a signature σ on the hidden message $m \in \mathcal{M}$ and common information $i \in \mathcal{I}$:

$$\mathcal{S}(SK, i) \leftrightarrow \mathcal{U}(PK, m, i) \rightarrow \sigma.$$

Verify(m, i, σ, PK) takes a public key PK, messages $m \in \mathcal{M}, i \in \mathcal{I}$, and a signature σ, and returns `valid` or `invalid`.

In the next two games, we define the security notions for partially blind signature schemes [AO00].

Definition 1 (Blindness). This is a game between an adversarial signer $\mathcal{A}$ and a user $\mathcal{U}$ that is controlled by the challenger. The goal of the adversary is to see whether it is signing a message that it chose itself, or a random message chosen by the challenger. The game proceeds as follows.

Setup Adversary $\mathcal{A}$ runs $(SK, PK) \leftarrow \mathsf{KeyGen}(1^k)$ and chooses a message-pair $m \in \mathcal{M}, i \in \mathcal{I}$. It sends PK, m and i to the challenger.

Run The challenger chooses a bit $d \in_R \{0,1\}$, sets $m_0 = m$ and $m_1 \in_R \mathcal{M}$, and gives m_d and i to the user $\mathcal{U}$. The user $\mathcal{U}$ engages with the adversary in the signing protocol on messages m_d and i.

Result If the user output a signature σ at the end of the signing protocol, then it is sent to the adversary.

Guess Adversary $\mathcal{A}$ outputs his guess $d' \in \{0,1\}$. It wins if $d = d'$ and if $\mathcal{U}$ produced a valid signature.

We say that a signer (t, ϵ)-breaks the blindness of a signature scheme if it can win this game with advantage ϵ in time t.

We have chosen for a real-or-random game here, because this form of the game is best suited for our needs when we are proving that our blind Boneh-Boyen issuing protocol is indeed blind in section 5.1. This game is equivalent to the real-or-real game, in which the adversary outputs two messages m_0 and m_1 (along with i), which are given to two users, after which it has to guess which user received which message. For probabilistic encryption schemes, whose security game closely resembles the one above, we have proven this equivalence in Appendix A.

Notice that the game guarantees unlinkability only if the common information i is the same for both the real message m_0 and the random message m_1, otherwise the adversary could use i to trivially link the signature with its view of the Sign protocol.

Definition 2 (Unforgeability under chosen-message attacks). We define unforgeability under chosen-message attacks of a partially blind signature scheme in terms of the following game. It is a game between an adversarial user $\mathcal{A}$ and a signer $\mathcal{S}$, controlled by the challenger. The game proceeds as follows.

Setup The challenger generates a private-public key pair $(SK, PK) \leftarrow \mathsf{KeyGen}(1^k)$. It sends PK the adversary $\mathcal{A}$.

Queries The adversary and challenger engage in the Sign protocol over at most q message-pairs $(m_j, i_j) \in \mathcal{M} \times \mathcal{I}$ that are chosen adaptively by the adversary. The runs of the Sign protocol may be arbitrarily interleaved as the adversary sees fit. Each time, the challenger sends the resulting signature σ_i to the adversary.

Output The adversary $\mathcal{A}$ outputs a triple (m, i, σ) and wins the game if σ is a valid signature over m and i, and $(m, i, \sigma) \neq (m_j, i_j, \sigma_j)$ for all $1 < j < q$.

We say that our signature scheme is (t, q, ϵ)-existentially unforgeable under chosen message attacks if there exists no probabilistic polynomial-time algorithm that can win the above game with probability ϵ, running in time at most t and making at most q signature queries. In this game the adversary can let each message on which it queries the challenger depend on the public key, and on the previous messages. Notice that it suffices for the adversary to output any new triple (m, i, σ); for example, it could be that σ is a new signature over an already seen message m_j or even message-pair (m_j, i_j), or perhaps the message pair is new but $\sigma = \sigma_j$ for some j. In these cases, the adversary still wins.

2.2 Known-message attacks for signature schemes

We will reduce the unforgeability (in terms of the game above) of our partially blind signature scheme to the unforgeability of weak Boneh-Boyen signatures. This signature schemes satisfies a weaker form of unforgeability, in the sense that the adversary has to send the messages that it wants signed before it receives the public key. The relevant game is as follows [GMR88].

Definition 3 (Unforgeability under known-message attacks). We define unforgeability under known-message attacks of a (non-blind) signature scheme in terms of the following game. It is a game between an adversarial user $\mathcal{A}$ and a signer $\mathcal{S}$, controlled by the challenger. The game proceeds as follows.

Announcement The adversary $\mathcal{A}$ announces at most q messages $m_1, \ldots, m_q \in \mathcal{M}$ that it wants signed.

Response The challenger generates a private-public key pair $(SK, PK) \leftarrow \mathsf{KeyGen}(1^k)$. It generates q signatures $\sigma_i \leftarrow \mathsf{Sign}(m_i, SK)$ over the messages m_i that $\mathcal{A}$ chose earlier. It sends PK and the signatures σ_i to $\mathcal{A}$.

Output The adversary $\mathcal{A}$ outputs a pair (m, σ) and wins the game if σ is a valid signature over m, and $(m, \sigma) \neq (m_i, \sigma_i)$ for all $1 < i < q$.

