A Survey on Identity-based Blind Signature

Mirko Kiscina[1 [0000−0003−4158−6952]], Pascal Lafourcade[2 [0000−0002−4459−511X]], Gael Marcadet[2 [0000−0003−1194−1343]], Charles Olivier-Anclin[1,2 [0000−0002−9365−3259]], and Léo Robert[2 [0000−0002−9638−3143]]

[1] be ys Pay

[2] Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, France

Abstract. Blind signatures are well-studied building blocks of cryptography, originally designed to enable anonymity in electronic voting and digital banking. Identity-based signature were introduced by Shamir in 1984 and gave an alternative to prominent Public Key Infrastructure. An identity-based blind signature (IDBS) allows any user to interact directly with the signer without any prior interaction with a trusted authority. The first IDBS has been proposed in 2002 and several schemes were proposed since then. Seeking for a full comparison of these primitives, we propose a survey on IDBS and list all such primitives that seems to maintain some security. We also classify their security assumptions based on the existing security expectation that have not been formalised yet in the literature. Moreover, we empirically evaluate the complexity of all the operations used in those schemes with modern cryptographic libraries. This allows us to perform a realistic evaluation of their practical complexities. Hence, we can compare all schemes in terms of complexity and signature size.

Keywords: Identity-based Blind Signature, Survey, Complexity Evaluation.

1 Introduction

Since the creation of the Internet, physical cash is progressively replaced through digitalisation by electronic payments methods like smart card or phone using NFC technology. Within this transformation, specific properties of cash were lost such as anonymity or unlinkability of the customer. In 1982, D. Chaum introduced a cryptographic response to this problem, called *blind signature* [14]. He described this concept as an analogue of an envelope composed of carbon paper that could be signed from the outside where the signature is engraved on a message inside.

For a concrete example, consider the following case where blind signature is helpful. Suppose that a customer wishes to buy a product at 10€ in a store. It asks to its bank a (blind) signature which is worth 10€ [3]. The customer then gives this signature to the shopkeeper against the 10€ worth product. The latter sends the signature back to the bank for payment. In this setting double spending is checked by the bank since each payment corresponds to a signature. Moreover, unlinkability is ensured since the bank knows that the customer has withdrawn 10€ but it cannot link it with the inquiry from the shopkeeper. Another well-known application for this primitive is the voting scheme in order to ensure that only registered voter can actually vote [44, 51].

[3] In this example, a signature defines a given amount of money.

One of the first scheme using blind signature was developed by D. Chaum, A. Fiat, M. Naor in 1988 [15]. In 1992, S. Von Solms and D. Naccache [85] described a hostage taking that could lead to a crime without possibility to trace down a ransom pay to the criminal through coins made of blind signatures. It shows the necessity to extend the definition of blind signature to give more power to the signer. The goal is to be able to apply blind signature without threat. Therefore, extensions of blind signature such as partially blind signature [3], signer-friendly blind signature, fair blind signature [75] and many others were developed. Those properties allow more control for the signer by adding information or putting constraints on the use of a signature.

Before 1994, factorisation was the only hard problem that yield to blind signature. That year was a turnover for the domain, J.L. Camenisch *et al.* [13] introduced the first a blind signature scheme based on the discrete logarithm problem. This scheme was an adaptation of the Nyberg-Rueppel scheme [63] leading to a relatively efficient blind signature. This scheme was also the first blind signature to have an additional property: *message recovery* (signed message is recovered from the public key and the signature).

Following A. Shamir's introduction of identity-based cryptography [72], signature and blind signature schemes were developed using this paradigm. The first ID-based blind signature was introduced by F. Zang and K. Kim [95] in 2002, only one year after the first use of pairing. In 2004, C. Sherman *et al.* [19] opened up the way to ID-based partially blind signature with a new scheme achieving partial restrictive blindness. The next year D. Galindo *et al.* [26] gave a general construction of IDBS only requiring a secure signature and a secure blind signature. This general framework achieved relatively good efficiency, but the signatures generated are about twice as large as a signature of made out schemes (the signature is the concatenation of both signature schemes).

There exist numerous properties proposed by a variety of IDBS schemes with the same practical applications as blind signature. Each situation has specific requirements and depending on the context one may use one schemes or another. Our main goal in this survey is to answer the question of how to choose an IDBS (with which property) for practical use. We list all existing schemes, classify them accordingly to their properties and security assumption; we also compare them using an empirical evaluation. We have included all IDBS[4] as they are for a vast majority independent works. Some does not meet the requirement to be use in practice, but we mention them for exhaustiveness as this may be of interest for authors trying to design new schemes. In such cases we have written the mentions "No reduction", "No proof" or "Not formal" depending on the category the fall within. The authors do not recommend usage of any schemes with one of these mentions in the upcoming table. Their evaluation is not included as this would be irrelevant to compare them with scheme that have guaranteed security.

Contributions. Our contribution aims at bring new considerations on IDBS. Our first contribution is a survey presenting the existing portfolio to someone seeking to implement these primitives. In this paper, we aveluate all existing IDBS, this is not less than 71 schemes. We classify them within several categories that we discuss throughout this paper. Some reach additional properties that we all present in here. This allows us to give a full overview of the literature in the field and the existing properties reach by some existing IDBS scheme. We notice that among the existing schemes, some of them

[4] The authors apologies if any scheme have been omitted in this survey.

(at least 24 schemes) do not reach today's security requirements as no formal security argument have been given by their authors or in the literature we have investigated. We point them out without going into further details on them. Scheme with existing security arguments are investigated further. We start by empirically evaluate the cost of all operations used in existing IDBS schemes. It allows us to establish a metric to evaluate the time efficiency of each part of the given signatures. This answer our goal *i.e.,* obtaining a taxonomy of the reliable schemes in terms of efficiency and cryptographic assumption. This enables us to give insights on the schemes that actually reach the best efficiency in practice.

In addition to a survey of all the ID-based blind signature with several properties, we have tried to give some formal security definitions for all the type of scheme we are investigating in this paper. These results are given in the appendix of the paper, see Section B. We hope it will bring up the security of the new ID-based blind signature that will be design in the future or at least help giving some further formalisation of their security as this has never been achieved for some of them.

Related Work. A few surveys related to blind signature schemes have been presented. To the best of the authors' knowledge, we noticed three of them. The first one [6], gives an overview of 8 existing blind signature schemes and other notions that are directly related to blind signature. It also presents some properties of blind signatures. A second short paper called survey on IDBS was proposed in 2015 by Girish *et al.* [32], but it does not give insights on the existing schemes instead present the concept and some existing property without much formalism. In 2018, M. Khater *et al.* [50] compared some blind signatures based on ElGamal. Only 5 schemes derived from the well-known signature are presented and evaluated. They compare the influence of modification in the scheme parameters, such as the number of blinding factor and its influence on the complexity. We include their signatures in our Survey.

All the above cited works only offer a partial view of existing identity-based blind signature schemes and yet it is hard to get a realistic view of the state of the art of the existing literature. Moreover, they do not compare the performance of the schemes in the literature. Our objective is to present a full overview of the existing literature, while our achievement is a detailed taxonomy of all existing IDBS schemes and of the numerous sub-properties. Unlike the above cited papers, we ambition to be exhaustive and to give a full description of field of IDBS.

Outline: Section 2 introduces the security assumptions and the definitions of an ID-based blind signature schemes and its additional properties. Details about our evaluation process are given in Section 3. In Section 4.1, we are comparing the existing schemes. Finally, in Section 5 we give insights of some work that should be done to put forward the domain. In Section 6 we conclude our study.

2 Cryptographic Definitions

Blind signature schemes rely on hard mathematical problems for their security. Those assumptions should be well-studied, and assumed to be intractable in resonable time. The Discrete Logarithm problem (DL) relies on the difficulty to compute the discrete

logarithm of an element in some groups. The Decision Diffie-Hellman (DDH), Computational Diffie-Hellman (CDH), Gap Diffie-Hellman (GDH) and the Chosen Target Accompanied Computational Diffie-Hellman problems (CT-ACDH) [16] result directly from it. There are also some variants such as the q-Strong Diffie-Hellman (q-SDH), the k-Bilinear Diffie-Hellman Inversion (k-BDHI), the One-more Bilinear Diffie-Hellman Inversion (1m-BDHI) or the Collusion Attack Algorithm with k traitors (k-CAA). These problems are mostly used for schemes based on elliptic curves. Recently, a polynomial time (PT) algorithm was disclosed solving the Over-determined Solvable System of Linear Equations modulo q with Random inhomogeneity problem (ROS). This led to attacks on many schemes [8] and some IDBS were relying on it.

Alternatives to elliptic curves have been investigated aiming at post-quantique security. Those solutions are essentially based on lattices, notably the Short Integer Solution problem (SIS), the Shortest Vector problem (SV) and its variant on quotient ring the Ring Short Integer Solution problem (R-SIS). One last rather unusual problem that we need here is the Chebyshev Polynomial Computation problem (CPC) [78]. This problem is known to have a reduction to the discrete logarithm in a finite group $GF(p)$, for some prime p [77]. Formal definitions of all these assumptions are given in Section A. All existing IDBS are based on one of these problem, we formally introduce the concept of IDBS and informally present the multiple properties that have been put based on this definition.

Definition 1 (IDentity-based Blind Signature - IDBS). *An IDBS with security parameter $\mathfrak{K}$ is a 4-tuple of polynomial-time algorithms (*Setup*,* Extract*, $\langle\mathcal{S},\mathcal{U}\rangle$*,* Verif*) involving an authority $\mathcal{M}$, a signer $\mathcal{S}$ and a user $\mathcal{U}$. Algorithms are as follows:*

- $\mathsf{Setup}(1^{\mathfrak{K}}) \rightarrow (mpk, msk)$ *calls $\mathfrak{K}$ to generate a master key pair (mpk, msk).*
- $\mathsf{Extract}(msk, ID) \rightarrow sk[ID]$ *on input $\mathcal{S}$'s identity and a master key msk. It returns a secret key $sk[ID]$ latter sent to $\mathcal{S}$ via a secure channel.*
- $\langle\mathcal{S}(sk[ID]), \mathcal{U}(mpk, m, ID)\rangle \rightarrow \sigma$ *is the signature issuing protocol between the signer $\mathcal{S}$ and the user $\mathcal{U}$ for a message $m \in \{0,1\}^*$. It generates the signature σ.*
- $\mathsf{Verif}(mpk, ID, m, \sigma)$ *outputs 1 if the signature σ is valid for m, otherwise 0.*

Secure IDBS must meet the three following security properties. *Correctness*, meaning that for any keys and any messages, the signature must always be accepted if all algorithms are honestly executed. *Blindness* requires that no information about the message could be revealed to the signer during the protocol. Finally, *unforgeability* requires that a user cannot forge new signatures from any set of existing signatures. Any of the upcoming schemes will have to meet these three basic properties. Formal security definitions are provided in Appendix B.

We now describe in turn the other primitives based on IDBS.

