Generic Construction for Identity-based Proxy Blind Signature

Xavier Bultel, Pascal Lafourcade, Charles Olivier-Anclin, Léo Robert

Generic Construction for Identity-based Proxy Blind Signature*

Xavier Bultel[1][0000−0002−8309−8984], Pascal Lafourcade[2][0000−0002−4459−511X], Charles Olivier-Anclin[2][0000−0002−9365−3259], and Léo Robert[2][0000−0002−9638−3143]

[1] LIFO, INSA Centre Val de Loire, Université d'Orléans, France
[2] Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, France

Abstract. Generic constructions of blind signature schemes have been studied since its appearance. Several constructions were made leading to generic blind signatures and achieving other properties such as identity-based blind signature and partially blind signature. We propose a generic construction for identity-based Proxy Blind Signature (IDPBS). This combination of properties has several applications in the real world, in particularly in e-voting or e-cash systems and it has never been achieved before with a generic construction. Our construction only requires two classical signatures schemes: a blind EUF-CMA blind signature and a SUF-CMA unique signature. The security of our generic identity-based proxy blind signature is proven under these assumptions.

1 Introduction

Designed in 1982 by D. Chaum [7], blind signatures are well known primitives, enabling anonymous system for banking and electronic voting. The end of the twentieth century and the beginning of the twenty-first was a golden age for blind signatures. Multiple improvements were made, *e.g.,* a scheme based on discrete logarithm proposed by J. L. Camenisch [6]. Several new properties were developed such as *proxy blind signature* [27], *partially blind signature* [2], or *fair blind signature* [25].

At the same time, identity-based cryptography has been introduced by A. Shamir in 1985 [23]. It took until 2002 to produce the first identity-based blind signature [34].

Recently, with the development of cryptocurrency and practical e-voting systems, blind signature returns to the centre of the attention. For instance self-sovereign identity is a new approach to digital identity. It gives an independent control of the identity information that are given by people when certified information needs to be provided. In particularly, it addresses the difficulty of establishing trust in an interaction. Another application can be found in digital cash. In July 2021 was launch by the European Central Bank a project for digital euro to issue a new means of payment through electronic money. In order to be competitive with existing cryptocurrencies this digital euro should

* This study was partially supported by the French ANR, grants 18-CE39-0019 (MobiS5), the French government research program "Investissements d´Avenir" through the IDEX-ISITE initiative 16-IDEX-0001 (CAP 20-25), the IMobS3 Laboratory of Excellence (ANR-10-LABX-16-01), the French ANR project DECRYPT (ANR-18-CE39-0007) and SEVERITAS (ANR-20-CE39-0009).

allow anonymity of payments. Identity-based blind signature could be the solution to facilitate the adoption of citizens. Moreover, the proxy property is needed to fit properly with the real world structure. In the case of the banks, they might want to distribute to several agencies located in different countries the ability to sign. In the case of e-voting, multiple polls are needed to organize an election. The delegation in several local pools is needed in order to distribute the election in each states or cities. In such a setup, identity-based proxy blind signature (IDPBS) is the solution for a secure voting protocol. There exist 14 IDPBS in the literature, 10 schemes use pairing [12, 13, 16, 22, 28–31, 33, 35] and the four others are paring free [15, 19, 20, 26].

Concerning generic constructions, D. Galindo *et al.* [10] shown that only a EUF-CMA (Existential UnForgeability under Chosen Message Attack) signature scheme and a EUF-CMA blind signature scheme are necessary to achieve an *Identity-based Blind Signature* (IDBS). Hence our aim is to design a generic construction for an IDBS but with an additional property: ability to delegates right to sign messages (*i.e.,* proxy).

Contributions: We first define the security notions of IDPBS that are not completely formalised in the literature. In order to prove our construction we need to have clear security experiments for all require properties.

We then propose the first generic construction for *Identity-based Proxy Blind Signature*. Our construction uses two building blocks:

- a SUF-CMA (Strong Existential Unforgeability under Chosen Message Attack) *unique signature scheme* $\mathsf{S} = (\mathsf{KeyGen}_\mathsf{S}, \mathsf{Sign}_\mathsf{S}, \mathsf{Verif}_\mathsf{S})$
- a EUF-CMA *blind signature scheme* $\mathsf{BS} = (\mathsf{KeyGen}_\mathsf{BS}, \mathsf{Protocol}_\mathsf{BS}, \mathsf{Verif}_\mathsf{BS})$.

We combine these two primitives in order to design a blind signature. In the literature there exist several SUF-CMA unique signature schemes, also known as Verifiable Unpredictable Functions (VUFs). For instance RSA-FDH [3] or [18] are unique signature schemes. There are also other unique signature schemes based on Diffie-Hellman assumption in bilinear groups [1, 8, 14, 17].

We formally prove the security of our construction that only relies on the security properties of the two primitives used. Our construction can be instantiated with any unique signature such as BLS [5] and any blind signature *e.g.,* a blind ECDSA [21, 32].

Related work: Since blind signature exists, numerous generic constructions are investigated. When they can be achieved, they allow to directly adapt new advances on more basic primitives. Few generic constructions have been presented for blind signatures. In [9], Fischlin *et al.* proved that blind signatures can be constructed by assembling a signature scheme with a zero-knowledge proof and an encryption scheme. The same year, another construction of identity-based (partially) blind signature was proposed by D. Galindo *et al.* [10]. This construction consists in two building blocks, a SUF-CMA signature scheme and a EUF-CMA blind signature scheme.They were all proved secure under some basic assumptions such as reliability of the underlying scheme in their respective settings.

Outline: In Section 2, we introduce the cryptographic material and notations for all building blocks of our construction. We also formally define the models of all the security properties of IDPBS. In Section 3, we present our main result *i.e.,* the generic

construction for IDPBS. In Section 4 we propose the security of our construction. Finally we conclude in Section 6.

Notations: In this paper we will be using the following notations. Take $\mathcal{D}$ and $\mathcal{Q}$ two algorithms, $\langle \mathcal{D}, \mathcal{Q} \rangle$ will correspond to an interactive protocol in between both parties. We will also denotes by $[\mathcal{D}]$ the set of all possible outputs of the specified algorithm. We will refer to the set of all values returned by an algorithm $\mathcal{D}$ using $Out(\mathcal{D})$.s

2 Formal Security Definitions and Properties for IDPBS

The definition of *identity-based proxy blind signature* varies in the literature. We give a definition based on [35] since it is the most generic one if we do not specify the ability to the original signer to actually sign messages (this ability is held to the proxy only). This feature could be added to the definition but there is no relevance for it. Note that our choice of definition is arbitrary yet we believe to be best suited.