We say that our signature scheme is (t, q, ϵ)-existentially unforgeable under known message attacks if there exists no probabilistic polynomial-time algorithm that can win the above game with probability ϵ, running in time at most t and sending at most q messages in the Announcement phase.

2.3 Bilinear group pairs

A bilinear group pair (G_1, G_2) consists of two (additively written) cyclic groups, both of prime order p, such that there exists a a *bilinear map* or *pairing*; that is, a map $e\colon G_1 \times G_2 \to G_T$ (with G_T a multiplicative group of order p) satisfying the following properties:

1. *Bilinearity*: for all $G, G' \in G_1$ and $H, H' \in G_2$ we have $e(G + G', H) = e(G, H)e(G', H)$ and $e(G, H + H') = e(G, H)e(G, H')$.
2. *Non-degeneracy*: The element $e(P, Q)$ is a generator of G_T (i.e., $e(P, Q) \neq 1$).

3. *Computability*: There exists an efficient algorithm for computing $e(G, H)$ for any $G \in G_1$, $H \in G_2$.

Such pairing exist for some special classes of elliptic curves. We only consider only Type 3 pairings, that is, bilinear group pairs such that there is no efficiently computable isomorphism either from G_1 to G_2 or vice versa. Such pairings exist for particular types of elliptic curves; we mention for example [BN06; MNT01]. For more information about bilinear group pairs and pairings we refer to [GPS08]; see also, for example, Chapters I and X from [BSS05].

We denote the generators of G_1 and G_2 with $P \in G_1$, $Q \in G_2$ respectively. We consider the coefficient k of a group element $K = kP$ to be elements of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

3 The Boneh-Boyen signature scheme

There are two versions of the Boneh-Boyen signature scheme [BB08]: a nondeterministic one that is unforgeable under chosen-message attacks, and one that is unforgeable under known-message attacks and deterministic. We describe the former one first.

KeyGen(1^k) Generate a Type 3 bilinear group pair (G_1, G_2), such that $|p| = k$. Pick two generators $P \in G_1$, $Q \in G_2$. Choose two private keys $a, b \in \mathbb{Z}_p^*$, and set $A = aP$ and $B = bP$. The public key is the description of the bilinear group pair, together with (p, e, P, Q, A, B).

Sign(m, a, b) Choose a random value $r \in \mathbb{Z}_p \setminus \{-\frac{a+m}{b}\}$ and compute $S = \frac{1}{a+m+rb}Q$ (the inverses are calculated modulo p). The signature is the pair (S, r).

Verify(m, A, B) Using the bilinear pairing e, verify that $e(A + mP + rB, S) = e(P, Q)$. Return `true` if and only if this equation holds.

If the signature was correctly generated, then

$$e(A + mP + rB, S) = e\left((a + m + rb)P, \frac{1}{a + m + rb}Q\right) = e(P, Q)$$

so that the signature will verify.

We will refer to this scheme as the strong Boneh-Boyen signature scheme. The weak Boneh-Boyen signature scheme is obtained by setting $r = 0$ and removing b and B from the private and public keys, respectively. Thus, a weak Boneh-Boyen signature on the message $m \in \mathbb{Z}_p$ would be $C = \frac{1}{a+m}Q$. This signature scheme is unforgeable under known-message attacks in the sense of Definition 3. Boneh and Boyen prove the unforgeability of their strong scheme by reducing it to that of their weak scheme. The unforgeability of the weak scheme, in turn, relies on the q-Strong Diffie-Hellman assumption, which says the following:

> Given as input a $(q+3)$-tuple of elements $(P, xP, x^2P, \ldots, x^qP, Q, xQ) \in G_1^{q+1} \times G_2^2$, it is intractable to output a pair $\left(d, \frac{1}{x+d}P\right) \in \mathbb{Z}_p \times G_1$ for a freely chosen value $d \in \mathbb{Z}_p \setminus \{-x\}$.

For a more elaborate description of the signature scheme and its properties, we refer to the paper by Boneh and Boyen [BB08] in which it was introduced.

4 The partially blind Boneh-Boyen scheme

In order to include the common information $i \in \mathcal{I}$, we first extend the Boneh-Boyen signature scheme as follows (resulting in a special case of the signature scheme called GSBB, for Generalized Strong Boneh-Boyen, from [Bha+09]). We take the strong Boneh-Boyen signature scheme and include $c \in \mathbb{Z}_p^*$ and $C = cP$ in the private and public keys, respectively, i.e.,

$$SK = (a, b, c), \qquad PK = (p, e, P, Q, A, B, C).$$

The message-space $\mathcal{M}$ and space of common information $\mathcal{I}$ both are $\mathbb{Z}_p$. For $m, i \in \mathbb{Z}_p$, a signature will be $(S, r) \in G_2 \times \mathbb{Z}_p$, where

$$S = \frac{1}{a + m + rb + ic} Q.$$

The signature is valid only if

$$e(A + mP + rB + nC, S) = e(P, Q).$$

The private keys a, b, c of the signer, as well as the messages m, i and randomness r of a signature are all elements of $\mathbb{Z}_p$. In the following, we will have to embed these elements in the message space of the Paillier encryption scheme [Pai99], which is $\mathbb{Z}_n$ (for some n that we will take to be much larger than p). We do this simply by taking the lowest representative, which we will denote by the same letter in the definition below. Thus, the elements a, b, c, m, i, r and also β should be considered as ordinary integers. Near the end of the protocol (in step 3), there will be a reduction modulo p that restores them as elements of $\mathbb{Z}_p$.