ID-based Proxy Blind Signature - IDPrBS. An original signer $\mathcal{S}$ delegates its right to sign to a proxy signer $\mathcal{P}$. After being provided with a key and a public agreement, $\mathcal{P}$ is allowed to sign any message coming from a user $\mathcal{U}$ and falling within the agreement. IDPrBS should satisfy the security properties of correctness, blindness and unforgeability. But should also meet additional properties [12]: *Prevention of misuse*: proxy signing key cannot be used for purposes other than generating valid proxy signatures. In case of misuse, the responsibility of the proxy signer should be determined explicitly. *Verifiability*: From a proxy signature, a verifier can be convinced of the original

signer's agreement on the signed message. *Strong Identifiability*: Anyone can determine the identity of the proxy signer from a proxy signature. *Strong Undeniability*: A proxy signer cannot repudiate a proxy signature it created.

ID-based (Restrictive) Partially Blind Signature - IDPBS/IDPRBS **[3].** Prior to the protocol, the user and the signer have to agree on a common part denoted info. Instead of signing the usual message, $m||\mathsf{info}$ is signed. Restrictiveness is an additional constraint put by the signer on the user. $\mathcal{U}$ is only able to get a signature on a message of a certain form, specified by the signer. Those schemes have almost the same security properties as IDBS schemes. The only added difference is the inability of the user to modify the common part unilaterally. We also have a modified version of blindness called *partial blindness* where the signer always knows the common part of the message.

ID-based Fair Blind Signature - IDFBS **[76].** *Fairness* gives the capability to a trusted entity to perform one or two types of link recoveries:

Type I: The trusted entity can output information that enables the signer to recognise the corresponding message-signature pair (*e.g.,* the judge can extract the message from the signer's view of the protocol).

Type II: The trusted entity can output information that enables the signer to efficiently identify the sender or to find the corresponding view of the signing protocol.

ID-based Blind Signature with Message Recovery - IDBSMR**.** For a given signature and public key pair, there exists a verification algorithm that outputs the signed message. This property is useful to reduce the size of exchanged information. It requires a bijection between the possible messages and the group elements that will be used during the signing process.

ID-based Forward-Secure Blind Signature - IDFSBS **[100].** Consider the lifetime of a system divided into N time periods. In a blind signature context, forward secrecy means that unforgeability of signatures is valid in previous time periods even if current signing secret key of the signer is compromised. Thus, if the private key is compromised, only the signature for the current time period are forgeable. No signature for any previous time period can be forged, hence they remain safe to use.

ID-based Blind Signature with Batch Verification - IDBSBV **[7].** Batch verification has been designed to allow fast verification of multiple signatures. In practice a specific algorithm of verification VerifMult allows to verify a list of message-signature pair $\{(m_1, \sigma_1), \ldots, (m_n, \sigma_n)\}$ with the public key pk and output 1 if all signatures are valid, otherwise 0. We can allow this verification to be probabilistic with negligible probability of failure. Yet we want this verification to run significantly faster than n computations of the Verif algorithm.

ID-based Weak Blind Signature - IDWBS **[102].** This type of scheme does not achieve unlinkability when the signature is revealed to the signer *i.e.,* the signer is able to link the revealed signature to a user when it has a clear view of the message-signature pair.

3 Evaluation Process

We have evaluated all known IDBS schemes with a proven security to choose the most practical one. Here we present a metric to evaluate their complexity. We further evaluate their inner operations in order to compare them.

In order to evaluate the schemes we had to choose concrete evaluation parameters. Our chosen parameters follow the recommendations of the ECRYPT's reports on key length [23]. These are similar to the more recent NIST's recommendations. We use 3072 bits integers and equivalent 256-bits elliptic curves *i.e.,* over finite field $\mathbb{F}_q$, with q of size 256 bits. In practice, it provides around 128 bits of security. Notice that recommendations for parameters of lattice differ from scheme to scheme, moreover, almost none of the authors of the listed papers gave concrete parameters for there schemes. Based on these elements, we chose to left out reduction for lattice based scheme as parameters for these schemes are still imprecise. However, we evaluate the numbers of operations that each existing scheme requires.

In order to compare all the existing scheme, we first compare the execution time of each operation with the execution time of a standard 3072 bits integer multiplication. Based on these result we can reduce the complexity of each signature scheme in terms of an unified unit: $T_{MUL_{3072}}$. Table 1 express the execution time of relevant operation op with the proposed conversion. T_{op} corresponds to the ratio between the execution time of each operation and a 3072 bits integer multiplication.[5] Our results are based on benchmarks on an Intel Core i7-1065G7 CPU @ 1.30GHz processor without parallelism and generated using modern cryptographic libraries like GMP library [33] (arithmetical operations on integers), MPHELL library [1] (elliptic curve's operations), PBC library [61] (pairing functions) and OpenSSL/Crypto [2] library (hash functions) using state-of-the-art speed up.

We use the notations Minv, Mmul, Mtran, Madd for associated arithmetical operations on matrices. MVmul denotes a multiplication between a matrix and a vector. SVmul is the multiplication of a vector by a scalar. Vadd stands for the addition of two vectors. Vh and Mh are hash functions returning respectively a vector or a matrix. Sample is a sampling operation defined in [31]. We also use the following notations for usual scalar operations: EXP, MUL, ADD, INV. Moreover, ECMUL [6] and ECADD hold for multiplication and addition on elliptic curve. PAIR is the evaluation of a pairing function. H is for evaluation of a hash function and PH holds for hash function mapping on elliptic curve. Less common operation as CHEBY denotes the evaluation of a Chebyshev polynomial. TR denotes the trace function $TR(h) = h + h^2 + h^4$ in $GF(p^6)$ in the context of XTR (Efficient and Compact Subgroup Trace Representation [57]) schemes.

We summarise our results in two types of tables. The first type of table (*e.g.,* Table 2) gives a quick overview of a scheme with the following characteristics: mathematical setting (EC, pairing, *etc.*), security assumptions (CDH, ECDL, *etc.*), number of needed interactions and the number of random elements generated by a user to blind a message, also called *blinding factor*.

[5] Note that our conversion are relatively similar to some existing literature [48, 62, 81].

[6] It is not clear whether authors recommend symmetric or asymmetric pairing for their schemes. Based on that, we chose to unified the execution time for the two based group G_1 and G_2.

Operation	256	512	3072	Operation	256	512	3072
$T_{Pairing}$	89.72	698.53		T_{GCD}	0.62	1.19	8.69
T_{TR}	52.12			T_{INV}	0.30	1.14	4.03
T_{EXP}	3.34	18.52	712.15	T_{ECADD}	0.16	0.67	
T_{HP}	3.99	4.65		T_{MUL}	0.08	0.10	1.00
T_{ECMUL}	2.99	12.14		T_{CHEBY}	0.05		
T_H	1.05	1.71		T_{ADD}	0.04	0.07	0.20
T_{GCD}	0.63	1.19	8.64				

Table 1: Conversion in $T_{MUL_{3072}}$.

The second type of table evaluates and compare the complexity of the schemes. It splits the complexity within the 3 entities in presence: the user $\mathcal{U}$, the signer $\mathcal{S}$ and the verifier $\mathcal{V}$. The total cost for all executions in terms of operations is in row T. The penultimate column gives our reduction in $T_{MUL_{3072}}$. Last column gives the number of elements composing the signature. Depending on the context, it can be group elements or vectors. The final size of the signature depends on the security parameter $\mathfrak{K}$.

4 Schemes Presentation

4.1 ID-based Blind Signature - IDBS

We have identified 32 IDBS schemes in the literature, they are listed in Table 2. The table gives the mathematical setting, the hard problem when a reduction is provided for the signature, the number of communications and the blinding factor. We chose these characteristics because communication between two distant machines can sometime be longer than running time of any algorithm of the signature edition. On another hand, we specify the number of random parameters to be generated each time. Generating cryptographically-secure randomness is costly, hence a low number of blinding factors can speed up the signature issuing and requires less resources.

Most schemes rely on pairing function and the CDH problem. Some such as [35,54] are pairing free and consequently faster to execute. Due to the increasing development of post-quantum cryptography, new IDBS schemes have been designed based on the SIS problem. Another base concept is XTR. Introduced by Lenstra *et al.* [57], this cryptographic basis leads to smaller signatures for the same security level. For instance, one would need 512-bits prime integers to achieve equivalent security to discrete logarithm problem with prime of 3072 bits. We have used the conversions from [57] to evaluate the operation of scheme from [80] as parameters of the scheme in [98] are not clear. Thus, we cannot propose a rigorous evaluation for this scheme. However, we can infer its relatively slow speed since a zero-knowledge proof procedure is used to sign a message.

Complexity evaluations of pairing based schemes are provided in Table 3 and 4, in Table 5 for lattice based schemes and in Table 6 for the others. From this evaluation we note that the execution of an elliptic curves based signature gives better complexity than evaluation of a pairing function. Thus, pairing based signatures are less efficient. We have observed that Chebyshev polynomials are fast to evaluate, hence it produces an efficient scheme. Chaotic maps can be efficient, but their security needs to be more studied, yet a reduction to the discrete logarithm problem is given [78].

We conclude that the fastest pairing based scheme is 4 times faster than the slowest one. And again, the best pairing free scheme is 5 times faster than the best pairing

Ref	Year	Mathematical base	Security reduction	Interactions	Blinding factor
[54]	2018	Elliptic curve	ECDL	3	4
[35]	2011				3
[22]	2020	Pairing	CDH	3	3
[98]	2010				1
[71]	2010				
[4]	2010				
[43]	2009				2
[42]	2005				
[95]	2002				
[96]	2002				
[41]	2010			2	4
[65]	2009				1
[30]	2012		1m-BDHI	2	2
[30]	2012				
[29]	2008				1
[53]	2017		ECDL	2	1
[40]	2011		Q-SDH	4	5
[55]	2017		GDH	3	1
[80]	2013		No reduction	3	2
[101]	2014				
[92]	2013				
[46]	2013				
[43]	2009				
[43]	2009				
[49]	2008				
[97]	2003				
[102]*	2007				3
[59]	2020	Lattice	SIS	4	3
[27]	2016			2	1
[28]	2017				
[73]	2018	Modular Groups	No reduction	3	3
[78]	2020	Chaotic map	CPC	3	1

Table 2: Identity-Based Blind Signature. (* Weak Linkability)

based scheme. The complexity of [54] and [35] is close, and the difference might be negligible regarding time needed for cache affectation during the execution of properly implemented scheme. The only advantage is for [35], it uses less random values, but it might be compensated by the lowest complexity of the former scheme. Elliptic curve schemes still remain the most efficient schemes relying on a well-studied problem.

4.2 ID-based Proxy Blind Signature - IDPrBS

Sorting the scheme by type of underlying problem, we give an overview of the existing IDPrBS in Table 7. Part of the existing schemes lack of formal security arguments. Three schemes are still recorded in our survey, but this is specified in the table. There exist IDPrBS based on the tree prominent type of problems: elliptic curves, pairing and lattice. Proxyness is the most studied property for IDBS, a generic construction exist for this primitive as highlighted in Section 4.5. The first scheme was introduced in 2003, only two years after the first appearing of pairing in cryptography in [56]. Ten years later was published the first paring-free scheme [79]. It led to one of the most efficient schemes of this survey and was proven as hard as the well-studied ECDL problem. With the development of quantum computer and the growing threat on classical assumptions, two lattice based schemes were developed [68, 74]. Sadly, attacks were found on both primitives. Thus, finding a lattice based IDPrBS is still an open problem.