Definition 1 (Identity-Based Proxy Blind Signature - IDPBS). *An IDPBS with security parameter $\mathfrak{K}$ is a 6-tuple of polynomial-time algorithms and protocols (Setup, Extract, $\langle \mathcal{S}, \mathcal{P} \rangle$, PKeyGen, $\langle \mathcal{P}, \mathcal{U} \rangle$, PBVerif) involving a public key generator PKG, an original signer $\mathcal{S}$, a proxy signer $\mathcal{P}$ and a user $\mathcal{U}$. Algorithms work as follows:*

- $\mathsf{Setup}(1^{\mathfrak{K}})$*: this protocol is run by* PKG*. It calls $\mathfrak{K}$ to generate the global parameters* params *of the system and a master key-pair* (mpk, msk).
- $\mathsf{Extract}(\mathsf{params}, msk, ID)$*: this protocol is run by the* PKG*. It takes as input an identity ID and a master key msk and return the corresponding secret key $sk[ID]$ via a secure channel.*
- $\langle \mathcal{S}, \mathcal{P} \rangle$ *is the* proxy-designation protocol *between $\mathcal{S}$ and $\mathcal{P}$. The inputs are the two identities $ID_{\mathcal{S}}$ and $ID_{\mathcal{P}}$ of the signers, their respective secret keys (query to* PKG *via* Extract*) and a delegation warrant m_w. As a result of the interaction, the expected local output of $\mathcal{P}$ is a secret key $sk_{\mathcal{P}}$ and a public agreement $w_{\mathcal{S}\to\mathcal{P}}$ that can be verified by any user. Formally $(sk_{\mathcal{P}}, w_{\mathcal{S}\to\mathcal{P}}) \leftarrow \langle \mathcal{S}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{P}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}]) \rangle$.*
- *Signature issuing is an interactive protocol between the proxy signer $\mathcal{P}(sk_{\mathcal{P}})$ with its secret key and the user $\mathcal{U}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m)$ knowing a message $m \in \{0,1\}^*$ and both identities $ID_{\mathcal{P}}$ and $ID_{\mathcal{S}}$. It generates the* signature *for the user $\sigma \leftarrow \langle \mathcal{P}(sk_{\mathcal{P}}), \mathcal{U}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m) \rangle$.*
- $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, w_{\mathcal{S}\to\mathcal{P}}, m, \sigma)$ *it outputs 1 if the signature σ is valid with respect to m, $ID_{\mathcal{S}}$, $ID_{\mathcal{P}}$, $w_{\mathcal{S}\to\mathcal{P}}$ and mpk, otherwise 0.*

The security of proxy signature has been defined in [4]. For this type of schemes, the adversary is allowed to corrupt an arbitrary number of users and learn their secret keys. Moreover, the adversary can register public keys on behalf of new users, possibly obtained otherwise than running the key-generation algorithm, and possibly depending on the public keys of already registered users. The adversary is also allowed to interact with honest users playing the role of a original signer or of a proxy signer.

Oracles. The adversary has access to oracles during this process. Elements returned by the adversary should not have been received from an oracle's query.

- **Query of Extraction:** $\mathcal{O}_{\mathsf{Extract}}(msk, \cdot) \rightarrow (sk_{ID_i}, w_{ID \rightarrow ID_i})$
  $\mathcal{A}$ request extraction for an identity ID_i, he sends ID_i to the PKG and receive the consistent answer $sk[ID_i]$.
- **Query of Keys Delegation:** $\mathcal{O}_{ID \rightarrow \mathcal{A}}(ID, sk[ID], m_w, ID_i)$
  The adversary produces an identity ID_i, a warrant m_w and request to the user with identity ID a delegation. The following protocol is executed $\langle \mathcal{A}(ID_i, ID, m_w), \mathcal{C}(ID, sk[ID]) \rangle \rightarrow (sk_{ID_i}, w_{ID \rightarrow ID_i})$
- **Query of Issuing Delegation:** $\mathcal{O}_{\mathcal{A} \rightarrow ID}(ID_i, sk[ID_i], m_w, ID)$
  For an already existing identity ID, $\mathcal{A}$ asks to delegate to an user with identity ID_i chosen by himself. The protocol $\langle \mathcal{A}(ID, sk[ID], ID_i, m_w), \mathcal{C}(ID_i, ID) \rangle \rightarrow (sk_{ID_i}, w_{ID \rightarrow ID_i})$ is executed. The transcript of the interactions is given to $\mathcal{A}$ but he does not learn the secret key.
- **Query of Secret Key:** $\mathcal{O}_{\mathsf{Exposure}}(ID_i) \rightarrow sk[ID_i]$
  For any already existing ID_i different to the identity of the user under attack, $\mathcal{A}$ can request a secret key to $\mathcal{S}$.
- **Query of Proxy Secret Key:** $\mathcal{O}_{\mathsf{PExposure}}(ID_i) \rightarrow sk_{ID_i}$
  For any already existing ID_i different to identity of the user under attack, $\mathcal{A}$ can request a proxy secret key.
- **Query of Transcript of Delegation:** $\mathcal{O}_{ID_i \rightarrow ID_j}$
  $\mathcal{A}$ chooses two identities ID_i and ID_j with ID_i already extracted.Then $\langle \mathcal{C}(ID_i), \mathcal{P}(ID_j) \rangle$ is executed and the adversary gets the transcript of the interactions. The identities ID_i and ID_j are not necessarily different.
- **Query of signature:** $\mathcal{O}_{\mathsf{S}}(ID_i, m) \rightarrow \sigma_m$
  $\mathcal{A}$ can ask for a blind signature from ID_i (an already claimed identity). $\mathcal{A}$ chooses the message and a signature σ is produced and returned to him.
- **Query of proxy signature:** $\mathcal{O}_{\mathsf{PS}}(ID_i, m) \rightarrow \sigma_m$
  $\mathcal{A}$ chooses a message m and two identities ID_i, ID_j with ID_i already extracted and ID_j provided with a delegation from ID_i. The proxy signature protocol is run with $\mathcal{A}$ playing the role of the user and the user associated to ID_j the proxy signer.

Security Properties. We formally defined all security properties that a IDPBS scheme should satisfy as follows:

- *Blindness* has to be consider from two points of view since attackers could be either $\mathcal{S}^*$ or $\mathcal{P}^*$. Both are still required to win the experiment $\mathsf{Exp}^{bl}_{\mathsf{IDPBS},*}(\mathfrak{K})$ of the game defined in Figure 1. A proxy blind signature achieves *blindness* if for any polynomial time adversary $\mathcal{A}$, $Adv^{bl}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) = |\mathsf{Exp}^{bl}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) - 1/2|$ is negligible.
- *Unforgeability* is quite similar to the context of identity-based proxy signature schemes defined in [4]. The experiment is given in Figure 2.
- *Verifiability* means that the verifier $\mathcal{V}$ can always be convinced of the original signer's agreement on the signed message. We formalise this property thanks to the experiment of Figure 3.
- *Prevention of misuse* requires that the proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature within the terms of a del-

$\mathsf{Exp}^{bl}_{\mathsf{IDPBS},\mathcal{S}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_0, m_1) \leftarrow \mathcal{A}(mpk)$
3. $b \xleftarrow{\$} \{0,1\}$
4. $\sigma_b, w_{\mathcal{S}\rightarrow\mathcal{P},b} \leftarrow \langle \mathcal{A}, \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_b)\rangle$
5. $\sigma_{1-b}, w_{\mathcal{S}\rightarrow\mathcal{P},1-b} \leftarrow \langle \mathcal{A}, \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_{1-b})\rangle$
6. $b^* \leftarrow \mathcal{A}((m_0, \sigma_0, w_{\mathcal{S}\rightarrow\mathcal{P},0}), (m_1, \sigma_1, w_{\mathcal{S}\rightarrow\mathcal{P},1}))$
7. Return $b^* = b$

Fig. 1: Security Experiment for Blindness of IDPBS [36].

$\mathsf{Exp}^{uf}_{\mathsf{IDPBS},\mathcal{U}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \langle \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}])\rangle$
5. $\{(ID_{\mathcal{P}_i}, m_i, \sigma_i)\}_{1\leq i\leq l'} \leftarrow \mathcal{A}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}})$
6. If $\exists i \neq j, m_i = m_j$ or $\exists i$, $\mathsf{Verify}(ID, m_i, \sigma_i) = 0$: Return 0
7. Else Return 1

Fig. 2: Security Experiment for UnForgeability of IDPBS [4]. In this game, l is the number of succeeding call to the signing oracle $\mathcal{O}_{\mathsf{PS}}$.

egation made by $\mathcal{S}$ to $\mathcal{P}$. In case of misuse, the responsibility of the proxy signer should be determined explicitly. This is formalized in Figure 4.