Definition 4. To obtain a signature on a message m and common information i (on which the user and signer agreed in advance), the user and the signer (who knows the private keys a, b, c), interact in the following way (see also Figure 1).

1. The user generates a new Paillier encryption system (n, g, λ) such that n is at least $2^l p^3$, where 2^{2-l} is an acceptable failure rate. Then, it generates a blinding factor $\beta \in_R \{1, \ldots, p\}$ and a randomizer $r_1 \in_R \{1, \ldots, p\}$ for use in the resulting signature, and sets $B = [\![\beta]\!]$ and $R = [\![\beta r_1]\!]$. It sends n, g, B, R to the signer, and proves that B and R are constructed correctly using

   $$\mathrm{PK}\{(\beta, r_1, \rho_1, \rho_2) : B = g^\beta \rho_1^n \bmod n^2 \ \wedge \ R = g^{\beta r_1} \rho_2^n \bmod n^2\}.$$

   (For how to perform such a proof, see [CDN01]).
2. If the proof is correct the signer generates a blinding term $\gamma \in_R \mathbb{Z}_n$ and randomness $r_2 \in_R \mathbb{Z}_p$, and calculates

   $$D = B^{a + r_2 b + ic} R^b [\![\gamma]\!] \bmod n^2 = [\![\beta(a + (r_1 + r_2)b + ic) + \gamma \bmod n]\!].$$

It sends D to the user and proves that it constructed D correctly using

$$\mathrm{PK}\{(a, b, c, r_2, \gamma, \rho_3) : D = B^{a+r_2 b+ic} R^b g^\gamma \rho_3^n \bmod n^2\}.$$

3. The user calculates

$$\tilde{s} = \mathsf{Decrypt}(D) + \beta m \bmod n = \beta(a + m + (r_1 + r_2)b + ic) + \gamma \bmod n,$$

and sends $\hat{s} = \tilde{s} \bmod p$ to the signer (here, the reduction modulo p is done by taking the lowest representative of $\tilde{s}$).
4. The signer removes γ by calculating $s = \hat{s} - (\gamma \bmod p) = \beta(a + m + (r_1 + r_2)b + ic) \bmod p$, and sends $\overline{S} = \frac{1}{c}Q$ together with r_2 to the user.
5. Finally, the user unblinds the signature to obtain $S = \beta\overline{S}$. Setting $r = r_1 + r_2$, it accepts if (S, r) is a valid signature on m and i.

The protocol is summarized in Figure 1.

Common information: Boneh-Boyen public key (e, p, P, Q, A, B, C), common information $i \in \mathcal{I}$		
User		**Signer**
knows message $m \in \mathbb{Z}_p$		knows secret keys $a, b \in \mathbb{Z}_p$
	Phase 1	
Generate Paillier n, λ, g		
Choose $\beta, r_1 \in_R \mathbb{Z}_p^*$		
send n, g, $[\![\beta]\!]$, $[\![\beta r_1]\!]$	$\longrightarrow$	into n, g, B, R
$\mathrm{PK}\{(\beta, r_1, \rho_1, \rho_2) : B = g^\beta \rho_1^n \bmod n^2 \ \wedge \ R = g^{\beta r_1} \rho_2^n \bmod n^2\}$		
	Phase 2	
		choose $\gamma \in_R \mathbb{Z}_n$, $r_2 \in_R \mathbb{Z}_p$
into D	$\longleftarrow$	send $B^{a+r_2 b+ic} R^b [\![\gamma]\!]$
$\mathrm{PK}\{(a, b, c, r_2, \gamma, \rho_3) : D = B^{a+r_2 b+ic} R^b g^\gamma \rho_3^n \bmod n^2\}$		
	Phase 3	
set $E \leftarrow \mathsf{Decrypt}(D)$		
send $E + \beta m \bmod p$	$\longrightarrow$	into $\hat{s}$
	Phase 4	
		set $s = \hat{s} - (\gamma \bmod p)$
into $\overline{S}, r_2$	$\longleftarrow$	send $\frac{1}{s}Q, r_2$
	Phase 5	
set $S = \beta\overline{S}, \ r = r_1 + r_2$		
$\mathsf{Verify}(m, i, S, PK)$		
return (S, r)		

Fig. 1. Our interactive partially blind signing protocol from Definition 4.

Proposition 5. *The blind Boneh-Boyen signature scheme as described in Definition 4 is correct with overwhelming probability.*

Proof. If both the user and the signer follow the protocol, then at the start of step 3 the user can calculate $\tilde{s} = \beta(a+m+(r_1+r_2)b+ic)+\gamma \bmod n$. We denote the lowest representative of $\tilde{s}$ by s', and that of γ by γ', and we set $r = r_1 + r_2$. Now, in step 3 the user sends $\hat{s} = s' \bmod p$ to the signer. This will result in a valid Boneh-Boyen signature only if $s' = \beta(a + m + rb + ic) + \gamma'$, which in turn will only hold if

$$\beta(a + m + rb + ic) + \gamma' < n.$$

The maximum value of the left hand side of this inequality is $p(p + p + (p + p)p + p^2) + n = 2p^2 + 3p^3 + n$. Thus the chance that the inequality does *not* hold satisfies

$$\begin{aligned} P\Big(\beta(a + m + rb + ic) + \gamma' > n\Big) &< \frac{2p^2 + 3p^3}{2p^2 + 3p^3 + n} \\ &< \frac{4p^3}{2p^2 + 3p^3 + 2^l p^3} < \frac{4p^3}{2^l p^3} < 2^{2-l}. \end{aligned}$$

Thus with chance at least $1 - 2^{2-l}$, we have $\hat{s} = s' \bmod p = \beta(a+m+rb+ic)+\gamma' \bmod p$, which will result in a valid signature.