Ref		EXP	PAIR	ECMUL	ECADD	MUL	ADD	INV	H	PH		Total	Size
[54]	$\mathcal{U}$			2		18	2	5	1		1 gcd	10.74	3
	$\mathcal{S}$			2		4	2					6.42	
	$\mathcal{V}$			3	1	1			1			10.30	
	T	0	0	7	1	23	4	5	2	0	1 gcd	27.46	
[35]	$\mathcal{U}$			4	3	2	2	1	2			15.16	3
	$\mathcal{S}$			1		1	1					3.13	
	$\mathcal{V}$			3	2				2			11.44	
	T	0	0	8	5	3	3	1	4	0		29.73	
[53]	$\mathcal{U}$			2	1	1	1		2	1		12.39	2
	$\mathcal{S}$			2		1		1	2			8.48	
	$\mathcal{V}$		2	1	1				1			183.66	
	T	0	2	5	2	2	1	1	5	1		204.54	
[95]	$\mathcal{U}$		1	3	2		2		1			100.20	2
	$\mathcal{S}$			3	1							9.17	
	$\mathcal{V}$	1	2			1		1	1			182.46	
	T	1	3	6	3	1	2	1	2	0		291.83	
[102]	$\mathcal{U}$			6	2	2	1	1	1			19.89	3
	$\mathcal{S}$			5	2	1						15.41	
	$\mathcal{V}$		3	1	1				2			274.43	
	T	0	3	12	5	3	1	1	3	0		309.74	
[22]	$\mathcal{U}$			6	2	4	1	1	1			20.06	3
	$\mathcal{S}$			5	2	1			2			17.52	
	$\mathcal{V}$		3	2	1							275.33	
	T	0	3	13	5	5	1	1	3	0		312.91	
[4]	$\mathcal{U}$		1	3	2	1	2		1			100.28	2
	$\mathcal{S}$	1	1	2	1							97.47	
	$\mathcal{V}$	1	2					1	1			182.38	
	T	2	4	5	3	1	2	1	2	0		380.14	
[71]	$\mathcal{U}$		1	4	2		1		1			103.15	2
	$\mathcal{S}$	1	1	2	1							97.47	
	$\mathcal{V}$	1	2						1			182.08	
	T	2	4	6	3	0	1	0	2	0		382.71	
[55]	$\mathcal{U}$		1	2		1		1	2			98.21	2
	$\mathcal{S}$		1	3		3	1		3			102.17	
	$\mathcal{V}$		2	1	1				1			183.66	
	T	0	4	6	1	4	1	1	6	0		384.04	
[96]	$\mathcal{U}$		1	3	3		2		1				2
	$\mathcal{S}$			3	1								
	$\mathcal{V}$	1	2			1		1	1				
	T	1	3	6	4	1	2	1	2	0			

Table 3: Evaluation of IDBS Schemes.

Ref		EXP	PAIR	ECMUL	ECADD	MUL	ADD	INV	H	PH	Total	Size
[42]	$\mathcal{U}$	3	3	1	1	3			1		278.38	2
	$\mathcal{S}$	1	1	1		1	1				94.43	
	$\mathcal{V}$	1	1								91.31	
	T	5	5	2	1	4	1	0	1	0	464.12	
[40]	$\mathcal{U}$			21	18	8	4	1			67.15	4
	$\mathcal{S}$			11	9	4					34.83	
	$\mathcal{V}$	1	4	6	6						379.48	
	T	1	4	38	33	12	4	1	0	0	481.46	
[30]	$\mathcal{U}$		4	4		1		2		1	375.56	3
	$\mathcal{S}$			3				1			9.30	
	$\mathcal{V}$		4								358.89	
	T	0	8	7	0	1	0	3	0	1	743.75	
[29]	$\mathcal{U}$		4	4		1		2		1	375.56	3
	$\mathcal{S}$			3				1			9.30	
	$\mathcal{V}$		4							1	362.88	
	T	0	8	7	0	1	0	3	0	2	747.74	
[30]	$\mathcal{U}$		4	5	3			1		2	382.68	3
	$\mathcal{S}$			4	1					1	16.16	
	$\mathcal{V}$		4		1						359.06	
	T	0	8	9	5	0	0	1	0	3	757.89	
[41]	$\mathcal{U}$			9	3|ID|+2|m|+10	3	1	1			245.00	4
	$\mathcal{S}$			4	|ID|+3	1					55.73	
	$\mathcal{V}$		5	1	2|ID|+|m|+3						581.56	
	T	0	5	14	6|ID|+3|m|+16	4	1	1	0	0	882.29	
[65]	$\mathcal{U}$		4	6	|ID|+|m|+3	2			Commit		463.85	3
	$\mathcal{S}$			2	2						6.34	
	$\mathcal{V}$		4		|ID|+|m|+2	2			Check		445.85	
	T	0	8	8	2|ID|+2|m|+7	4	0	0	0	0	915.53	

Table 4: Evaluation of IDBS Schemes.
($|\cdot|$ denote the hamming weight of an element in binar representation.)

Lattice based IDBS																
Ref		Minv	Mmul	Madd	MVmul	SVmul	Vadd	Norm	Sqrt	Mul	Inv	Vh	Mh	Sample	Size
[59]	$\mathcal{U}$	Commit			3		4						1		2
	$\mathcal{S}$				2		1								
	$\mathcal{V}$	Check			1	1	1	1					1		
	T	0	0	0	6	1	6	1	0	0	0	0	2	0	
[28]	$\mathcal{U}$	1	1		1	2	2				1	1	1		1
	$\mathcal{S}$	1	1		1			1	1	1			1	1	
	$\mathcal{V}$	1	1		1			1	1	1			1		
	T	3	3	0	3	2	2	2	2	2	1	1	3	1	
[27]	$\mathcal{U}$		1	2+k	1	1					1	2	1		1
	$\mathcal{S}$				1			1						1	
	$\mathcal{V}$		1	2+k	1			1					1		
	T	0	2	0	3	1	0	2	0	0	1	2	2	1	

Ref		Minv	Mmul	Mtran	MVmul	Vadd	Norm	Sqrt	MUL	Mh	Sample	size
[100]	$\mathcal{U}$	2	1	1	3	1			I	I+1		1
	$\mathcal{S}$										1	
	$\mathcal{V}$	1	1	1	1		1	1	1	I+1		
	T	3	2	2	4	1	1	1	1	0	1	

Table 5: Evaluation of IDBS Schemes using Lattice.
"I" represents the time session index in a context of a Forward Security scheme

Ref		TR	CHEBY	EXP	MUL	ADD	INV	H	Total	Size
[78]	$\mathcal{U}$		3		9		2		17.20	2
	$\mathcal{S}$		1		13	1		1	17.77	
	$\mathcal{V}$		6		12	1			12.36	
	T	0	10	0	34	2	2	1	47.34	

Table 6: Evaluation of IDBS Schemes using (from top to bottom)
Chaotic Maps, XTR and Modular Groups.

In Table Table 8, 9 and 10, make up our complexity comparison of the existing IDPrBS for the issuing and verification part. Note that we do not report complexity of schemes with existing security flaw in this paper. A list of all operations used in the generating protocol and verification process of a new signature is given from the point of view of the user, the signer, and the verifier. We left out of our estimation the other algorithms (setup, extraction, delegation, and key generation) as they have to be run only once. Due to the complexity of computing a pairing function, all schemes using such function are less efficient than the one using only elliptic curve's operations.

A record of the number of elements necessary for the signature is also given. As we are working on 256-bits elliptic curves, one can reduce the size of an element to 257 bits. Signature can thus be reduced to 257 bits per element. For IDPrBS it leads to signatures of size 514, 771 or in some cases 1028 bits. For lattice based schemes those signatures are longer and depend on the dimension. The signature length corresponds to two or four vectors of elements.

With our comparison, we claim that the most efficient, proven secure, ID-based proxy blind signature is the one from S. James *et al.* [48].

Scheme	Year	Mathematical base	Security proof	Interactions	Blinding factor
[48]	2020	Elliptic curve	ECDL	3	2
[79]	2013				
[64]	2016		No proof	3	3
[67]	2013				
[36]	2012	Pairing	ECDL	3	2
[37]	2008		k-BDHI	3	2
[94]	2008		No proof	3	2
[56]	2004				
[69]	2017		Not formal	3	2
[86]	2009				
[93]	2008				
[91]	2005				
[88]	2012			4	2
[99]	2014	Lattice	Attack	2	3
[103]	2018				2

Table 7: ID-based Proxy Blind Signature Scheme.

Ref		Pair	ECMul	ECAdd	Exp	Mul	Add	Inv	Hash	PHash	Total	Size
[37]	$\mathcal{U}$		1		2	2	2	1	1		7.77	3
	$\mathcal{S}$		1		1						4.58	
	$\mathcal{V}$	1	2	2	2	4	1		3		102.75	
	T	1	4	2	5	6	3	1	4	0	115.11	
[36]	$\mathcal{U}$	2	2	2					1		186.83	3
	$\mathcal{S}$	2	1	1							182.61	
	$\mathcal{V}$	2	2		2				4		192.81	
	T	6	5	3	2	0	0	0	5	0	562.26	

Table 8: Analysis of Signature Issuing of IDPrBS Scheme Using Pairing.

4.3 ID-based Partially Blind Signature - IDPBS

IDPBS sometime with restrictiveness as described in Section 2 are exposed in Table 11. These signatures allow adding auxiliary information to the message making them relevant for practical usages. This common information put in context improves management of signature and security. For example, it allows the signer to add an expiration date to its signatures. Up to today, 14 IDPBS have been published. As explained before, restrictiveness requires the user to fit its message to a specific structure. The user has fewer capabilities while the signer has more control. Due similarities between restrictive IDPBS and classical IDPBS, we are evaluating them all together.

The complexity of the secure schemes is given in Table 12 and 13. IDPBS were published from 2004. The first published scheme had restrictiveness and was based on

Ref		Minv	Mmul	MVmul	SVmul	Vadd	Norm	sqrt	Vhash	Mhash	SamplePre	Size
[99]	$\mathcal{U}$	2	2	2	2	log(M)+1				2		2 vect
	$\mathcal{S}$	2	2				2	1		2	2	
	$\mathcal{V}$	2	2	2		log(M)	2	1		2		
	T	6	6	4	2	2 log(M)+1	4	2	0	6	2	
[103]	$\mathcal{U}$			1	2	7			1			4 vect
	$\mathcal{S}$			3	1	4	1	1	2			
	$\mathcal{V}$			2	2	4	2	1	3			
	T	0	0	6	5	15	3	2	6	0	0	

Table 9: Analysis of Signature Issuing of IDPrBS Using Lattice.