– *Strong Identifiability* requires anyone to be able to determine the identity of the corresponding proxy signer from the signature as described by the experiment of Figure 5. This is to allow linkability of a signature to a proxy signer in case of a fraud. In the context of identity-based proxy signature, it is straight forward achieved.
– *Strong Undeniability*. Once a proxy signer creates a valid proxy signature with the delegation of an original signer, it cannot repudiate the produced signature. Here the validity of the signature holds as a proof against deniability of the proxy user as we can see in the experiment of Figure 6.

An adversary breaks an identity-based proxy blind signature if for any of these experiments he has non negligible probabilities of winning the corresponding advantages.

$\mathsf{Exp}^{veri}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}} \in Out(\mathcal{A}) \leftarrow \langle \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{A}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}])\rangle$
5. $(m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}$
6. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$,
$w'_{\mathcal{S}\rightarrow\mathcal{P}} \notin Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$ and $m'_w \neq m_w$: Return 1
7. Else Return 0

Fig. 3: Security experiment for Verifiability of IDPBS.

$\mathsf{Exp}^{PoM}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}} \in Out(\mathcal{A}) \leftarrow \langle \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{A}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}]) \rangle$
5. $(ID, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}$
8. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$ with $ID \neq ID_{\mathcal{P}}$, $m'_w \neq m_w$ and $w'_{\mathcal{S}\rightarrow\mathcal{P}} \notin Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$: Return 1
7. Else Return 0

Fig. 4: Security Experiment for Prevention of Misuse of IDPBS.

$\mathsf{Exp}^{st-id}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}} \in Out(\mathcal{A}) \leftarrow \langle \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{A}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}]) \rangle$
5. $\sigma \leftarrow \mathsf{Protocol}\langle \mathcal{A}(mpk, sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}), \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m) \rangle$
6. $ID \leftarrow \mathcal{A}(\sigma)$
7. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$ with $ID \neq ID_{\mathcal{P}}$: Return 1
8. Else Return 0

Fig. 5: Security Experiment for Strong Identification of IDPBS.

$\mathsf{Exp}^{st-und}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}} \in Out(\mathcal{A}) \leftarrow \langle \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w), \mathcal{A}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{P}}]) \rangle$
5. $(Id, (m, \sigma), m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}$
6. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$,
$\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$ with $ID \neq ID_{\mathcal{P}}$: Return 1
7. Else Return 0

Fig. 6: Security Experiment for Strong Undeniability of IDPBS.

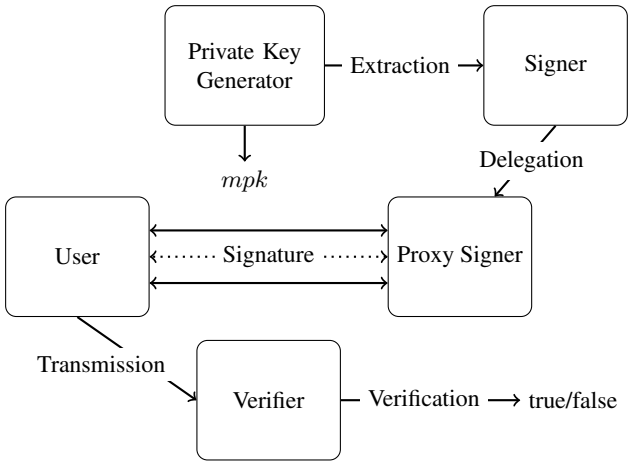

Fig. 7: General Framework for our Generic Construction of IDPBS.

3 Our IDPBS Construction

A general idea of the interactions of our construction is given in Figure 7. $\mathcal{S}$ and $\mathcal{P}$ both start with their respective identities $ID_{\mathcal{S}}$ and $ID_{\mathcal{P}}$. We suppose them known by the user. A message m is generated by $\mathcal{U}$ prior to the signature protocol.

We now give the description of each step of the issuing of a new signature. The algorithms are presented in Figure 8.

Key Generation. The KeyGen algorithm runs first. It generates the keys for the PKG.

Extraction. The private key generator (PKG) produces a signing key for $\mathcal{S}$ and the associated certificate $\mathsf{cert}_{\mathcal{S}}$ following algorithm Extract. The PKG sends the user secret key associated to the identify $ID_{\mathcal{S}}$, $USK[ID_{\mathcal{S}}] = (\mathsf{cert}_{\mathcal{S}}, vk_{\mathcal{S}}^{\mathsf{S}}, sk_{\mathcal{S}}^{\mathsf{S}})$ to $\mathcal{S}$ via a secure channel and $\mathcal{S}$ verifies the signature $\mathsf{cert}_{\mathcal{S}}$.

At the end of this phase, $\mathcal{S}$ is provided with public/private keys $(vk_{\mathcal{S}}^{\mathsf{S}}, sk_{\mathcal{S}}^{\mathsf{S}})$ and a certificate $\mathsf{cert}_{\mathcal{S}}$ linking the public key to its identity. Later, the user is able to verify this certificate with the master public key mpk. $\mathcal{U}$ can thus be convinced that this key was produced by a private key generator.

Delegation. Proceeding to the delegation from the signer $\mathcal{S}$ to the proxy signer $\mathcal{P}$ is generally described as an interactive protocol. Here, we chose to proceed as follows. Let m_w be a contract produced after a negotiation prior to that step. The signer produces a link in between the contract m_w, a blind signature public key $vk_{\mathcal{P}}^{\mathsf{BS}}$ and both identities $ID_{\mathcal{S}}$ and $ID_{\mathcal{P}}$. For the creation of the proxy signer, $\mathcal{S}$ only has to be in procession of its identity $ID_{\mathcal{P}}$. The procedure is described in algorithm DelGen.

After running the algorithm $\mathcal{S}$ sends $(w_{\mathcal{S}\to\mathcal{P}}, \mathsf{cert}_{\mathcal{S}}, vk_{\mathcal{S}}^{\mathsf{S}})$ to $\mathcal{P}$. It is also necessary to send information through a secure channel $USK[ID_{\mathcal{P}}] = (vk_{\mathcal{P}}^{\mathsf{BS}}, sk_{\mathcal{P}}^{\mathsf{BS}})$.

When receiving this information, the proxy $\mathcal{P}$ runs the mandatory verification of certificates $\mathsf{cert}_{\mathcal{S}}$ and $w_{\mathcal{S}\to\mathcal{P}}$. If both pass, $\mathcal{P}$ accepts the keys and the certificates.