5 Blindness and unforgeability

5.1 Blindness

We will reduce the partial blindness of our issuing protocol to the real-or-random indistinguishability of the Paillier encryption scheme. We define this kind of indistinguishability below, and prove in Appendix A that it is equivalent with left-or-right indistinguishability under chosen plaintext attacks.

Definition 6 (Real-or-random indistinguishability (ROR-CPA)). Let $(\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a public key encryption scheme. The ROR-CPA game goes as follows.

Setup The challenger runs $(SK, PK) \leftarrow \mathsf{KeyGen}(1^k)$ for some security parameter k, and gives PK to the adversary.

Query The challenger chooses a message $m \in \mathcal{M}$ and sends it to the challenger. The challenger chooses a bit $b \in_R \{0, 1\}$, sets $m_0 = m$ and chooses a random message m_1. It sends $\mathsf{Encrypt}(PK, m_d)$ to the adversary.

Result The adversary returns his guess d'. It wins if $d' = d$.

We say that an adversary (t, ϵ)-breaks the real-or-random indistinguishability under chosen plaintext attacks if it has advantage at least ϵ and runs in time t.

In order to prove partial blindness of our issuing protocol, first we argue that the advantage of no adversarial signer can depend on the ciphertext $[\![\beta]\!]$ that it receives in the first step of the issuing protocol (see Definition 4).

Definition 7. We say that a user sends *the correct* B in the first step of the issuing protocol when the plaintext β of B is the same β that occurs in the value $\hat{s} = \beta(a + m + rb + ic) + \gamma \bmod p$ that the user sends in step 3.

Proposition 8. *No adversarial signing algorithm can win the blindness game (as in Definition 1) for our blind Boneh-Boyen issue algorithm with an advantage that depends on whether the user sends him the correct B or not, provided that Paillier is ROR-CPA secure.*

Proof. Suppose that we have an adversary $\mathcal{A}_{\mathrm{BBB}}$ whose advantage at the Blind Boneh-Boyen game is ϵ_+ when the user sends the correct B, and ϵ_- when the user does not. We assume[3] $\epsilon_+ > \epsilon_-$. We build an algorithm $\mathcal{A}_{\mathrm{ROR-CPA}}$ that has an advantage $\epsilon/2$ at winning the ROR-CPA game. $\mathcal{A}_{\mathrm{ROR-CPA}}$ will act as the adversary in the ROR-CPA game, and as the user in the blindness game, as follows.

1. The challenger of $\mathcal{A}_{\mathrm{ROR-CPA}}$ outputs a Paillier public key. $\mathcal{A}_{\mathrm{ROR-CPA}}$ chooses $\beta \in \mathbb{Z}_p$ and sends it to his challenger, who responds by choosing $d \in_R \{0, 1\}$, setting $\beta_0 = \beta$ and $\beta_1 \in_R \mathbb{Z}_p$, and sending $[\![\beta_d]\!]$ to $\mathcal{A}_{\mathrm{ROR-CPA}}$.
2. $\mathcal{A}_{\mathrm{ROR-CPA}}$ engages in the signing protocol with $\mathcal{A}_{\mathrm{BBB}}$, simulating the role of the user. In step 1 of the issuing protocol it sends $B = [\![\beta_d]\!]$ that it received from his challenger. In the rest of step 1 it behaves normally (using the Paillier public key that it received from his challenger).
3. At the end of step 2, it extracts a, b, c, r_2, γ from the zero-knowledge proof performed by $\mathcal{A}_{\mathrm{BBB}}$, so that it can calculate $\hat{s} = \beta(a + m + (r_1 + r_2)b + ic) + \gamma \bmod p$ which it sends to $\mathcal{A}_{\mathrm{BBB}}$ in step 3. Thus, the value $\hat{s}$ is what it would normally be, while B is only correct if the challenger chose $d = 0$.
4. We have $\mathcal{A}_{\mathrm{ROR-CPA}}$ send guess $d' = 0$ if $\mathcal{A}_{\mathrm{BBB}}$ won and $d' = 1$ if it lost.

With probability $\frac{1}{2}$, the challenger chose $d = 0$ in step 1. In that case, $\mathcal{A}_{\mathrm{BBB}}$ has chance $\frac{1}{2} + \epsilon_+$ of winning. In the other case, when the challenger chose $d = 1$, $\mathcal{A}_{\mathrm{BBB}}$ has chance $\frac{1}{2} - \epsilon_-$ of losing (note the sign). The chance of $\mathcal{A}_{\mathrm{ROR-CPA}}$ winning is thus

$$\frac{1}{2}\left(\frac{1}{2} + \epsilon_+\right) + \frac{1}{2}\left(\frac{1}{2} - \epsilon_-\right) = \frac{1}{2} + \frac{1}{2}(\epsilon_+ - \epsilon_-)$$

meaning that the advantage of $\mathcal{A}_{\mathrm{ROR-CPA}}$ at winning the ROR-CPA game is $(\epsilon_+ - \epsilon_-)/2$. If Paillier is $(\epsilon/2)$-ROR-CPA secure, it follows that $\epsilon_+ - \epsilon_- < \epsilon$.