Ref		ECMul	ECAdd	Exp	Mul	Add	Inv	Hash	Total	Size
[48]	$\mathcal{U}$	2			4	1	1	4	10.87	3
	$\mathcal{S}$	2			1	1			6.12	
	$\mathcal{V}$	5	4			1		6	22.02	
	T	9	4	0	5	3	1	10	39.03	
[79]	$\mathcal{U}$	7	5		4	2	1	4	26.76	2
	$\mathcal{S}$	1			1	1			3.12	
	$\mathcal{V}$	7	5					3	24.99	
	T	15	10	0	5	3	1	7	54.88	

Table 10: Analysis of Signature Issuing of Pairing Free IDPrBS Scheme.

Scheme	Year	Mathematical base	Security proof	Interactions	Blinding factor
[21]*	2019	Elliptic curve	ECDL	3	4
[45]	2016				2
[58]	2013	Pairing	CDH	2	2
[89]	2007			3	4
[90]*	2008				4
[18]	2007				4
[39]*	2007				4
[18]*	2007				7
[17]*	2005				7
[19]*	2004				3
[16]	2009		CT-ACDH	2	2
[38]	2007		Attack	3	2
[82]	2009				2
[87]*	2008		Not formal	3	7

Table 11: ID-based Partially Blind Signature Scheme. (*Scheme with Restrictiveness)

pairing. Only latter, in 2016, a first scheme was proposed avoiding the use of pairing based cryptography, published by H. Islam *et al.* [45] it introduced the first elliptic curve based scheme leading to better efficiency when issuing signatures. Pairing free schemes are faster than pairing based by a factor of 1.5 to more than 10. Up to now, no lattice based or quantum resistant blind signature has been proposed with the aforementioned properties. The scheme's signature sizes varies from 2 elements (*i.e.,* 514 bits), being relatively short, up to 6 elements (*i.e.,* 1542 bits) clearly leading to more computation during the verification process.

Restrictive IDPBS from [18] is a combination of two schemes. One achieving partial blindness and the other restrictiveness. This construction is not optimal since it is more than twice as complex as the one achieving only partial blindness. Its complexity and signature size would exclude it from any further use.

Efficiency of [58] mostly depends on the length of the message m, the info info and the identity ID. The number of operations for issuing a signature depends on the previous lengths. In our evaluation, the complexity of the scheme is given for elements of length 256 *i.e.,* $|m| = |\mathsf{info}| = |ID| = 256$.

Scheme from [45] seems to be the best fitted algorithms as it is one of the most efficient schemes that we have recorded in our survey. Although its security is proven in the random oracle model, it is an efficient signature algorithm with a short signature, thus could be use in practice.

Ref		ECMul	ECAdd	Exp	Mul	Add	Inv	Hash	Total	Size
[45]	$\mathcal{U}$	3	2		3	2	1	1	11.02	2
	$\mathcal{S}$	1			1	1			3.12	
	$\mathcal{V}$	2	1					1	7.21	
	T	6	3	0	4	3	1	2	21.36	
[21]*	$\mathcal{U}$	11	7		8	2	1	1	36.26	4
	$\mathcal{S}$	4			1	1			12.12	
	$\mathcal{V}$	4	2					1	13.38	
	T	19	9	0	9	3	1	2	61.77	

Table 12: Analysis of Pairing Free IDPBS Scheme. (*Restrictiveness)

4.4 ID-based Blind Signature With Other Properties

We describe and evaluate IDBS schemes with additional properties: message recovery, fairness, forward security and batch verification. These notions are quickly introduced in Section 2. Fewer signatures have been presented in the literature with these properties. A brief overview of their usefulness is given, followed by the usual evaluation routine (see Section 3). For a short overview of the characteristics of the schemes see Table 14. For their evaluation refer to Table 15.

ID-based Blind Signature with Message Recovery - IDBSMR

IDBS schemes with message recovery allow to recover the message from the signature and the public key. The six existing schemes are presented in Table 14. They rely for the most recent one on elliptic curves and on pairing function for the rest of them. Efficiency of these schemes are comparable to the most efficient of this survey. The best known pairing based IDBSMR here only requires half of the computation expected toward the best pairing based IDBS. For their evaluation refer to Table 15.

A scheme with message recovery has to handle carefully the verification phase. All schemes with message recovery have a small signature only composed of two group elements. The size of the signature can be reduced to 514 bits via a simple compression algorithm. It is still an open problem to present a round-optimal IDBS with message recovery. The existing IDBS with message recovery all need 3 communications. This is an essential point for a blind signature scheme as communication comes at a cost in terms of time efficiency of the protocol.

ID-based Fair Blind Signature - IDFBS

With a moderate cost, Wand *et al.* [88] where able to introduce an ID-based Fair Blind Signature. Moreover, it has two additional properties: enabling proxy signature and weak linkability. The drawbacks consist in a relatively long signature (1028 bits) and 4 communications to obtain the signature. Note that the weak linkability property could also be considered as a weakness of the scheme. Latter, an alternative was proposed by Verma *et al.* [83]. The scheme relies on a Fiat-Shamir signature and is based on oblivious transfer, which is known to be a relatively expensive primitives. Hence, the scheme has a low efficiency and needs many communications. We are not providing a complexity analysis of the latest as one willing to put such a signature in practice may not consider it due to its deficiency of proven security. The authors want to highlight that none of the schemes have been proven secure. In [88], discussion of the security of the scheme is provided, but no attention is given to unforgeability. Security proofs are almost mandatory in today's development of cryptography and here no model has

Ref		Pair	ECMul	ECAdd	Exp	Mul	Add	Inv	Hash	PHash	Total	Size
[16]	$\mathcal{U}$			4	2			2		1	8.43	2
	$\mathcal{S}$			4	2			1			4.14	
	$\mathcal{V}$	1	4						3		104.87	
	T	1	4	8	4	0	0	3	3	1	117.45	
[18]	$\mathcal{U}$		6	2		2	1	1	1	1	23.88	3
	$\mathcal{S}$		4				1			1	16.03	
	$\mathcal{V}$	3	1	1					1	1	277.38	
	T	3	11	3	0	2	2	1	2	3	317.30	
[19]*	$\mathcal{U}$		6	3		1	1	1	1	1	23.97	3
	$\mathcal{S}$		4	1			1			1	16.20	
	$\mathcal{V}$	3	1	1					1	1	277.38	
	T	3	11	5	0	1	2	1	2	3	317.55	
[58]	$\mathcal{U}$		4	2|m|+2|info|+8					2		188.03	3
	$\mathcal{S}$		2	|m|+1							47.12	
	$\mathcal{V}$	4		|ID|+|m|+|info|+4					3		492.16	
	T	4	6	3|m|+3|info|+|ID|+13	0	0	0	0	0	0	727.32	
[39]	$\mathcal{U}$	4	10	6	1	6	1		3		395.16	3
	$\mathcal{S}$	1	4	1		1					101.96	
	$\mathcal{V}$	3			2	4		2	2		275.36	
	T	8	14	7	3	11	1	2	5	0	772.50	
[89]	$\mathcal{U}$	7	3	4	2	10		1	2		644.11	4
	$\mathcal{S}$		3	1	1	1			1		11.88	
	$\mathcal{V}$	2	2			3			1		186.73	
	T	9	8	5	3	14	0	1	4	0	842.73	
[90]*	$\mathcal{U}$	4	8	5	2	6	1		3		390.58	3
	$\mathcal{S}$	2	5	1		2	1		1		195.86	
	$\mathcal{V}$	3			2	1		2	2		275.12	
	T	9	13	6	4	9	2	2	6	0	861.57	
[17]*	$\mathcal{U}$	8	3	10	5	10	1	1	1	1	742.58	6
	$\mathcal{S}$		3	5	2		1				13.05	
	$\mathcal{V}$	2	6	1	1	2			1	1	204.39	
	T	10	12	16	8	12	2	1	2	2	960.04	
[18]*	$\mathcal{U}$	3	10	5	8	12	1	2	1	1	319.34	6
	$\mathcal{S}$	3	5	2			1			1	288.53	
	$\mathcal{V}$	6	1	1	2	2			1	1	549.87	
	T	12	16	8	10	14	2	2	2	3	1157.76	

Table 13: Analysis of Signature Issuing of IDPBS Scheme Using Pairing.
(*Scheme With Restrictiveness)

Ref	Year	Mathematical base	Security reduction	Interactions	Blinding factor
Message Recovery					
[52]	2019	Elliptic curve	ECDL	3	4
[34]	2005	Pairing	ECDL	3	2
[84]	2018		k-CAA		
[20]	2018		Q-SDH		
[24]	2008		CDH		
[47]	2017		Not formal	3	2
Fairness					
[88]	2012	Pairing	No reduction	4	2
[83]	2016			2 with Oblivious Transfer	$2\kappa + 1$
Forward-Security					
[100]	2016	Lattice	SIS	3	2
Batch Verification					
[60]	2006	Pairing	k-CAA	2	2

Table 14: IDBS with properties.

ever been proposed for these schemes. Despite the real practicality provided by fairness, none of the scheme would be considered as reliable enough. We conclude that some work remains to do to propose to the community an efficient and secure IDFBS. We propose a security model for IDFBS in Appendix B.

ID-based Forward-Secure Blind Signature - IDFSBS

Forwards security is gradually becoming a central property in cryptography. In the context of signature scheme is allows to divide the lifetime of a key pair into N periods. The secret key is modified for each period while keeping the same public key, thus providing additional security as on leakage of a secret key, previous signature are no longer affected by this security breach. Thus, signatures made during the $N - 1$ others are still reliable. This increase the global security of signatures.

IDFSBS are not possible to compare since the authors of [100] were the only one to propose such a signature. It relies on the well-studied SIS problem over lattices and requires 3 communications and 2 blinding factor. The signature is composed of one vector of size m (the message) with elements in $\mathbb{Z}_q$. Lattice based signatures known to produce relatively long outputs which is a drawback compensated by the absence of known algorithm to be efficient against them even on quantum computers.

We list all operations needed to proceed to the signature in Table 5 and let the reader directly refer to [100] for a more in-depth complexity comparison of this scheme where three other lattice based signatures (not blind or ID-based) are compare to that one.

ID-based Blind Signature with Batch Verification - IDBSBV

Batch verification allows faster signature verification. For signatures with batch verification it is possible to specify an algorithm verifying multiples instance in the same time and significantly faster than the normal verification.

We have observed only one such scheme by Li *et al.* [60]. The scheme is efficient, still relying on pairing function known to be costly. They proposed an efficient signature process leading a relatively short signature with fast verification. Note also that the scheme has a costly verification process, based on pairing. The batch verification allows to drastically reduce the need of pairing function for the verification and thus gives scheme that is comparable to the best pairing free algorithm of the literature.