$\mathsf{KeyGen}(1^{\aleph})$: 1. $(msk, mpk) \leftarrow KeyGen_{\mathsf{S}}(1^{\aleph})$ Return msk, mpk	$\mathsf{Extract}(msk, ID_{\mathcal{S}})$: 1. $(vk^{\mathsf{S}}_{\mathcal{S}}, sk^{\mathsf{S}}_{\mathcal{S}}) \leftarrow KeyGen_{\mathsf{S}}(1^{\aleph})$ 2. $\mathsf{cert}_{\mathcal{S}} \leftarrow Sign_{\mathsf{S},msk}(ID_{\mathcal{S}}\|vk^{\mathsf{S}}_{\mathcal{S}})$ Return $USK[ID_{\mathcal{S}}] = (\mathsf{cert}_{\mathcal{S}}, vk^{\mathsf{S}}_{\mathcal{S}}, sk^{\mathsf{S}}_{\mathcal{S}})$
$\mathsf{DelGen}(ID_{\mathcal{S}}, sk^{\mathsf{S}}_{\mathcal{S}}, ID_{\mathcal{P}}, m_w)$: 1. $(vk^{\mathsf{BS}}_{\mathcal{P}}, sk^{\mathsf{BS}}_{\mathcal{P}}) \leftarrow KeyGen_{\mathsf{BS}}(1^{\aleph})$ 2. $w_{\mathcal{S}\rightarrow\mathcal{P}} \leftarrow$ $Sign_{\mathsf{S},sk^{\mathsf{S}}_{\mathcal{S}}}(ID_{\mathcal{S}}\|ID_{\mathcal{P}}\|vk^{\mathsf{BS}}_{\mathcal{P}}\|m_w)$ Return $(vk^{\mathsf{BS}}_{\mathcal{P}}, sk^{\mathsf{BS}}_{\mathcal{P}}), w_{\mathcal{S}\rightarrow\mathcal{P}}$	$\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}})$: 1. If $\mathsf{Verif}_{\mathsf{S},mpk}(\mathsf{cert}_{\mathcal{S}}, ID_{\mathcal{S}}\|vk^{\mathsf{S}}_{\mathcal{S}}) = 0$: Return 0 2. If $\mathsf{Verif}_{\mathsf{S},vk^{\mathsf{S}}_{\mathcal{S}}}(w_{\mathcal{S}\rightarrow\mathcal{P}}, ID_{\mathcal{S}}\|ID_{\mathcal{P}}\|vk^{\mathsf{BS}}_{\mathcal{P}}\|m_w) = 0$: Return 0 3. If $m \notin m_w$: Return 0 4. If $\mathsf{Verif}_{\mathsf{BS},vk^{\mathsf{BS}}_{\mathcal{P}}}(\sigma, m) = 0$: Return 0 5. Else: Return 1

Fig. 8: Algorithm of the Generic Construction of IDPBS.

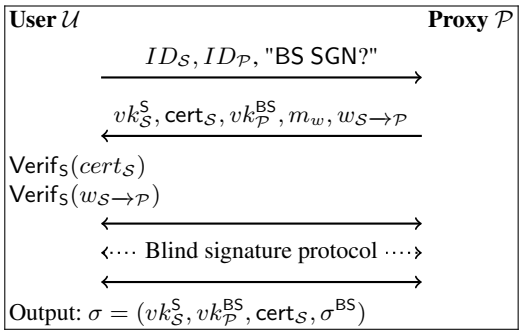

Fig. 9: Signature Issuing of IDPBS.

Signature issuing. At this point $\mathcal{P}$ is in possession of: $mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, vk^{\mathsf{S}}_{\mathcal{S}}, \mathsf{cert}_{\mathcal{S}}$, $(vk^{\mathsf{BS}}_{\mathcal{P}}, sk^{\mathsf{BS}}_{\mathcal{P}}), m_w, w_{\mathcal{S}\rightarrow\mathcal{P}}$. He now interacts with $\mathcal{U}$ in possession of a message m in order to issue a blind signature on m. The final signature is composed of $\sigma = (vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{P}}, \mathsf{cert}_{\mathcal{S}}, \sigma^{\mathsf{BS}})$, where σ^{BS} is the signature obtained from the blind signature scheme. Figure 9 describes these interactions. Note that the two first steps can be combined with the upcoming ones if the user speaks first in the blind signature protocol. Thus, it is possible to achieve the round optimal property with this construction *i.e.,* reaching the minimum of two communications in the issuing of an IDPBS signature.

Verification. $\mathcal{U}$ transmits the inputs of the algorithm to the verifier. The validity of the signature is assessed by running Verif.

As we can see in algorithm Verif of Figure 8 the verification process implies to attest the validity of all certificates and adding to that checking the final signature. It needs 2 executions of $Verif_{\mathsf{S}}()$ and 1 execution of $Verif_{\mathsf{BS}}()$, thus leading to a relatively long process of verification compare to other blind signatures.

4 Security of the proposed scheme

We can now study the security of our construction, assuming that the chosen schemes do not have serious security issues. Correctness and unforgeability of both schemes are taken as granted, blindness of the blind signature scheme is also required. The rest of this paper is dedicated to the security properties, we are recalling there description and proving that they are fulfilled by our construction. Our proofs involves reduction of games, we will consider various scenarios S_i and the probability that a polynomial time adversary $\mathcal{A}$ allows the associated experiment to return 1. We use $\Pr[S_i]$ as the probability of such an outcome.

Correctness. This property is straightforward if both signature meet this basic property.

Blindness. The blindness of the scheme require a unique signature scheme. The notion of unique signature was introduced by S. Goldwasser and R. Ostrovsky [11]

Let $\mathsf{S} = (\mathsf{KeyGen_S}, \mathsf{Sign_S}, \mathsf{Verif_S})$ be a signature scheme. To be a unique signature, the algorithms must satisfy the following requirements of uniqueness: For every public parameter of the scheme, every key pair (sk, pk) produced by algorithm $\mathsf{KeyGen_S}$, every message m, and every pair of signatures σ_1 and σ_2, if we have $\mathsf{Verif_S}(pk, m, \sigma_1) = \mathsf{Verif_S}(pk, m, \sigma_2) = 1$, then it must imply $\sigma_1 = \sigma_2$. In our case it is sufficient to have negligible probability to output two signatures verifying for the same message even with the secret key. We define $\mathsf{Adv}^{uni}_{\mathsf{S},\mathcal{A}_\mathsf{S}}$ as the advantage of an adversary against it.

Lemma 1 (Blindness). *Given* S *a unique signature scheme and* BS *a blind signature scheme with blindness, our construction gives rise to a blind identity-based proxy blind signature scheme. In particular, we show that:* $\mathsf{Adv}^{bl}_{\mathsf{IDPBS},\mathcal{A}} \leq \mathsf{Adv}^{bl}_{\mathsf{BS},\mathcal{A}_\mathsf{BS}} + 3 \cdot \mathsf{Adv}^{uni}_{\mathsf{S},\mathcal{A}_\mathsf{S}}$.

Proof. Fix $\mathcal{A}$, a polynomial time adversary. Let us define Game 0 to be the security game against for blindness of our scheme. The game can be described as follows.

Game 0_1:
1. $(mpk, msk) \leftarrow \mathsf{KeyGen_S}(1^\mathfrak{K})$
2. $(ID_\mathcal{S}, ID_\mathcal{P}, m_0, m_1, m_w) \leftarrow \mathcal{A}(mpk)$
3. $b \xleftarrow{\$} \{0, 1\}$
4. $\sigma_b, w_{\mathcal{S}\rightarrow\mathcal{P},b} \leftarrow \mathsf{Protocol}\langle\mathcal{A}, \mathcal{C}(ID_\mathcal{S}, ID_\mathcal{P}, m_b)\rangle$
5. $\sigma_{1-b}, w_{\mathcal{S}\rightarrow\mathcal{P},1-b} \leftarrow \mathsf{Protocol}\langle\mathcal{A}, \mathcal{C}(ID_\mathcal{S}, ID_\mathcal{P}, m_{1-b})\rangle$
6. $b^* \leftarrow \mathcal{A}((m_0, \sigma_0), (m_1, \sigma_1))$

If we define S_0 to be the event that $b = b^*$ in Game 0_1, then the adversary's advantage is $\mathsf{Adv}^{bl}_{\mathsf{IDPBS},\mathsf{B}} = |\Pr[S_0] - 1/2|$. First we need to investigate more in depth the interactive protocol of the proxy blind signing. For that we consider lines 4 and 5 and put forward their description in Game 0_2. For each $i \in \{0, 1\}$,