Theorem 9. *No adversary can break the blindness of the blind Boneh-Boyen signature scheme with advantage ϵ, provided that Paillier is $(\epsilon/2)$-ROR-CPA secure.*

Proof. The view of the signer of an issuing is

$$D = \{i, [\![\beta]\!], [\![\beta r]\!], \beta(a + m + (r_1 + r_2)b + ic) + \gamma \bmod p, \gamma, r_2\}.$$

[3] The opposite assumption does not make much sense, but with minor modifications the proof can then still be made to work.

Let us call the second, third and fourth elements of this trace B, R and $\hat{s}$ respectively, so that $D = \{i, B, R, \hat{s}, \gamma, r_2\}$. By the previous proposition, the advantage of the adversary cannot depend on the correctness of B, nor of R by the same argument. In addition, the common information i has the same value, independent from the choice for d that the challenger makes.

Therefore the only information that the signer has to work with that could possibly increase his advantage is $\hat{s}$, γ and r_2. Now it can subtract γ from $\hat{s}$ it in order to learn $s := \hat{s} - \gamma \bmod p = \beta(a + m + (r_1 + r_2)b + ic) \bmod p = \beta(a + m + rb + ic) \bmod p$. Now take another valid message-signature pair (m', S', r'). Then,

$$\beta' = \frac{\beta(a + m + rb + ic)}{(a + m' + r'b + ic)} \bmod p$$

is precisely such that $s = \beta'(a+m'+r'b+ic) \bmod p$. Therefore, $\hat{s}$ is information-theoretically hiding. The same holds for r_2; for any r' and r_2 there is an $r_1 \in \mathbb{Z}_p$ such that $r' = r_1 + r_2$.

Thus, any view can correspond to any message-signature pair.

5.2 Unforgeability

Theorem 10. *If the weak Boneh-Boyen scheme is (q, ϵ)-unforgeable under known-message attacks, then our Blind Boneh-Boyen scheme is (q, ϵ')-unforgeable under chosen-message attacks, where $\epsilon' - \epsilon$ is negligible.*

Proof. Suppose we have an adversary $\mathcal{A}$ that breaks the unforgeability of our scheme under chosen-message attacks. We will use this adversary to make a forger $\mathcal{B}$ that breaks the unforgeability of the weak Boneh-Boyen scheme under chosen-message attacks, much in the same way that Boneh and Boyen reduced the unforgeability of their strong scheme to that of the weak scheme.

$\mathcal{B}$ will do this by acting as the challenger of $\mathcal{A}$, and as the adversary in the unforgeability game for weak Boneh-Boyen signatures. We have $\mathcal{B}$ proceed as follows.

Announcement $\mathcal{B}$ chooses q messages $w_1, \ldots, w_q \in \mathbb{Z}_p$ and sends them to his challenger as the messages that it wants signed. In response, the challenger chooses a private-public key pair $a \in_R \mathbb{Z}_p$, $A = aP$ for weak Boneh-Boyen signatures, and sends A to $\mathcal{B}$, together with q signatures C_i over the messages $w_1, \ldots, w_q$.

Setup $\mathcal{B}$ generates additional private keys $b, c \in_R \mathbb{Z}_p$ and sends $A, B = bP, C = cP$ to $\mathcal{A}$.

Queries Proceeding adaptively, adversary $\mathcal{A}$ engages with $\mathcal{B}$ in the Blind Boneh-Boyen signing algorithm for q message-pairs $(m_1, i_1), \ldots, (m_q, i_q)$. When signing (m_j, i_j), we have $\mathcal{B}$ act in the following way.

- At the end of step 1, $\mathcal{B}$ extracts β, r_1 that $\mathcal{A}$ chose for message m_j from the zero-knowledge proof.

- In step 2, $\mathcal{B}$ chooses some $a' \in_R \mathbb{Z}_p$ and acts as if this is are the private key of his challenger. In addition, it acts as if $r_2 = 0$. As these values are never sent directly to the user, $\mathcal{A}$ could impossibly notice this.
- In step 4, $\mathcal{B}$ learns $\beta(a' + m_j + r_1 b + i_j c)$. As it knows all variables except for m_j, it can solve this to learn m_j. It now chooses $r_2 \in \mathbb{Z}_p$ such that $m_j + (r_1 + r_2)b + i_j c = w_j \bmod p$. For this message it received a valid signature S_j in the Announcement phase. Then, it sends $(\beta^{-1} S_j, r_2)$ back to $\mathcal{A}$ in step 4.

Output $\mathcal{A}$ sends his forgery (m, i, r, S) to $\mathcal{B}$, who sends $(m + rb + ic, S)$ to his challenger.

The output of $\mathcal{B}$ will be correct if and only if that of $\mathcal{A}$ is correct. However, $\mathcal{B}$ wins only if its output $(m + rb + ic, S)$ is new, i.e., there is no j such that $m + rb + ic = w_j$. We now show that this is so with overwhelming probability.