Message Recovery												
Ref		EXP	PAIR	ECMUL	ECADD	MUL	ADD	INV	H	PH	Total	Size
[52]	$\mathcal{U}$			7	6	10	5	2	4	2 gcd	29.11	2
	$\mathcal{S}$			2		2	2				6.25	
	$\mathcal{V}$			2	1				4		10.37	
	T	0	0	11	7	12	7	2	8		45.74	
[20]	$\mathcal{U}$	2		1		3	1	1	3		9.91	2
	$\mathcal{S}$	1		1			1				4.62	
	$\mathcal{V}$	1	1	1	1	1			4		98.76	
	T	4	1	3	1	4	2	1	7		113.30	
[24]	$\mathcal{U}$		1	4	2	2		1			102.52	2
	$\mathcal{S}$			2	1						6.16	
	$\mathcal{V}$	1	2			1		1			181.41	
	T	1	3	6	3	3	0	2	0		290.09	
[84]	$\mathcal{U}$		1	3	1	1	1	1	3		102.47	2
	$\mathcal{S}$			2			1		1		7.09	
	$\mathcal{V}$	1	2		1						181.19	
	T	1	3	5	2	1	2	1	4		290.76	
[34]	$\mathcal{U}$		1	3	3		1				99.27	2
	$\mathcal{S}$			3	1						9.16	
	$\mathcal{V}$	1	3			2		1			271.21	
	T	1	4	6	4	2	1	1	0		379.65	

Ref		EXP	PAIR	ECMUL	ECADD	MUL	ADD	INV	H	PH	Total	Size
[26]	$\mathcal{U}$		4	2	2				1		366.27	1
	$\mathcal{S}$			1					1		4.05	
	$\mathcal{V}$		2						1		180.49	
	T		6	3	2	0	0	0	3		550.82	

Table 15: Evaluation of IDBS Schemes with properties.

4.5 Comparison to the Generic Construction

Generic construction of IDBS have been introduced by D. Galindo *et al.* [26]. It gives a generic framework based on a signature scheme $\mathcal{S} = (KG_{\mathcal{S}}, SGN_{\mathcal{S}}, VFY_{\mathcal{S}})$ and a blind signature scheme $\mathcal{BS} = (\mathsf{KG}_{\mathcal{BS}}, \mathsf{SGN}^{com}_{\mathcal{BS}}, \mathsf{SGN}^{blind}_{\mathcal{BS}}, \mathsf{SGN}^{sgn}_{\mathcal{BS}}, \mathsf{SGN}^{unb}_{\mathcal{BS}}, \mathsf{VFY}_{\mathcal{BS}})$. Combining these two structures we can construct a IDBS scheme. In order to accomplish their roles the three entities (user, signer, verifier) have to execute the following algorithm to output and verify a signature: User: $VFY_{\mathcal{S}}, \mathsf{SGN}^{blind}_{\mathcal{BS}}, \mathsf{SGN}^{unb}_{\mathcal{BS}}$; Signer: $\mathsf{SGN}^{com}_{\mathcal{BS}}, \mathsf{SGN}^{sgn}_{\mathcal{BS}}$; Verifier: $VFY_{\mathcal{S}}, \mathsf{VFY}_{\mathcal{BS}}$.

The authors of [26] proposed an instantiation for their ID-based blind signature construction based on two schemes: the Boneh-Lynn-Shacham (BLS) signature [11] and Boldyreva's blind signature [9]. At the time D. Galindo *et al.* idea was published, they claimed to be among the most efficient schemes.

Here we compare the cost of this scheme to the one of the previous IDBS (see Table 15). The observed complexity is mostly due to the use of pairing function in the signature scheme. Based on our reduction, we can deduce that the total complexity of the generated scheme is barely the addition of the cost of both schemes and is around the average of the observed complexity for the existing IDBS schemes. Relying on secure pairing free schemes would lead to a secure IDBS with improved complexity.

A more recently study [12] introduced a new generic construction for IDPBS. As the in the previous construction, they rely on a signature and a blind signature. They are organised in a manner reaching an acceptable complexity as explained in the article, with approximately the same complexity as the previous construction.

5 Synthesis of the Current Literature

There exists an extensive literature on IDBS, numerous schemes have been presented by multiple authors. In total 71 schemes are presented in this survey. We noticed that the literature is mostly independent and that no global courses of action was followed by the authors of these schemes. Only few works mostly based on lattices were following previous work due to some attacks found on them: the latest schemes were made to fix some security breach in the existing work. This survey aims at putting some coherence in future work in the field, it brings up formalism for security assumption based on the existing security expectation for each of the properties. In here we have tried to resolve this issue, and we are proposing some formalisation of the security games in Appendix B. The given experiments are a formalisation of the expected security of each IDBS in the context where it is put by the associated properties. Even if these experiments needs further discussion before being fully adopted by the community, we believe it as a step forward in the study of the security of these primitives.

This is motivated by the fact than no security proofs or formal arguments have been disclosed for 22 of the investigated schemes. It implies that it may remain unknown vulnerabilities for existing schemes and possible attacks might be found in the future. We do not recommend using any unproven schemes for practical purposes. Also, some authors provided a reduction for their scheme. Yet, the security may not be ensured as their assumption are weak *e.g.,* IDBS rely on quite unusual hypothesis and some other

Scheme	Pairing	Other	Scheme	Pairing	Other
IDBS	24	8	IDFBS	2	0
IDPBS	9	6	IDFSBS	0	1
IDPrBS	12	2	IDBSBV	1	0
IDBSMR	5	1	Total	53	18

Table 16: Number of Schemes for each Property Based on their use of Pairing.

schemes rely on the broken ROS problem. The latter should no longer be used as they do not bring any security to their users.

While exploring the literature, we noticed that it lacks pairing free IDFBS, IDFSBS or IDBSBV schemes. Further studies could potentially improve efficiency and quantum resistance of such primitives. No pairing free IDFBS or IDBSBV yet exists and no post quantum assumption was ever used to design an IDPBS, IDPrBS, IDBSMR, IDFBS or IDBSBV that withdraw proven security until today. A big step forward on the development of new schemes on post quantum assumptions is necessary to guarantee the future of these primitives. A list of all existing schemes for each of the existing properties and based on pairing or not is givent in Table 16.

On another hand, minimising the number of transmission to obtain round optimal IDBS is also of interest for the field as it bring a non-negligible speedup as most construction archives a computational cost comparable of to the order of magnitude of a Round Trip Time. For example, no round optimal IDBSMR have ever been introduced, combined with this type of primitive that seems to achieve efficient computational time would be of interest.

As highlighted in [96], numerous schemes had issues while being performed in parallel execution due. This is mostly due to a polynomial time algorithm capable of solving the ROS problem [8]. Other studies could focus on bringing an IDBS with proven security under parallel execution.

We see that some works is still to be done in this domain to guarantee the future security and the practicality of the IDBS and other signature schemes evoked in this paper.

6 Conclusion

In this survey we review the literature on ID-based blind signature with several existed properties presented throughout this paper. We show that depending on the case of use, there exist several IDBS schemes to consider. The studied schemes have specific properties and their efficiency relies on manifold requirements. In this survey we answer the question: how to choose an IDBS scheme? For that we have listed all existing IDBS schemes, we present them all with their most notable properties and a reproducible, bias free evaluation of their complexity. Providing a time reduction of all arithmetical operations used for IDBS schemes in order to evaluate them all at the same security level is our first contribution. We directly exploit it to give a metric on the complexity of any these scheme. With this metric we can compute the total computational cost of a signature issuing and verification process. Hence, it is easy to compare their efficiencies.

We can conclude from thanks to our study that the most computationally efficient IDBS scheme using EC is [54]. But schemes can be chosen from other kind of feature

such as number of communications, number of blinding factors or the size of the signature. We enable anybody to quickly choose from the existing literature the best feted properties and signature for its use based on their characteristics. We also give new insights by proposing formal security experiment and open axes of research for these primitives.

References

1. MPHELL: Multi-Precision (Hyper) Elliptic curve Library, 2020.
2. Openssl library, 2021.
3. M. Abe and E. Fujisaki. How to date blind signatures. In *Advances in Cryptology — ASIACRYPT '96*. Springer, 1996.
4. K. A. Ajmath, P. V. Reddy, T. Gowri, and buprasad. An id-based blind signature scheme from bilinear pairings. 2010.
5. M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC, 1996.
6. N. Asghar. A survey on blind digital signatures. 2015.
7. M. Bellare, J. A. Garay, and T. Rabin. Fast batch verification for modular exponentiation and digital signatures. In *EUROCRYPT*, 1998.
8. F. Benhamouda, T. Lepoint, J. Loss, M. Orrù, and M. Raykova. On the (in)security of ros. Cryptology ePrint Archive, Report 2020/945, 2020.
9. A. Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography*, PKC. Springer, 2003.
10. A. Boldyreva, A. Palacio, and B. Warinschi. Secure proxy signature schemes for delegation of signing rights. *J. Cryptol.*, Jan. 2012.
11. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In *Advances in Cryptology — ASIACRYPT 2001*. Springer, 2001.
12. X. Bultel, P. Lafourcade, C. Olivier-Anclin, and L. Robert. Generic construction for identity-based proxy blind signature. In *The 14th International Symposium on Foundations and Practice of Security, FPS*, 2021.
13. J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler. Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology — EUROCRYPT'94*. Springer, 1995.
14. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of CRYPTO '82*. Plenum, 1982.
15. D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Advances in Cryptology — CRYPTO' 88*. Springer, 1990.
16. W. Chen, B. Qin, Q. Wu, L. Zhang, and H. Zhang. Id-based partially blind signatures: A scalable solution to multi-bank e-cash. In *International Conference on Signal Processing Systems*, 2009.
17. X. Chen, F. Zhang, and S. Liu. Id-based restrictive partially blind signatures. In *International Conference on Computational and Information Science*. Springer, 2005.
18. X. Chen, F. Zhang, and S. Liu. Id-based restrictive partially blind signatures and applications. *Journal of Systems and Software*, 2007.
19. S. S. M. Chow, L. C. K. Hui, S. M. Yiu, and K. P. Chow. Two improved partially blind signature schemes from bilinear pairings. In *Proceedings of the 10th Australasian Conference on Information Security and Privacy*, ACISP'05. Springer, 2005.
20. W. Cui and Q. Jia. Efficient provably secure id-based blind signature with message recovery. In *4th Workshop on Advanced Research and Technology in Industry (WARTIA 2018)*. Atlantis Press, 2018.
21. W. Cui and Q. Jia. Provably secure pairing-free identity-based restrictive partially blind signature scheme. In *Information Technology, Networking, Electronic and Automation Control Conference*. IEEE, 2019.
22. L. Deng, X. He, and T. Xia. Secure identity-based blind signature scheme for online transactions. *Wireless Personal Communications*, 2021.
23. ECRYPT-CSA. Algorithms, Key Size and Protocols Report. Technical report, 2018.
24. H. M. Elkamchouchi and Y. Abouelseoud. A new blind identity-based signature scheme with message recovery. *IACR Cryptol. ePrint Arch.*, 2008.
25. G. Fuchsbauer and D. Vergnaud. Fair blind signatures without random oracles. Cryptology ePrint Archive, Report 2010/101, 2010.
26. D. Galindo, J. Herranz, and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In *Advances in Cryptology – ASIACRYPT*. Springer, 2006.
27. W. Gao, Y. Hu, B. Wang, and J. Xie. Identity-based blind signature from lattices in standard model. In *International Conference on Information Security and Cryptology*. Springer, 2016.
28. W. Gao, Y. Hu, B. Wang, J. Xie, and M. Liu. Identity-based blind signature from lattices. *Wuhan University Journal of Natural Sciences*, 2017.
29. W. Gao, G. Wang, X. Wang, and F. Li. One-round id-based blind signature scheme without ros assumption. In *International Conference on Pairing-Based Cryptography*. Springer, 2008.