Game 0_2:
1. $vk^\mathsf{S}_\mathcal{S}, \mathsf{cert}_{\mathcal{S},i}, vk^\mathsf{BS}_\mathcal{S}, w_{\mathcal{S}\rightarrow\mathcal{P},i} \leftarrow \mathcal{A}$
2. If $(\mathsf{Verif_S}(\mathsf{cert}_{\mathsf{S},i}) \neq 1)$ or $(\mathsf{Verif_S}(w_{\mathcal{S}\rightarrow\mathcal{P},i}) \neq 1)$, Abort
3. $\sigma^\mathsf{BS}_i \leftarrow \mathsf{Protocol_{BS}}\langle\mathcal{A}, \mathcal{C}(vk^\mathsf{BS}_\mathcal{S}, m_i)\rangle$
4. $\sigma_i \leftarrow (vk^\mathsf{S}_\mathcal{S}, vk^\mathsf{BS}_\mathcal{S}, \mathsf{cert}_{\mathcal{S},i}, \sigma^\mathsf{BS}_i)$

We now make one small change to the underlying Game 0_2. The warrant $w_{\mathcal{S}\to\mathcal{P}}$ will be fixed for both execution of the protocol and produced by $\mathcal{A}$ in the second step. Line 2 of Game 0_1 becomes $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_0, m_1, m_w, w_{\mathcal{S}\to\mathcal{P}}) \leftarrow \mathcal{A}(mpk)$ in Game 1_1. Let S_1 be the event that $b = b^*$ in Game 1. Here the difference between S_0 and S_1 correspond to the event $F =$"non unique determination of the signature $w_{\mathcal{S}\to\mathcal{P}}$ of a warrant m_w". Thus $|\mathsf{Pr}[S_0] - \mathsf{Pr}[S_1]| \leq 2 \cdot \mathsf{Adv}^{uni}_{\mathsf{S}}(k)$ by the difference lemma [24]; this probability is considered negligible by hypothesis.

Game 2_1:
1. $(mpk, msk) \leftarrow \mathsf{KeyGen}_{\mathsf{S}}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_0, m_1, m_w, w_{\mathcal{S}\to\mathcal{P}}, \mathsf{cert}_{\mathcal{S}}) \leftarrow \mathcal{A}(mpk)$
3. $b \xleftarrow{\$} \{0,1\}$
4. $\sigma_b, w_{\mathcal{S}\to\mathcal{P},b} \leftarrow \mathsf{Protocol}\langle\mathcal{A}, \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_b)\rangle$
5. $\sigma_{1-b}, w_{\mathcal{S}\to\mathcal{P},1-b} \leftarrow \mathsf{Protocol}\langle\mathcal{A}, \mathcal{C}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_{1-b})\rangle$
6. $b^* \leftarrow \mathcal{A}((m_0, \sigma_0), (m_1, \sigma_1))$

Game 2_2:
1. $vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{S}}, w_{\mathcal{S}\to\mathcal{P}} \leftarrow \mathcal{A}$
2. If $(\mathsf{Verif}_{\mathsf{S}}(\mathsf{cert}_{\mathsf{S}}) \neq 1)$ or $(\mathsf{Verif}_{\mathsf{S}}(w_{\mathcal{S}\to\mathcal{P}}) \neq 1)$, Abort
3. $\sigma_i^{\mathsf{BS}} \leftarrow \mathsf{Protocol}_{\mathsf{BS}}\langle\mathcal{A}, \mathcal{C}(vk^{\mathsf{BS}}_{\mathcal{S}}, m_i)\rangle$
4. $\sigma_i \leftarrow (vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{S}}, \mathsf{cert}_{\mathcal{S}}, \sigma_i^{\mathsf{BS}})$

Just like we did for certificate $w_{\mathcal{S}\to\mathcal{P}}$, we restrict our adversary to output an unique $\mathsf{cert}_{\mathcal{S}}$ at the beginning of the game. Only signature containing this certificate are accepted, otherwise the procedure fails. After changing Game 1 into Game 2 as described, we can define an event S_2 representing the event $b = b^*$ after Game 2. $\mathsf{cert}_{\mathcal{S}}$ is supposed to be fixed at the beginning of the session. Applying the difference lemma a second time, we obtain a difference of happening between the two game with an upper bound $|\mathsf{Pr}[S_0] - \mathsf{Pr}[S_1]| \leq \mathsf{Adv}^{uni}_{\mathsf{S}}(k)$. This step has the same consequences as for the previous one and $\mathcal{A}$ gained the same advantage.

Our thirds step consist of neutralising the ability $\mathcal{A}$ has to distinguish in between σ_0^{BS} and σ_1^{BS}. Let us restate the games and draw a random value from the possibles outputs of the blind signature protocol without executing it. Hence, the adversary obtains no information from the element σ_i^{BS} he receives at the last step. We have assumed blindness of the blind signature scheme, thus the gained advantage is negligible.

Game 3_2:
1. $vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{S}}, w_{\mathcal{S}\to\mathcal{P}} \leftarrow \mathcal{A}$
2. If $(\mathsf{Verif}_{\mathsf{S}}(\mathsf{cert}_{\mathsf{S}}) \neq 1)$ or $(\mathsf{Verif}_{\mathsf{S}}(w_{\mathcal{S}\to\mathcal{P}}) \neq 1)$, Abort
3. $\sigma_i^{\mathsf{BS}} \xleftarrow{\$} [\mathsf{Protocol}_{\mathsf{BS}}\langle\cdot,\cdot\rangle]$
4. $\sigma_i \leftarrow (vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{S}}, \mathsf{cert}_{\mathcal{S}}, \sigma_i^{\mathsf{BS}})$

An extra bridging steps would be to reformulate line 4 of Game 3,2 to ignore this random value that has no impact on the choice of $\mathcal{A}$ and set $\sigma_i \leftarrow (vk^{\mathsf{S}}_{\mathcal{S}}, vk^{\mathsf{BS}}_{\mathcal{S}}, \mathsf{cert}_{\mathcal{S}})$ in line 4 of Game 4_2. This formulation leads to a complete incapability of the adversary to decide anything as all of its input are produced directly by himself. Therefore, by the triangular inequality, $\mathsf{Adv}^{bl}_{\mathsf{IDPBS},\mathcal{A}} = |\mathsf{Pr}[S_0] - \mathsf{Pr}[S_3]| \leq \mathsf{Adv}^{bl}_{\mathsf{BS},\mathcal{A}_{\mathsf{BS}}} + 3 \cdot \mathsf{Adv}^{uni}_{\mathsf{S},\mathcal{A}_{\mathsf{S}}}$.

Unforgeability. The unforgeability of our construction relies on this theorem.

Lemma 2 (Unforgeability). *Given a signature scheme* S *and a blind signature scheme* BS *both with unforgeability, our construction has unforgeability. In particular, we show that:* $\mathsf{Adv}^{uf}_{\mathsf{IDPBS},\mathcal{A}} \leq q \cdot (\mathsf{Adv}^{uf}_{\mathsf{BS},\mathcal{A}_{\mathsf{BS}}} + \mathsf{Adv}^{uf}_{\mathsf{S},\mathcal{A}_{\mathsf{S}}})$.

Proof. Fix an adversary $\mathcal{A}$ against the unforgeability of our scheme given access to the previously described oracles. $\mathcal{A}$ is allowed to make any number of queries to each of them, but the final outputs of the game should be no element obtained from an oracle. We may write the security game as follows.