Indeed, suppose that with non-negligible probability, $\mathcal{B}$ produces (m, i, r, S) such that there is a j such that $m + rb + ic = w_j$. But $w_j = m_j + r_j b + i_j c$, yet the triple (m, i, r) is unequal to (m_j, i_j, r_j) because of the assumption that $\mathcal{A}$ won. Therefore,

$$0 = (m - m_j)P + (r - r_j)B + (i - i_j)C$$

is a nontrivial representation of 0 with respect to P, B, C. One can prove that being able to construct such nontrivial representations of 0 is equivalent with being able to compute discrete logarithms (see, e.g., [Bra00]).

Thus, this can only happen with negligible probability. Therefore, if $\mathcal{A}$ has advantage ϵ, then the advantage of $\mathcal{B}$ will be negligibly close to ϵ.

6 Related schemes and applications

6.1 Blind Boneh-Boyen signatures

If we include no common information by setting $i = 0$ and removing c and C from the signer's private and public key, then Figure 1 reduces to a blind issuing protocol for Boneh-Boyen signatures, and the theorems above then prove that this protocol is blind and that the scheme is unforgeable.

6.2 Generalizing to tuples of common information

We can also go the other way, and generalize our scheme to including more than one piece i of common information. Let the signer's secret key contain not $c \in \mathbb{Z}_p^*$ but a tuple of numbers $c_1, \ldots, c_t \in \mathbb{Z}_p^*$ (and the public key contains not C but $C_1 = c_1 P, \ldots, C_t = c_t P$). Then the signer can sign a hidden message m and tuple $i_1, \ldots, i_t$ by setting

$$D = B^{\delta} R^b [\![\gamma]\!] \qquad \text{with} \qquad \delta = a + r_2 b + \sum_{k=1}^{t} i_k c_k$$

in step 2 of the Sign protocol. The resulting signature (S, r) over $(m, i_1, \ldots, i_t)$ is then valid only if

$$e\left(A + mP + rB + \sum_{k=1}^{t} i_k C_k, S\right) = e(P, Q).$$

This results in a partially blind signature scheme for GSBB signatures [Bha+09], which is such that if one takes $t = 1$ then it reduces to the scheme from the previous sections. It is not difficult to adapt the unforgeability and blindness proofs to this scheme.

6.3 An application: single-show attribute-based credentials

In an attribute-based credential scheme, users obtain a signature from the issuer over a set of attributes (generally elements of $\mathbb{Z}_m$ for some integer m), which they can then selectively show to other parties. Well-known examples of such schemes include Idemix [CL01] and U-Prove [Bra00]. Idemix credentials are *unlinkable*: that is, multiple showings of the same credential cannot be linked to each other. By contrast, the showing protocol of U-Prove is not unlinkable (for this reason U-Prove credentials are called *single-show* credentials in the context of anonymous credentials). As a result of the lesser complexity of U-Prove's showing protocol, however, it is much more efficient than that of Idemix.

However, there is no known unforgeability proof for U-Prove credentials, and it has even been suggested that no such proof exists under any standard intractability assumption [BL13]. In addition, the showing protocol is *honest-verifier* zero-knowledge, meaning that it guarantees safety against dishonest users but not necessarily against dishonest verifiers (i.e., they might be able to learn the private key or hidden attributes, breaking the user's anonymity and possibly even allowing it to impersonate the user). Finally, U-Prove relies on the Random Oracle model. As an application of our partially blind signature scheme, we now introduce a single-show attribute-based credential scheme that suffers from none of these issues.

Issuing a credential The tuple of common information $i_1, \ldots, i_k$ will serve as the attributes of the credential, while the hidden message m will be the user's private key. The user and issuer decide in advance on the attributes $i_1, \ldots, i_k$ that the credential will have. Then the user chooses a value for m, and performs the Sign protocol with the issuer on $(m, i_1, \ldots, i_k)$. The user the receives a signature on the attributes $(i_1, \ldots, i_k)$ and private key m, which the issuer does not know. The signature together with the attributes and secret key form the credential.

Showing a credential The user can show such a credential as follows. Let $\mathcal{D} \subset \{1, \ldots, t\}$ be the index set of the attributes that the user wants to disclose, and let $\mathcal{C} = \{1, \ldots, t\} \setminus \mathcal{D}$ be the remaining attributes.

– The user sends S, r and the attributes $(i_k)_{k\in\mathcal{D}}$ that it wishes to disclose to the verifier, together with $D = mA + \sum_{k\in\mathcal{C}} i_k C_k$.
– The user performs a zero-knowledge proof of knowledge of the private key and hidden attributes:

$$\mathrm{PK}\left\{(m, (i_k)_{k\in\mathcal{C}})\colon D = mA + \sum_{k\in\mathcal{C}} i_k C_k\right\}.$$

– The verifier checks that the signature (S, r) is valid as follows:

$$e\left(A + mP + rB + D + \sum_{k\in\mathcal{D}} i_k C_k, S\right) \stackrel{?}{=} e(P, Q).$$

Theorem 10 then guarantees unforgeability of these credentials. In addition, as a consequence of Theorem 9, issuer-unlinkability is provided in the following sense: if in two executions of the showing protocol outlined above, the same attributes with the same values were disclosed, and the traces of the two executions are sent to the issuer, then the issuer cannot tell if those two executions came from one and the same or from two distinct credentials. Furthermore, assuming that a black-box zero-knowledge proof of knowledge is used such as the one from [CDM00] (instead of the Schnorr Σ-protocol, which is only honest-verifier zero-knowledge), it is impossible for the verifier to learn the secret key or hidden attributes. Finally, contrary to U-Prove the scheme does not rely on the Random Oracle Model.