30. W. Gao, G. Wang, X. Wang, and F. Li. Round-optimal id-based blind signature schemes without ros assumption. *Journal of Communications*, 2012.
31. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC, 2008.
32. Girish, Krupa, and D. Phaneendra. Survey on identity based blind. 2015.
33. T. Granlund. GNU MP: The GNU Multiple Precision Arithmetic Library, 2020.
34. S. Han and E. Chang. A pairing-based blind signature scheme with message recovery. *International Journal of Information Technology*, 2005.
35. D. He, J. Chen, and R. Zhang. An efficient identity-based blind signature scheme without bilinear pairings. *Computers & Electrical Engineering*, 2011.
36. J. He, C. Qi, and F. Sun. A new identity-based proxy blind signature scheme. In *IEEE International Conference on Information Science and Technology*. IEEE, 2012.
37. P. Heng, K. Ke, and C. Gu. Efficienct id-based proxy blind signature schemes from pairings. In *International Conference on Computational Intelligence and Security*. IEEE, 2008.
38. X. Hu and S. Huang. An efficient id-based partially blind signature scheme. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD)*. IEEE, 2007.
39. X. Hu and S. Huang. An efficient id-based restrictive partially blind signature scheme. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD)*, 2007.
40. X. Hu, J. Wang, and Y. Yang. Secure id-based blind signature scheme without random oracle. In *International Conference on Network Computing and Information Security*. IEEE, 2011.
41. X.-M. Hu and S.-T. Huang. Secure identity-based blind signature scheme in the standard model. *J. Inf. Sci. Eng.*, 2010.
42. Z. Huang, K. Chen, and Y. Wang. Efficient identity-based signatures and blind signatures. In *International Conference on Cryptology and Network Security (CANS)*. Springer, 2005.
43. Z. Huang, Q. Chen, R. Huang, and X. Lin. Efficient schnorr type identity-based blind signatures from bilinear pairings. In *WRI World Congress on Computer Science and Information Engineering*. IEEE, 2009.
44. S. Ibrahim, M. Kamat, M. Salleh, and S. Aziz. Secure e-voting with blind signature. In *4th National Conference of Telecommunication Technology*, 2003.
45. S. H. Islam, R. Amin, G. Biswas, M. S. Obaidat, and M. K. Khan. Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. *Arabian Journal for Science and Engineering*, 2016.
46. R. Jain and A. A. Patel. Computationally efficient id-based blind signature scheme in e-voting. *International Journal for Scientific Research and Development*, 2013.
47. S. James, T. Gowri, G. Babu, and P. V. Reddy. Identity-based blind signature scheme with message recovery. *International Journal of Electrical & Computer Engineering*, 2017.
48. S. James, G. Thumbur, and P. Reddy. An efficient pairing-free identity based proxy blind signature scheme with message recovery. *The ISC International Journal of Information Security*, 2021.
49. S. Kalkan, K. Kaya, and A. A. Selcuk. Generalized id-based blind signatures from bilinear pairings. In *International Symposium on Computer and Information Sciences*. IEEE, 2008.
50. M. M. Khater, A. Al-Ahwal, M. M. Selim, and H. H. Zayed. Blind signature schemes based on elgamal signature for electronic voting: A survey. *International Journal of Computer Applications*, 2018.
51. M. Kucharczyk. Blind signatures in electronic voting systems. In *Computer Networks*. Springer, 2010.
52. M. Kumar and S. Chand. A pairing-less identity-based blind signature with message recovery scheme for cloud-assisted services. In *International conference on information security and cryptology*. Springer, 2019.
53. M. Kumar, C. Katti, and P. Saxena. An identity-based blind signature approach for e-voting system. *International Journal of Modern Education and Computer Science*, 2017.
54. M. Kumar, C. Katti, and P. Saxena. An untraceable identity-based blind signature scheme without pairing for e-cash payment system. In *International Conference on Ubiquitous Communications and Network Computing*. Springer, 2017.
55. M. Kumar, C. P. Katti, and P. C. Saxena. A secure anonymous e-voting system using identity-based blind signature scheme. In *International conference on information systems security*. Springer, 2017.
56. W. Lang, Y. Tan, Z. Yang, G. Liu, and B. Peng. A new efficient id-based proxy blind signature scheme. In *Ninth International Symposium on Computers And Communications*. IEEE, 2004.
57. A. K. Lenstra and E. R. Verheul. The xtr public key system. In *Annual International Cryptology Conference*. Springer, 2000.

58. F. Li, M. Zhang, and T. Takagi. Identity-based partially blind signature in the standard model for electronic cash. *Mathematical and Computer Modelling*, 2013.
59. Q. Li, C. Hsu, D. He, K.-K. R. Choo, and P. Gong. An identity-based blind signature scheme using lattice with provable security. *Mathematical Problems in Engineering*, 2020.
60. R. Li, J. Yu, G. Li, and D. Li. A new identity-based blind signature scheme with batch verifications. In *International Conference on Multimedia and Ubiquitous Engineering*. IEEE, 2007.
61. B. Lynn. PBC library: The Pairing-Based Cryptography Library, 2021.
62. M. Nikooghadam and A. Zakerolhosseini. An efficient blind signature scheme based on the elliptic curve discrete logarithm problem. *ISC Int. J. Inf. Secur.*, 2009.
63. K. Nyberg and R. A. Rueppel. A new signature scheme based on the dsa giving message recovery. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS, 1993.
64. S. Padhye and N. Tiwari. An efficient id-based proxy blind signature with pairing-free realization. In *International conference on Innovative Engineering Technologies*, 2016.
65. L. T. Phong and W. Ogata. New identity-based blind signature and blind decryption scheme in the standard model. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 2009.
66. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptol.*, Jan. 2000.
67. S. Prabhadevi and A. Natarajan. Utilization of id-based proxy blind signature based on ecdlp in secure vehicular communications. *International Journal of Engineering and Innovative Technolog*, 2013.
68. S. Rawal and S. Padhye. Cryptanalysis of id based proxy-blind signature scheme over lattice. *ICT Express*, 2020.
69. P. Sarde and A. Banerjee. A secure id-based blind and proxy blind signature scheme from bilinear pairings. *Journal of Applied Security Research*, 2017.
70. C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In *Information and Communications Security*. Springer, 2001.
71. R. Shakerian, T. MohammadPour, S. H. Kamali, and M. Hedayati. An identity based public key cryptography blind signature scheme from bilinear pairings. In *International Conference on Computer Science and Information Technology*. IEEE, 2010.
72. A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology*. Springer, 1985.
73. W. Shuang, Y. Hao, and L. Dongnan. A new identity based blind signature scheme and its application. In *Advanced Information Technology, Electronic and Automation Control Conference*. IEEE, 2018.
74. S. Singh and S. Padhye. Identity based blind signature scheme over ntru lattices. *Information Processing Letters*, 2020.
75. M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1995.
76. M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In *Advances in Cryptology — EUROCRYPT '95*. Springer, 1995.
77. N. Tahat and E. Abdallah. Hybrid publicly verifiable authenticated encryption scheme based on chaotic maps and factoring problems. *Journal of Applied Security Research*, 2018.
78. N. Tahat, A. A. Tahat, R. B. Albadarneh, and T. A. Edwan. Design of identity-based blind signature scheme upon chaotic maps. *International Journal of Online & Biomedical Engineering*, 2020.
79. Z. Tan. Efficient pairing-free provably secure identity-based proxy blind signature scheme. *Security and Communication Networks*, 2013.
80. Q. Tang and F. Shen. Identity-based xtr blind signature scheme. *Intelligent Automation & Soft Computing*, 2013.
81. A. A. Thu and K. T. Mya. Implementation of an efficient blind signature scheme. *International journal of innovation, management and technology*, 2014.
82. X.-X. Tian, H.-J. Li, J.-P. Xu, and Y. Wang. A security enforcement id-based partially blind signature scheme. In *International conference on web information systems and mining*. IEEE, 2009.
83. G. K. Verma and B. Singh. New id-based fair blind signatures. *Futuristic Trends in Engineering, Science, Humanities, and Technology FTESHT-16*, 2016.
84. G. K. Verma and B. Singh. Efficient identity-based blind message recovery signature scheme from pairings. *IET Information Security*, 2018.
85. S. Von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers & Security*, 1992.
86. B. Wang, W. Liu, and C. Wang. ID-based proxy blind signature scheme with proxy revocation. In *International Workshop on Computer Science and Engineering, WCSE*, 2009.
87. C. Wang and R. Lu. An id-based transferable off-line e-cash system with revokable anonymity. In *International Symposium on Electronic Commerce and Security*, 2008.

88. C. H. Wang and J.-Y. Fan. The design of id-based fair proxy blind signature scheme with weak linkability. In *International Conference on Information Security and Intelligent Control*, 2012.
89. C.-J. Wang, Y. Tang, and Q. Li. Id-based fair off-line electronic cash system with multiple banks. *Journal of computer science and technology*, 2007.
90. S. Wang, P. Han, Y. Zhang, and X. Wang. An improved id-based restrictive partially blind signature scheme. In *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*. IEEE, 2008.
91. 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*, 2005.
92. G. Xu and G. Xu. An id-based blind signature from bilinear pairing with unlinkability. In *International Conference on Consumer Electronics, Communications and Networks*. IEEE, 2013.
93. M. Yang and Y. Wang. A new efficient id-based proxy blind signature scheme. *Journal of electronics*, 2008.
94. 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*. Springer, 2008.
95. F. Zhang and K. Kim. Id-based blind signature and ring signature from pairings. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2002.
96. F. Zhang and K. Kim. Id-based blind signature and ring signature from pairings. In *Advances in Cryptology — ASIACRYPT 2002*. Springer, 2002.
97. F. Zhang and K. Kim. Efficient id-based blind signature and proxy signature from bilinear pairings. In *Australasian Conference on Information Security and Privacy*. Springer, 2003.
98. L. Zhang, Y. Hu, X. Tian, and Y. Yang. Novel identity-based blind signature for electronic voting system. In *Second International Workshop on Education Technology and Computer Science*. IEEE, 2010.
99. L. Zhang and Y. Ma. A lattice-based identity-based proxy blind signature scheme in the standard model. *Mathematical Problems in Engineering*, 2014.
100. Y. Zhang and Y. Hu. Forward-secure identity-based shorter blind signature from lattices. *American Journal of Networks and Communications*, 2016.
101. B. Zhao and S. Yang. Anonymous identity-based blind signature in the performance evaluation. In *International Conference on Mechatronics, Control and Electronic Engineering*. Atlantis Press, 2014.
102. Z.-m. Zhao. Id-based weak blind signature from bilinear pairings. *IJ Network Security*, 2008.
103. 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.