Game 0:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $\{(ID_{\mathcal{P}_i}, m_i, \sigma_i)\}_{1\leq i\leq l'} \leftarrow \mathcal{A}$
6. If $\exists i \neq j, m_i = m_j$ or $\exists i$, $\mathsf{Verify}(ID_{\mathcal{P}_i}, m_i, \sigma_i) = 0$: Return 0
7. Else Return 1

We can define the event S_0 corresponding to Game 0 outputting 1. If such an outputs happens this would be considered as a valid forgery, thus $\mathsf{Adv}^{uf}_{\mathsf{IDPBS},\mathcal{A}} = \mathsf{Pr}(S_0)$. Let l be the number of proxy blind signature queries that are successfully completed. With probability $\mathsf{Adv}^{uf}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K})$, the adversary $\mathcal{A}$ succeeds and outputs a valid forgery *i.e.,* a list of l' tuples $\{(ID_{\mathcal{P}_i}, m_i, \sigma_i)\}_{1\leq i\leq l'}$ with $l < l'$. Since $l < l'$, there exists at least some identity ID_i in the output list such that the number $l(ID_i)$ of completed blind signature queries during the attack involving ID_i is strictly less than the number $l'(ID_i)$ of tuples involving identity ID_i in the output list. This has to hold by the pigeonhole principal. If we outputted a forgery for the right identity $ID = ID_{\mathcal{P}_*}$, then we have completed $l(ID)$ executions of the blind signature protocol during our attack $\mathsf{F}_{\mathcal{BS}}$ against the blind signature scheme BS, with public key $vk^{\mathsf{BS}}_{\mathcal{P}_*}$ and we can easily obtain $l'(ID)$ valid signatures under the same public key from the list output by $\mathcal{A}$ satisfying $l(ID) < l'(ID)$ for that identity. Hence, we can modify our game to restrict our adversary to output a forgery on a specified identity. He has probability $1/q$ to get a forgery for the right identity. Game 1 is modified accordingly. This gives the relation $1/q \cdot \mathsf{Pr}[S_0] = \mathsf{Pr}[S_1]$ between the probability of the two events S_0 and S_1.

Game 1:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $\{(m_i, \sigma_i)\}_{1\leq i\leq l'} \leftarrow \mathcal{A}$
6. If $\exists i \neq j, m_i = m_j$ or $\exists i$, $\mathsf{Verify}(ID_{\mathcal{P}}, m_i, \sigma_i) = 0$: Return 0
7. Else Return 1

$\mathcal{A}$ has the capability to forge new signatures $\mathsf{cert}_{\mathcal{S}}$ embedded proxy blind signature, leading to new signature. In Game 2, we will ask $\mathcal{A}$ to output $\mathsf{cert}_{\mathcal{S}}$ at the beginning. As a consequence, modification of the key $vk^{\mathsf{S}*}_{\mathcal{S}}$ will lead to failure. Define event S_2 as "$\mathcal{A}$

wins the Game 2", the probability of realisation of these event only differ by $\mathsf{Adv}_{\mathsf{S}}^{uf}(k)$ from $\mathsf{Pr}[S_1]$, which is supposed negligible.

Game 2:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $\mathsf{cert}_{\mathcal{S}} \leftarrow \mathsf{Sign}_{\mathsf{S},msk}(ID_{\mathcal{S}}||vk_{\mathcal{S}}^{\mathsf{S}})$
6. $\{(m_i, \sigma_i = (vk_{\mathcal{S}}^{\mathsf{S}}, vk_{\mathcal{S}}^{\mathsf{BS}}, \mathsf{cert}_{\mathcal{S}}, \sigma_i^{\mathsf{BS}})\}_{1\leq i\leq l'} \leftarrow \mathcal{A}$
7. If $\exists i \neq j, m_i = m_j$ or $\exists i, \mathsf{Verify}(ID_{\mathcal{P}}, m_i, \sigma_i) = 0$: Return 0
8. Else Return 1

A second restriction can now be put forward: inability to forge blind signatures on scheme BS. In Game 3, $\sigma_{m_i}^{\mathsf{BS}}$ is the blind signature given by a legit execution of the blind signature scheme for the key pair $(vk_{\mathcal{S}}^{\mathsf{BS}}, sk_{\mathcal{S}}^{\mathsf{BS}})$. This time we have have $|\mathsf{Pr}[S_2] - \mathsf{Pr}[S_3]| \leq \mathsf{Adv}_{\mathsf{BS}}^{uf}(k)$.

Game 3:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $\mathsf{cert}_{\mathcal{S}} \leftarrow \mathsf{Sign}_{\mathsf{S},msk}(ID_{\mathcal{S}}||vk_{\mathcal{S}}^{\mathsf{S}})$
6. $\{(m_i, \sigma_i = (vk_{\mathcal{S}}^{\mathsf{S}}, vk_{\mathcal{S}}^{\mathsf{BS}}, \mathsf{cert}_{\mathcal{S}}, \sigma_{m_i}^{\mathsf{BS}})\}_{1\leq i\leq l'} \leftarrow \mathcal{A}$
7. If $\exists i \neq j, m_i = m_j$ or $\exists i, \mathsf{Verify}(ID_{\mathcal{P}}, m_i, \sigma_i) = 0$: Return 0
8. Else Return 1

All part of each signature have to be legit, thus the adversary is totally unable to conduct any action that could lead to a new signature. We conclude that $l = l'$. In that Game 3, any signature outputted by $\mathcal{A}$ was produced directly by the proxy signer. We observe a total advantage of an adversary against the generic IDPBS scheme of $\mathsf{Adv}_{\mathsf{IDPBS},\mathcal{A}}^{uf} \leq q \cdot (\mathsf{Adv}_{\mathsf{BS},\mathcal{A}_{\mathsf{BS}}}^{uf} + \mathsf{Adv}_{\mathsf{S},\mathcal{A}_{\mathsf{S}}}^{uf})$.

Verifiability. From a proxy signature, a verifier can be convinced of the original signer's agreement on the signed message.

Lemma 3 (Verifiability). *The adversary's advantage against the verifiability of the generic* IDPBS *scheme is* $\mathsf{Adv}_{\mathsf{IDPBS},\mathcal{A}}^{veri}(\mathfrak{K}) \leq \mathsf{Adv}_{\mathsf{S},\mathcal{A}_{\mathsf{S}}}^{uf}$.

Proof. It is possible for an adversary $\mathcal{A}$ against verifiability to issue any blind signature by executing the protocol with himself. Thus any $\mathcal{A}$ is able to produced proxy signature under warrant m_w due to the settings of that game. Modifying Game 0 into Game 1, changes correspond to the inability of the adversary to forge a new certificate $w_{\mathcal{S}\rightarrow\mathcal{P}}$.

Game 1 :
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $(m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}})$,
with $w'_{\mathcal{S}\rightarrow\mathcal{P}} \in Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$
6. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$, $m'_w \neq m_w$
and $w'_{\mathcal{S}\rightarrow\mathcal{P}} \notin Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$: Return 1
7. Else Return 0

Let S_0 and S_1 by the respective event "Game i returns 1". By the difference lemma, we can conclude that $|\mathsf{Pr}[S_0] - \mathsf{Pr}[S_1]| \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$. Differences in the games would directly lead to another adversary exploiting it to forge new signatures.

Note that, n Game 1 lines 5 and 6 contradict themselves, hence it is impossible for the adversary to win Game 1. We conclude that $\mathsf{Adv}^{veri}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) \leq \mathsf{Adv}^{uf}_{\mathsf{S},\mathcal{A}_{\mathsf{S}}}$.

Prevention of misuse. Relatively similar to *verifiability*, *prevention of misuse* require that a proxy signing key cannot be used for purposes other than generating valid proxy signatures. In such a case of fraud it should be possible to identify the proxy signer.

Lemma 4 (Prevention of misuse). *The advantage of an adversary against prevention of misuse is* $\mathsf{Adv}^{PoM}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$.

Proof. Start with Game 0 being the experiment $\mathsf{Exp}^{st-id}_{\mathsf{IDPBS},\mathcal{P}^*}$.