This results in a credential scheme of which the length of the signatures and the efficiency of the showing protocol is comparable with U-Prove. Although the issuing protocol is not as efficient as that of U-Prove, stronger security guarantees are provided.

7 Conclusion

By providing a partially blind issuing protocol for Boneh-Boyen-like signatures and proving its security, we have enabled applications of these signatures in situations where it is important that the issuer does not learn (part of) the message being signed as well as the resulting signature. As an example of the simplicity and flexibility of our scheme, we have introduced a single-show attribute-based credential scheme that is an improvement over its well-known predecessor U-Prove in almost every way, and we hope to see many more such applications in the future.

References

[AO00] M. Abe and T. Okamoto. "Provably Secure Partially Blind Signatures". In: *Advances in Cryptology – CRYPTO 2000*. Ed. by M. Bellare. Vol. 1880. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2000, pp. 271–286 (cit. on pp. 1, 3).

[BB08] D. Boneh and X. Boyen. "Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups". In: *J. Cryptology* 21.2 (2008), pp. 149–177 (cit. on pp. 1, 5, 6).

[Bha+09] R. Bhaskar, K. Chandrasekaran, S. V. Lokam, P. L. Montgomery, R. Venkatesan, and Y. Yacobi. "An Observation about Variations of the Diffie-Hellman Assumption". In: *Serdica Journal of Computing* 3 (2009) (cit. on pp. 6, 12).

[BL13] F. Baldimtsi and A. Lysyanskaya. "On the Security of One-Witness Blind Signature Schemes". In: *Advances in Cryptology - ASIACRYPT 2013*. Ed. by K. Sako and P. Sarkar. Vol. 8270. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 82–99 (cit. on p. 12).

[BN06] P. Barreto and M. Naehrig. "Pairing-Friendly Elliptic Curves of Prime Order". In: *Selected Areas in Cryptography*. Ed. by B. Preneel and S. Tavares. Vol. 3897. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, pp. 319–331 (cit. on p. 5).

[Bra00] S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, 2000 (cit. on pp. 1, 2, 11, 12).

[BSS05] I. F. Blake, G. Seroussi, and N. P. Smart, eds. *Advances in Elliptic Curve Cryptography*. Cambridge Books Online. Cambridge University Press, 2005 (cit. on p. 5).

[CDM00] R. Cramer, I. Damgård, and P. MacKenzie. "Efficient Zero-Knowledge Proofs of Knowledge without Intractability Assumptions". In: *Public Key Cryptography*. Ed. by H. Imai and Y. Zheng. Vol. 1751. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2000, pp. 354–372 (cit. on p. 13).

[CDN01] R. Cramer, I. Damgård, and J. Nielsen. "Multiparty Computation from Threshold Homomorphic Encryption". In: *Advances in Cryptology — EUROCRYPT 2001*. Ed. by B. Pfitzmann. Vol. 2045. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 280–300 (cit. on p. 6).

[CFN90] D. Chaum, A. Fiat, and M. Naor. "Untraceable Electronic Cash". English. In: *Advances in Cryptology — CRYPTO' 88*. Ed. by S. Goldwasser. Vol. 403. Lecture Notes in Computer Science. Springer New York, 1990, pp. 319–327. URL: http://dx.doi.org/10.1007/0-387-34799-2_25 (cit. on p. 1).

[Cha83] D. Chaum. "Blind Signatures for Untraceable Payments". In: *Advances in Cryptology*. Ed. by D. Chaum, R. Rivest, and A. Sherman. Springer US, 1983, pp. 199–203 (cit. on p. 1).

[Cha90] D. Chaum. "Showing credentials without identification transferring signatures between unconditionally unlinkable pseudonyms". In: *Advances in Cryptology — AUSCRYPT '90*. Ed. by J. Seberry and J. Pieprzyk. Vol. 453. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1990, pp. 245–264 (cit. on p. 1).

[CL01] J. Camenisch and A. Lysyanskaya. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation". In: *Advances in Cryptology - EUROCRYPT 2001*. 2001, pp. 93–118 (cit. on p. 12).

[CS97] J. Camenisch and M. Stadler. "Efficient group signature schemes for large groups". In: *Advances in Cryptology — CRYPTO '97*. Ed. by B. S. J. Kaliski. Vol. 1294. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1997, pp. 410–424 (cit. on p. 2).

[DY05] Y. Dodis and A. Yampolskiy. "A Verifiable Random Function with Short Proofs and Keys". In: *Public Key Cryptography - PKC 2005*. Ed. by S. Vaudenay. Vol. 3386. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, pp. 416–431 (cit. on p. 1).

[GMR88] S. Goldwasser, S. Micali, and R. L. Rivest. "A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks". In: *SIAM Journal on Computing* 17.2 (Apr. 1988), pp. 281–308 (cit. on p. 4).

[GPS08] S. D. Galbraith, K. G. Paterson, and N. P. Smart. "Pairings for cryptographers". In: *Discrete Applied Mathematics* 156.16 (2008), pp. 3113–3121 (cit. on p. 5).