A Security Assumptions

In this section we give the definitions of the security assumptions mentioned above. We start with the most usual ones and follows through with the least known ones. Then we formalise the security assumptions based on lattices.

Definition 2 (DL - Discrete Logarithm). *Given two group elements g and h in a group $\mathbb{G}$, find an integer n, such that $h = g^n$ whenever such an integer exists.*

On an elliptic curve it is possible to reformulate this problem in an additive manner. This gives rise to the ECDL hypothesis. Here the objective is to find an GT45element n such that $H = n \cdot G$ for a generator G and a random element H. Many other variants of these problems are also known to be hard. The most classical ones are all present here.

Definition 3 (DDH - Decision Diffie-Hellman). *Given $a, b, c \in \mathbb{Z}_q$ and $g \in \mathbb{G}$ a generator of a group of order q, knowing (g, g^a, g^b, g^c), check if $a = bc$.*

Definition 4 (CDH - Computational Diffie-Hellman). *Given two integers $a, b \in \mathbb{Z}_q$ and a group element $g \in \mathbb{G}$ knowing (g, g^a, g^b), compute g^{ab}.*

Definition 5 (GDH - Gap Diffie-Hellman). *DDH problem is easy while CDH is hard.*

Definition 6 (q-SDH - q-Strong Diffie-Hellman). *Consider P and Q respective generators of the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p. Given a $q+2$-tuple $(P, Q, aQ, a^2Q, \ldots, a^qQ)$. Find a pair $(c, \frac{1}{c+a}P)$ with $c \in \mathbb{Z}_p^*$.*

Definition 7 (k-CAA - Collusion Attack Algorithm with k traitors). *Let $\mathbb{G}$ a cyclic group generated by P. For a know $k \in \mathbb{Z}$ product of two integers n and m and an unknown $s \in \mathbb{Z}_q^*$. Given a tuple $\{f_1, \ldots, f_m, g_1, \ldots, g_n\} \subset \mathbb{Z}$ and $\{sP, \frac{f_1}{s+g_1}P, \frac{f_2}{s+g_1}P, \ldots, \frac{f_1}{s+g_2}P, \ldots, \frac{f_n}{s+g_m}P\} \subset \mathbb{G}$. For $f, g \in \mathbb{Z}_q^*$ such that $f \notin (f_1, \ldots, f_m)$, $g \notin (g_1, \ldots, g_n)$, compute $\frac{f}{s+g}P$.*

Let $\mathbb{G}$ be a multiplicative group with a pairing function (a bilinear, non-degenerated map) $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive groups. These maps should be computationally fast. They are usually produced on specific elliptic curves, two of the most know ones are the Weil Pairing and the Tate Pairing. We only assume their existence and won't go into more details.

Definition 8 (k-BDHI - k-Bilinear Diffie-Hellman Inversion [37]). *Given $(P, aP, a^2P, \ldots, a^kP) \in (\mathbb{G}^*)^{k+1}$, output $e(P,P)^{a^{-1}}$*

Definition 9 (1m-BDHI - One-more Bilinear Diffie-Hellman Inversion). *Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of prime order q and P be a generator of $\mathbb{G}_1$. Let $x, y \in \mathbb{Z}_q$ two randomly chosen elements and let $X = xP$, $Y = yP$. Given $(e, \mathbb{G}_1, \mathbb{G}_2, q, P, X, Y)$ and access to oracles:*

- *The Target Oracle $\mathcal{TO}$ returns a random point from $\mathbb{G}_1$ when it is invoked.*
- *The Helper Oracle $\mathcal{HO}$ given $Z \in \mathbb{G}_1$, returns random $S, T \in \mathbb{G}_1$ such that $e(S,T) = e(Y,Z)^x$. Additionally, it also returns R satisfying $e(R,S) = e(X,Y)$ and $e(R,Z) = e(P,T)$.*

The objective is to output a sequence of points $S_1, T_1, \cdots, S_n, T_n \in \mathbb{G}_1$ satisfying $e(S_1,T_1) = e(xyP, Z_1)^x, \ldots, e(S_n,T_n) = e(xyP, Z_n)^x$, where all different $Z_1, \ldots, Z_n$ are random points returned by $\mathcal{TO}$ and the number of queries that were made to $\mathcal{HO}$ is strictly less than n.

One important hypothesis in the field of blind signature is the ROS problem. It plays a crucial role as many schemes rely on it for some specific case of use (multi-session issuing process). In 2019, Benhamouda *et al.* [8] found a PT algorithm solving the ROS problem. The attack is practical. Many schemes have been affected via parallel attacks [66] (*i.e.,* when one can open multiple session at the same time to conduct its attacks).

Definition 10 (ROS - Overdetermined Solvable System of Linear Equations modulo q with Random inhomogeneity [70]). *Given a random oracle function $F\colon \mathbb{Z}_q^l \to \mathbb{Z}_q$, find coefficients $a_{k,i} \in \mathbb{Z}_q$ and a solvable system of $l+1$ distinct equations of the following form in the unknowns $c_1, c_2, \cdots, c_l$ over $\mathbb{Z}_q$, $a_{k,1}c_1 + \cdots + a_{k,l}c_l = F(a_{k,1}, \cdots, a_{k,l})$.*

Definition 11 (CT-ACDH - Chosen Target Accompanied Computational Diffie-Hellman [16]). *Let $\mathbb{G}$ be a cyclic group of prime order p. Let $(g, g^x, g^y, g^\alpha, g^\beta) \in \mathbb{G}^5$. The adversary $\mathcal{A}$ is allowed to access two oracles:*

- *Target Oracle $\mathcal{O}_T$, which randomly samples a random element $g^{\gamma_i} \in \mathbb{G}$ whenever it is invoked for the i^{th} time.*
- *Helper Oracle $\mathcal{O}_H$, which takes input $(c, M) \in \mathbb{Z}_p \times \mathbb{G}$, outputs $((g^{\alpha x + c\beta y} M)^z, g^z, g^{\frac{1}{z}}) \in \mathbb{G}^3$.*

The adversary $\mathcal{A}$ wins if it outputs a string c' and $k+1$ tuples $(g^{a_1}, g^{b_1}), \ldots, (g^{a_{k+1}}, g^{b_{k+1}})$ such that $a_j b_j = \gamma_{\pi(j)} + \alpha x + c\beta y$, where $\pi(\cdot)$ is a permutation on $\{1, \ldots, q_T\}$, q_T is the number of queries to $\mathcal{O}_T$ and the adversary $\mathcal{A}$ queries the helper oracle $\mathcal{O}_H$ with c' at most k times.

With the recent rise of quantum computers, most classical assumptions would not be reliable if such a machine was produced. Lately some new, known hard problems have been extensively studied. Among them lattice based problems have been trusted to provide high security and to lead to relatively efficient schemes. A *lattice* is an infinite discrete structure generated by a finite set of vectors called *basis* $(b_0, \ldots, b_{n-1})$. It is the set of all linear integer combinations of n (with $n \leq m$) linearly independent basis vectors $\{b_j\} \subset \mathbb{R}^m$, namely, $\mathcal{L} = \{\sum_j z_j b_j | z_j \in \mathbb{Z}\}$. In the context of a lattice $\mathcal{L}$, λ_i will be the i[th] minimum of $\mathcal{L}$, $\lambda_i(\mathcal{L}) = inf\{r > 0 | dim(Span(\mathcal{L} \cap B_m(0, r))) > i\}$.

Definition 12 (SIS - Short Integer Solution). *Given $A \in \mathbb{Z}_q^{n \times m}$ chosen from the uniform distribution, the SIS is to find $\boldsymbol{z} = (z_1, \ldots, z_m)^t \in \mathbb{Z}^m$ such that $A \cdot \boldsymbol{z} = 0 \ mod \ q$ and $0 < \|\boldsymbol{z}\| < \beta$, with $\|\cdot\|$ the Euclidean norm.*

Let $\Phi(X)$ be a monic irreducible polynomial of degree n. We used the 2n[th] cyclotomic polynomial $\Phi(X) = X^n + 1$ with $n = 2^s$ for some positive integer s. Define R as the ring $\mathbb{Z}[X]/\langle \Phi(X) \rangle$. Let q be the positive integer and define $R_q = R/qR$. For each $z = z(X) = \sum_{i=0}^{n-1} c_i X^i \in R$, for $c_i \in \mathbb{Z}$ we can define the norm $\|z\| = (\sum_{i=0}^{n-1} c_i^2)^{1/2}$. Similarly, for each $\mathbf{z} = (z_1, \ldots, z_m)^t \in R^d$, where each $z_i = \sum_{i=0}^{n-1} c_{ij} X^j \in R$, we define $\|\mathbf{z}\| = (\sum_{i=0}^{d} \sum_{j=0}^{n-1} c_{ij}^2)^{1/2}$.

Definition 13 (R-SIS - Ring Short Integer Solution [5]). *The problem R-SIS$_{q,m,\beta}$ is defined as follows: Given $a_1, \ldots, a_m \in R_q$ chosen independently at uniform, the R-SIS is to find $z_1, \ldots, z_m \in R$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \ mod \ q$ and $0 < \|\boldsymbol{z}\| < \beta$ where $\boldsymbol{z} = (z_1, \ldots, z_m)^t \in R^m$.*

Definition 14 (SV - Shortest Vector). *Let n and m be positive integers. Given a basis $(b_0, \ldots, b_{n-1})$ of a lattice $\mathcal{L} \subset \mathbb{R}^m$ that verifies $\lambda_2(\mathcal{L}) > \lambda_1(\mathcal{L})$. Find a vector $v \in \mathcal{L}$ such that $\|v\| = \lambda_1(\mathcal{L})$.*

One last problem is the Chebyshev polynomial computation problem. For that problem the reader can refer to [78]. This problem even it has not been extensively studied in the literature is known to have a reduction to the discrete logarithm in a finite group $GF(p)$, for some primer p [77].

B Security Games

This section presents the security experiments formalising the security of the studied primitives. As for some studied primitives no security games have ever been introduced, we have tried to formalise the expected security it should withstand when confronted to an adversary. Some properties can easily be derived from existing work, we specify it when this is the case. We consider two probabilistic polynomial-time algorithm $\mathcal{A}$(the adversary) and $\mathcal{C}$ (the challenger) depending on a security parameter $\mathfrak{K}$. $\mathcal{A}$ tires to solve a the below experiment $\mathsf{Exp}^{\cdot}_{\cdot}$ when $\mathcal{C}$ simulate it.

The security for schemes with batch verification or message recovery directly falls within the experiments liked to IDBS scheme. So does unforgeability and blindness of a IDPBS when one considers $m = m'||\mathsf{info}$. To avoid redundancy the games are only specified once.

Identity-based Blind Signature. Let us now start with the basic IDBS schemes, its definition has been given in definition 1. Hence, only the security properties are given in this section.