Adversary $\mathcal{A}$ receives a warrant m_w with certificate $w_{\mathcal{S}\rightarrow\mathcal{P}}$. If he wants to use his keys for an unauthorised message, $\mathcal{A}$ has to produce a fake warrant and its associated certificate, otherwise the signature would not verify. But latter he could be identify as the cheater and be reprimand. In order not to be identify, $\mathcal{A}$ has to produced this certificate of delegation for another identity. We introduce change in our previous experiment and obtain Game 1.

Game 1 :
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $(ID, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}})$,
with $w'_{\mathcal{S}\rightarrow\mathcal{P}} \notin Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$
6. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) = 1$ with $ID \neq ID_{\mathcal{P}}$, $m'_w \neq m_w$ and $w'_{\mathcal{S}\rightarrow\mathcal{P}} \notin Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m'_w))$: Return 1
7. Else Return 0

In Game 0, $\mathcal{A}$ was able to output a forgery of a signature, this not the case in Game 1. We consider the adversary's advantage $\mathsf{Adv}^{uf}_{\mathsf{S}}(k)$ as negligible. We obtain $|\mathsf{Pr}[S_0] - \mathsf{Pr}[S_1]| \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$. In Game 1, condition of lines 5 and 6 of Game 1 cannot be fulfilled both at the time, we conclude to $\mathsf{Pr}[S_1] = 0$, from this fact we can conclude to the upper bound $\mathsf{Adv}^{PoM}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) = \mathsf{Pr}[S_0] \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$.

Strong Identifiability. Anyone can determine the identity of the corresponding proxy signer from a proxy signature. Let now be $\mathcal{A}$ an adversary against strong identifiability of the IDPBS. Set Game 0 as the experiment $\mathsf{Exp}^{st-id}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$ for this scheme.

Lemma 5 (Strong Identifiability). *The advantage of an adversary $\mathcal{A}$ against strong identifiability is* $\mathsf{Adv}^{st-id}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$.

Proof. In order to win the experiment $\mathsf{Exp}^{st-id}_{\mathsf{IDPBS},\mathcal{P}^*}(\mathfrak{K})$ an adversary $\mathcal{A}$ has to outputs a second identity ID such that $ID_{\mathcal{P}}$ and ID verifies:

$$\begin{aligned} w_{\mathcal{S}\to\mathcal{P}} &= Sign_{\mathsf{S},sk^{\mathsf{S}}_{\mathcal{S}}}(ID_{\mathcal{S}}||ID_{\mathcal{P}}||vk^{\mathsf{BS}}_{\mathcal{P}}||m_w) \\ &= Sign_{\mathsf{S},sk^{\mathsf{S}}_{\mathcal{S}}}(ID_{\mathcal{S}}||ID||vk^{\mathsf{BS}}_{\mathcal{P}}||m_w) = w'_{\mathcal{S}\to\mathcal{P}}. \end{aligned}$$

If this equality holds, even if $w_{\mathcal{S}\to\mathcal{P}}$ was given to $\mathcal{A}$ during the game, it is clear that $\mathsf{Adv}^{st-id}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) = \mathsf{Pr}[(m,m') \leftarrow \mathcal{A}|Sign_{\mathsf{S},sk^{\mathsf{S}}_{\mathcal{S}}}(m) = Sign_{\mathsf{S},sk^{\mathsf{S}}_{\mathcal{S}}}(m')] \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$.

Strong Undeniability. A proxy signer cannot repudiate a proxy signature it created. Given the information that $\mathcal{U}$ has at the end of a blind signing session, he has enough knowledge to expose $\mathcal{P}$. This would lead to ability to revoke the signature $w_{\mathcal{S}\to\mathcal{P}}$ of $\mathcal{S}$.

Lemma 6 (Strong Undeniability). *Strong undeniability of our scheme holds. The adversary's advantage against this property is* $\mathsf{Adv}^{st-und}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k) + \mathsf{Adv}^{uni}_{\mathsf{S}}(k)$.

Proof. Let Game 0 be the experiment associated to strong undeniability. Once published a signature cannot be repudiated as all information were revealed to the public, in particularly, in an identity-based setup $ID_{\mathcal{S}}$ and $ID_{\mathcal{P}}$ were transited. Using the Verif algorithm we will output 1 if the signature is valid. Thus $\mathcal{A}$ as to trick around this and propose an alternative possibility. $\mathcal{A}$ can output a second ID that could work for the same setup and thus causing doubts. We have modify our experiment in Game 1.

Game 1 :
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}, ID_{\mathcal{P}}, m_w) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(sk_{\mathcal{P}}, w_{\mathcal{S}\to\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $(Id, (m,\sigma), m'_w, w'_{\mathcal{S}\to\mathcal{P}}) \leftarrow \mathcal{A}(sk_{\mathcal{P}}, w_{\mathcal{S}\to\mathcal{P}})$,
with $w'_{\mathcal{S}\to\mathcal{P}} \in Out(\mathcal{O}_{\mathsf{DelGen}}(ID_{\mathcal{S}}, ID, sk[ID_{\mathcal{S}}], m'_w))$:
6. If $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m_w, w_{\mathcal{S}\to\mathcal{P}}) = 1$,
$\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m'_w, w'_{\mathcal{S}\to\mathcal{P}}) = 1$ with $ID \neq ID_{\mathcal{P}}$: Return 1
7. Else Return 0

The difference in between our games 0 and 1 is the ability of the adversary to forge new delegations. It would lead to a forgery against the scheme S if $\mathcal{A}$ was able to outputs such a certificate. Hence $|\mathsf{Pr}[S_0] - \mathsf{Pr}[S_1]| \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k)$. We can now consider the probability such that $\mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID_{\mathcal{P}}, m, \sigma, m_w, w_{\mathcal{S}\to\mathcal{P}}) = \mathsf{Verif}(mpk, ID_{\mathcal{S}}, ID, m, \sigma, m'_w, w'_{\mathcal{S}\to\mathcal{P}}) = 1$ for $ID \neq ID_{\mathcal{P}}$. From the steps of the Verif algorithm, it is equivalent to $\mathsf{Verif}_{\mathsf{S},vk^{\mathsf{S}}_{\mathcal{S}}}(w_{\mathcal{S}\to\mathcal{P}}, ID_{\mathcal{S}}||ID_{\mathcal{P}}||vk^{\mathsf{BS}}_{\mathcal{P}}||m_w) = \mathsf{Verif}_{\mathsf{S},vk^{\mathsf{S}}_{\mathcal{S}}}(w'_{\mathcal{S}\to\mathcal{P}}, ID_{\mathcal{S}}||ID||vk^{\mathsf{BS}'}_{\mathcal{P}}||m'_w) = 1$. But S is an unique signature scheme and thus this advantage is negligible. We directly conclude that $\mathsf{Adv}^{st-und}_{\mathsf{IDPBS},\mathcal{A}}(\mathfrak{K}) \leq \mathsf{Adv}^{uf}_{\mathsf{S}}(k) + \mathsf{Adv}^{uni}_{\mathsf{S}}(k)$.

5 Analysis of the construction

Warrant modification. The type of delegation used for our scheme implies to generates a new key pair to issued or change the contract m_w for a proxy user. Otherwise anyone getting a signature for the first contract could easily get a forgery for the new contract. This specificity requires a new communication with the signer when the warrant is changed and the issue of new keys for the proxy. This is similar to most IDPBS schemes.