[Gro07] J. Groth. "Fully Anonymous Group Signatures Without Random Oracles". In: *Advances in Cryptology – ASIACRYPT 2007*. Ed. by K. Kurosawa. Vol. 4833. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, pp. 164–180 (cit. on p. 1).

[JC97] W.-S. Juang and L. Chin-Laung. "A secure and practical electronic voting scheme for real world environments". In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 80.1 (1997), pp. 64–71 (cit. on p. 1).

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano. "New explicit conditions of elliptic curve traces for FR-reduction". In: *IEICE transactions on fundamentals of electronics, communications and computer sciences* 84.5 (2001), pp. 1234–1243 (cit. on p. 5).

[MPR11] H. Maji, M. Prabhakaran, and M. Rosulek. "Attribute-Based Signatures". In: *Topics in Cryptology – CT-RSA 2011*. Ed. by A. Kiayias. Vol. 6558. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, pp. 376–392 (cit. on p. 1).

[Pai99] P. Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by J. Stern. Vol. 1592. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1999, pp. 223–238 (cit. on p. 6).

A Ciphertext indistinguishability

In this section we will prove that left-or-right indistinguishability and real-or-random indistinguishability under chosen plaintext attacks are equivalent for asymmetric encryption schemes, in the sense that they imply each other.

Definition 11 (Left-or-right indistinguishability (IND-CPA)). Let (KeyGen, Encrypt, Decrypt) be a public key encryption scheme with message space $\mathcal{M}$. The IND-CPA game goes as follows.

Setup The challenger runs $(SK, PK) \leftarrow \mathsf{KeyGen}(1^k)$ and gives PK to the adversary.

Query The challenger chooses two messages $m_0, m_1 \in \mathcal{M}$ and sends them to the challenger. The challenger chooses a bit $d \in_R \{0, 1\}$ and sends $\mathsf{Encrypt}(PK, m_d)$ to the adversary.

Result The adversary returns his guess d'. It wins if $d' = d$.

Proposition 12. *If, for some encryption scheme, no adversary can win the IND-CPA game with advantage ϵ, then no adversary can win the ROR-CPA game with advantage ϵ.*

Proof. Suppose that there is an algorithm $\mathcal{A}_{\mathrm{ROR-CPA}}$ that can win the ROR-CPA game with advantage ϵ. Then we build an adversary $\mathcal{A}_{\mathrm{IND-CPA}}$ that can win the IND-CPA game as follows:

1. $\mathcal{A}_{\mathrm{ROR-CPA}}$ chooses $m_0 \in \mathcal{M}$ and sends it to $\mathcal{A}_{\mathrm{IND-CPA}}$, who additionally randomly chooses $m_1 \in_R \mathcal{M}$.
2. $\mathcal{A}_{\mathrm{IND-CPA}}$ sends m_0, m_1 to his challenger and receives $[\![m_d]\!]$.
3. Then it sends $[\![m_d]\!]$ to $\mathcal{A}_{\mathrm{ROR-CPA}}$.
4. Lastly, it forward $\mathcal{A}_{\mathrm{ROR-CPA}}$'s guess to challenger.

If the challenger chose $d = 0$, then $\mathcal{A}_{\mathrm{ROR-CPA}}$ will with chance $\frac{1}{2} + \epsilon$ see that the ciphertext it received corresponds with the plaintext that it chose, so that it will return $d' = 0$. Otherwise his guess will be $d' = 1$. Therefore, $\mathcal{A}_{\mathrm{IND-CPA}}$ will have advantage ϵ in winning the IND-CPA game.

Proposition 13. *If, for some encryption scheme, no adversary can win the ROR-CPA game with advantage ϵ, then no adversary can win the ROR-CPA game with advantage $\epsilon/2$.*

Proof. Suppose that there is an algorithm $\mathcal{A}_{\mathrm{ROR-CPA}}$ that can win the ROR-CPA game with advantage ϵ. Then we build an adversary $\mathcal{A}_{\mathrm{IND-CPA}}$ that can win the IND-CPA game as follows:

1. $\mathcal{A}_{\mathrm{ROR-CPA}}$ receives $m_0, m_1 \in \mathcal{M}$ from $\mathcal{A}_{\mathrm{IND-CPA}}$. It flips a bit d and sends m_d to its challenger.
2. $\mathcal{A}_{\mathrm{ROR-CPA}}$ receives either $[\![m_d]\!]$ or encrypted randomness from its challenger, and forwards this to $\mathcal{A}_{\mathrm{IND-CPA}}$.
3. If $\mathcal{A}_{\mathrm{ROR-CPA}}$ outputs a guess d' and $d = d'$ then $\mathcal{A}_{\mathrm{IND-CPA}}$ guesses 0, otherwise it guesses 1. If $\mathcal{A}_{\mathrm{ROR-CPA}}$ does not output a guess then $\mathcal{A}_{\mathrm{IND-CPA}}$ guesses randomly.

If the challenger sent $[\![m_d]\!]$ instead of encrypted randomness, then $\mathcal{A}_{\mathrm{IND-CPA}}$ will with probability $\frac{1}{2} + \epsilon$ guess d correctly. If, on the other hand, the challenger sent encrypted randomness then $\mathcal{A}_{\mathrm{IND-CPA}}$ can have no advantage. Thus, $\mathcal{A}_{\mathrm{IND-CPA}}$ guesses correctly with probability $\frac{1}{2} + \frac{\epsilon}{2}$.