Efficiency. Let $\mathsf{S} = (\mathsf{KeyGen}_\mathsf{S}, \mathsf{Sign}_\mathsf{S}, \mathsf{Verif}_\mathsf{S})$ and $\mathsf{BS} = (\mathsf{Commit}_\mathsf{BS}, \mathsf{Blind}_\mathsf{BS}, \mathsf{Sign}_\mathsf{BS}, \mathsf{Unblind}_\mathsf{BS}, \mathsf{Verif}_\mathsf{BS})$ respectively be a unique signature scheme and a blind signature scheme with the desired properties to assemble them and form a generic IDPBS as it is described above. For any IDPBS signature issuing in between a proxy signer $\mathcal{P}$ and a user $\mathcal{U}$ algorithm that need to be executed are reported in Table 1. The efficiency of this generic construction is not competitive with the best IDPBS schemes of the literature (see Section 1 for an exhaustive list), this is mostly due to the multiple sub-signature verification that have to be processed during the verification of the signature.

	$\mathsf{Verif}_\mathsf{S}$	$\mathsf{Commit}_\mathsf{BS}$	$\mathsf{Blind}_\mathsf{BS}$	$\mathsf{Sign}_\mathsf{BS}$	$\mathsf{Unblind}_\mathsf{BS}$	$\mathsf{Verif}_\mathsf{BS}$
$\mathcal{U}$	2		1		1	1
$\mathcal{P}$		1	1		1	
$\mathcal{V}$	2					1
T	4	1	1	1	1	2

Table 1: Underlying algorithm to issue or verify generic IDPBS signatures.
($\mathcal{U}$: User, $\mathcal{P}$: Proxy, $\mathcal{V}$: Verifier, T: Total)

Communication Efficiency. Both communications specified in protocol 9 (*i.e.,* between the user and the proxy signer) can be merged into the first interaction of the blind signature scheme to obtain a round optimal blind signature. The number of communications can thus be reduced to the minimum as long as round optimal signature scheme is used in the generic construction.

6 Conclusion

We propose a new generic construction for identity-based proxy blind signature, based on two basic primitives, namely a unique signature scheme and blind signature scheme. The purpose of such generic construction is to reunite fundamental, "low level" primitives with blind signature construction with additional properties. Another contribution is a formalisation of the security for identity-based proxy blind signature based on the 4 usual statements of security property that are proposed in numerous articles. We formally prove that our construction is secure. For this, we only require blindness and unforgeability of the blind signature and unforgeability and hardness to determined two different signatures for the same message. The latest property is clearly achieved by some existing schemes such as the well known BLS signature. Adding up this result with the previous literature, it is now possible to construct a secure identity-based proxy blind signature from only a few building blocks such as a signature scheme, a zero-knowledge proof, a commitment and an encryption scheme.

References

1. M. Abdalla, D. Catalano, and D. Fiore. Verifiable random functions: Relations to identity-based key encapsulation and new constructions. *Journal of Cryptology*, 2014.
2. M. Abe and E. Fujisaki. How to date blind signatures. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology — ASIACRYPT*, 1996.
3. M. Bellare and P. Rogaway. The exact security of digital signatures-how to sign with rsa and rabin. In *Eurocrypt 1996*, pages 399–416. Springer.
4. A. Boldyreva, A. Palacio, and B. Warinschi. Secure proxy signature schemes for delegation of signing rights. *J. Cryptol.*, (1), Jan. 2012.
5. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In *ASIACRYPT 2001*. Springer Berlin Heidelberg, 2001.
6. J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler. Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology — EUROCRYPT*, 1995.
7. D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, 1982.
8. Y. Dodis. Efficient construction of (distributed) verifiable random functions. In *International Workshop on Public Key Cryptography*, pages 1–17. Springer, 2003.
9. M. Fischlin. Round-optimal composable blind signatures in the common reference string model. In C. Dwork, editor, *Advances in Cryptology - CRYPTO*, 2006.
10. D. Galindo, J. Herranz, and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In *ASIACRYPT*, 2006.
11. S. Goldwasser and R. Ostrovsky. Invariant signatures and non-interactive zero-knowledge proofs are equivalent. In *Advances in Cryptology — CRYPTO' 92*, 1993.
12. J. He, C. Qi, and F. Sun. A new identity-based proxy blind signature scheme. In *2012 IEEE International Conference on Information Science and Technology*, 2012.
13. P. Heng, K. Ke, and C. Gu. Efficienct id-based proxy blind signature schemes from pairings. In *2008 International Conference on Computational Intelligence and Security*, 2008.
14. T. Jager. Verifiable random functions from weaker assumptions. In *Theory of Cryptography Conference*. Springer, 2015.
15. S. James, G. Thumbur, and P. Reddy. An efficient pairing-free identity based proxy blind signature scheme with message recovery. *ISC*, 2021.
16. W. Lang, Y. Tan, Z. Yang, G. Liu, and B. Peng. A new efficient id-based proxy blind signature scheme. In *ISCC 2004*, 2004.
17. A. Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In M. Yung, editor, *CRYPTO 2002*, volume 2442, pages 597–612, 2002.
18. S. Micali, M. Rabin, and S. Vadhan. Verifiable random functions. In *40th annual symposium on foundations of computer science (cat. No. 99CB37039)*, pages 120–130. IEEE, 1999.
19. S. Padhye and N. Tiwari. An efficient id-based proxy blind signature with pairing-free realization. In *ICIET'2016*, 2016.
20. S. Prabhadevi and A. Natarajan. Utilization of id-based proxy blind signature based on ecdlp in secure vehicular communications. *IJEIT*, (5), 2013.
21. X. Qin, C. Cai, and T. H. Yuen. One-more unforgeability of blind ecdsa. In *European Symposium on Research in Computer Security*. Springer, 2021.
22. P. Sarde and A. Banerjee. A secure id-based blind and proxy blind signature scheme from bilinear pairings. *Journal of Applied Security Research*, (2), 2017.
23. A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology*, 1985.
24. V. Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptol. ePrint Arch.*, 2004:332, 2004.

25. M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In *Advances in Cryptology — EUROCRYPT*, 1995.
26. Z. Tan. Efficient pairing-free provably secure identity-based proxy blind signature scheme. *Security and Communication Networks*, (5), 2013.
27. Z. Tan, Z. Liu, and C. Tang. Digital proxy blind signature schemes based on dlp and ecdlp. *MM Research preprints*, 21(7):212–217, 2002.
28. B. Wang, W. Liu, and C. Wang. ID-based proxy blind signature scheme with proxy revocation. In *2nd International Workshop on Computer Science and Engineering, WCSE 2009*.
29. C. H. Wang and J.-Y. Fan. The design of id-based fair proxy blind signature scheme with weak linkability. In *ISIC*, 2012.
30. L. Wei-min, Y. Zong-kai, C. Wen-qing, and T. Yun-meng. A new id-based proxy blind signature scheme. *Wuhan University Journal of Natural Sciences*, (3), 2005.
31. M. Yang and Y. Wang. A new efficient id-based proxy blind signature scheme. *Journal of electronics (CHINA)*, (2), 2008.
32. X. Yi, K.-Y. Lam, and D. Gollmann. A new blind ecdsa scheme for bitcoin transaction anonymity. Cryptology ePrint Archive, Report 2018/660, 2018.
33. Y. Yu, S. Zheng, and Y. Yang. Id-based blind signature and proxy blind signature without trusted pkg. In *Computer Society of Iran Computer Conference*, 2008.
34. F. Zhang and K. Kim. Id-based blind signature and ring signature from pairings. In *ASIACRYPT*, 2002.
35. F. Zhang and K. Kim. Efficient id-based blind signature and proxy signature from bilinear pairings. In *Australasian Conference on Information Security and Privacy*, 2003.
36. H. Zhu, Y.-a. Tan, L. Zhu, Q. Zhang, and Y. Li. An efficient identity-based proxy blind signature for semioffline services. *Wireless Communications and Mobile Computing*, 2018.