- *Correctness.* For an algorithm A, $[A]$ will denote the set of the possibles outcomes. This expression must be fulfilled to achieve correctness: $\forall m \in M, \forall (msk, mpk) \in [\mathsf{Setup}()], \forall ID \in \{0,1\}^*, sk[ID] \in [\mathsf{Extract}(msk, ID)], \forall \sigma \in [\langle \mathcal{S}(sk[ID]), \mathcal{U}(ID, m)\rangle], \mathsf{Verif}(mpk, ID, m, \sigma) = 1$.
- *Unforgeability.* An adversary $\mathcal{U}^*$ against the unforgeability tries to generate $q_s + 1$ valid signature after at most q_s complete interaction with the honest signer $\mathcal{S}$ with identity $ID_{\mathcal{S}}$. He has access to an oracle $\mathcal{O}_{\mathcal{M}}(ID_i)$ corresponding to queries of a secret key $sk[ID_i]$ associated to a new identity ID_i. $\mathcal{O}_{\mathcal{M}}(ID_i)$ only answer to queries with $ID_i \neq ID_{\mathcal{S}}$. The experiment for unforgeability is defined in Figure 1. The probability of success for a given scheme is denoted by $Adv^{uf}_{\mathsf{IDBS},\mathcal{U}^*}(\mathfrak{K}) = Pr[\mathsf{Exp}^{uf}_{\mathsf{IDBS},\mathcal{U}^*}(\mathfrak{K}) = 1]$, it denotes the advantage of the attacker. An adversary wins if after polynomial time and a polynomial number of queries to $\mathcal{O}_{\mathcal{M}}$ he is able to succeed with non-negligible probability $Adv^{uf}_{\mathsf{IDBS},\mathcal{U}^*}(\mathfrak{K})$.

$\mathsf{Exp}^{uf}_{\mathsf{IDBS},\mathcal{U}^*}(\mathfrak{K})$
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $sk[ID] \leftarrow \mathsf{Extract}(msk, ID)$
3. For $i = 1, \ldots, q_s$, $\mathsf{Protocol}\langle \mathcal{C}(sk[ID]), \mathcal{A}(ID)\rangle$
4. $((m_1, \sigma_1), \ldots, (m_{q_s+1}, \sigma_{q_s+1})) \leftarrow \mathcal{A}(mpk, ID)$
5. If $\exists i \neq j, m_i = m_j$ or if $\exists i$, $\mathsf{Verif}(ID, m_i, \sigma_i) = 0$: Return 0
6. Else Return 1

Fig. 1: Security Game for Unforgeability of IDBS.

- *Blindness.* This condition protects the user from a malicious signer $\mathcal{S}^*$, a malicious signer signing two messages m_0 and m_1 chosen by himself should be unable to de-

cide which one was signed first. The associated game is given in Figure 2. The probability of success is defined by $Adv^{bl}_{\mathsf{IDBS},\mathcal{S}^*}(\mathfrak{K}) = |1/2 - Pr[\mathsf{Exp}^{bl}_{\mathsf{IDBS},\mathcal{S}^*}(\mathfrak{K}) = 1]|$. An adversary wins the blindness game if after polynomial time he is able to succeed in the game with non-negligible probability $Adv^{bl}_{\mathsf{IDBS},\mathcal{S}^*}(\mathfrak{K})$. If $Adv^{bl}_{\mathsf{IDBS},\mathcal{S}^*}(\mathfrak{K}) = 0$, the blindness is considered as *unconditional*.

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

Fig. 2: Security Game for Blindness of IDBS.

Identity-based proxy Blind Signature.

Definition 15 (ID-based Proxy Blind Signature - IDPrBS**).** *An* IDPrBS *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 master entity $\mathcal{M}$, 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 $\mathcal{M}$. It call $\mathfrak{K}$ to generate a master keys (mpk, msk).*
- $\mathsf{Extract}(msk, ID)$*: this protocol is run by the master entity $\mathcal{M}$. It takes as input an identity ID and a master key msk and returns the corresponding secret key $sk[ID]$ via a secure channel.*
- $\langle \mathcal{S}, \mathcal{P}\rangle$ *is the* proxy-designation protocol *in between $\mathcal{S}$ and $\mathcal{P}$. The input are the two identities $ID_{\mathcal{S}}$ and $ID_{\mathcal{P}}$ of the signers, they respective secret keys (query to $\mathcal{M}$ 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 [10] in the general context of proxy signatures. The definition given here have been first given in [12]. For these types 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. We allow the adversary to interact with honest users playing the role of a designator or of a proxy signer. The adversary has access to oracles during this. Elements returned by the adversary should not have been received from any query to an oracle.

- ***Query of Extraction:*** $\mathcal{O}_{\mathsf{Extract}}(msk, \cdot) \rightarrow (sk[ID_i], \mathsf{cert}_{ID_i})$
  $\mathcal{A}$ request extraction for an identity ID_i, he sends ID_i to the PKG and receive the consistent answer $sk[ID_i]$ with the certificate cert_{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.

We formally defined all security properties that a IDPrBS scheme should satisfy as follows:

- *Blindness* has to be considered from the points of view of a malicious signer $\mathcal{S}^*$. He is required to win the experiment of Figure 3 [103]. A proxy blind signature achieves *blindness* if for any polynomial time adversary $\mathcal{A}$, the advantage $Adv^{bl}_{\mathsf{IDPrBS},\mathcal{A}}(\mathfrak{K}) = |\mathsf{Pr}[\mathsf{Exp}^{bl}_{\mathsf{IDPrBS},\mathcal{A}}(\mathfrak{K})] - 1/2|$ is negligible.
- *Unforgeability* is quite similar to the context of ID-based proxy signature schemes defined in [10]. The experiment is given in Figure 4.
- *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 5.

$\mathsf{Exp}^{bl}_{\mathsf{IDPrBS},\mathcal{S}^*}(\mathfrak{K})$:
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. 3: Security experiment for blindness of IDPrBS [103].

$\mathsf{Exp}^{uf}_{\mathsf{IDPrBS},\mathcal{U}^*}(\mathfrak{K})$:
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. 4: Security experiment for unforgeability of IDPrBS [10].

$\mathsf{Exp}^{veri}_{\mathsf{IDPrBS},\mathcal{P}^*}(\mathfrak{K})$:
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. $(sk_{\mathcal{P}}, w_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathsf{DelGen}(ID_{\mathcal{S}}, ID_{\mathcal{P}}, sk[ID_{\mathcal{S}}], m_w)$
5. $(m, \sigma, m'_w, w'_{\mathcal{S}\rightarrow\mathcal{P}}) \leftarrow \mathcal{A}(mpk, sk_{\mathcal{P}}, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}})$
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. 5: Security experiment for verifiability of IDPrBS.

– *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 delegation made by $\mathcal{S}$ to $\mathcal{P}$. In case of misuse, the responsibility of the proxy signer should be determined explicitly. This is formalised in Figure 6.

$\mathsf{Exp}^{PoM}_{\mathsf{IDPrBS},\mathcal{P}^*}(\mathfrak{K})$:
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. 6: Security experiment for Prevention of Misuse of IDPrBS.

– *Strong Identifiability* requires that anyone can determine the identity of the corresponding proxy signer from the proxy signature as described by the experiment in Figure 7. This is necessary to allow linkability of a signature to a proxy signer in case of a fraud. In the context of ID-based proxy signature, it is straight forward achieved.

$\mathsf{Exp}^{st-id}_{\mathsf{IDPrBS},\mathcal{P}^*}(\mathfrak{K})$:
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. 7: Security experiment for strong identification IDPrBS.

– *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 8.

An adversary breaks an identity-based proxy blind signature if for any of these experiments $\mathsf{Exp}^{game}_{\mathsf{IDPrBS},\mathcal{A}}$ he has non-negligible probabilities of winning the corresponding

$\mathsf{Exp}^{st-und}_{\mathsf{IDPrBS},\mathcal{P}^*}(\mathfrak{K})$:
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. 8: Security Experiment for Strong Undeniability of IDPrBS.

advantages

$$\mathsf{Adv}^{game}_{\mathsf{IDPrBS},\mathcal{A}} = \mathsf{Pr}[\mathsf{Exp}^{game}_{\mathsf{IDPrBS},\mathcal{A}} = 1].$$

Identity-based Fair Blind Signature.

Definition 16 (ID-based Fair Blind Signature - IDFBS). *An IDFBS with security parameter $\mathfrak{K}$ is a 5-tuple of polynomial-time algorithms and protocols (Setup, Extract, $\langle \mathcal{S}, \mathcal{U} \rangle$, Verif, LinkRecov) involving a master entity $\mathcal{M}$ (sometime call judge), an original signer $\mathcal{S}$, a user $\mathcal{U}$. Algorithms work as follows:*

- $\mathsf{Setup}(1^{\mathfrak{K}}) \rightarrow (mpk, msk)$ *calls $\mathfrak{K}$ to generate a master key pair (mpk, msk) to issue message and a link recovery key rk.*
- $\mathsf{Extract}(msk, ID) \rightarrow sk[ID]$ *takes as input the identity a signer $\mathcal{S}$ and a master key msk. It returns the corresponding secret key $sk[ID]$ which is sent to $\mathcal{S}$ via a secure channel.*
- $\langle \mathcal{S}(sk[ID]), \mathcal{U}(mpk, m, ID) \rangle \rightarrow (Out_{\mathcal{S}}, \sigma)$ *is the signature issuing protocol between the signer $\mathcal{S}(sk[ID])$ and the user $\mathcal{U}(m, ID)$ for a message $m \in \{0,1\}^*$. It generates the signature σ for the user and the signer's view of the protocol Out_S to $\mathcal{S}$.*
- $\mathsf{Verif}(mpk, ID, m, \sigma)$ *outputs 1 if the signature σ is valid, otherwise 0.*
- $\mathsf{LkRecov}(Out_{\mathcal{S}}/m, \sigma)$ *is the link recovery. Its specifications depend on the context and the type of fairness achieved by the scheme. It either outputs a linkage in between the signer's view of the protocol and a message-signature pair (Type 1) or given a message-signature pair enables recovery of the identity of the sender of the message (Type II).*

Security notions for identity-based fair blind signature are specified within six properties that need to be achieved by a scheme. Correctness and blindness are still mandatory but remains the same as for IDBS, the experiments have been presented in Tables 1 and 2. Four other experiments are needed to describe the security of a IDFBS scheme [25].

– *Identity Traceability.* No coalition of users can produce a set of signatures containing signatures which cannot be linked to an identity. This property is formalised in the experiment of Figure 9.
– *Signature Traceability*: No one should be able to produce a message-signature pair which is not traced by any issuing transcript or two pairs which are traced by the same transcript. This is formalised in Figure 6.

$\mathsf{Exp}^{Id-Trac}_{\mathsf{IDFBS},\mathcal{U}^*}(\mathfrak{K})$:
1. $((mpk, msk), rk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $\{(ID_i, m_i, \sigma_i)\}_{1 \leq i \leq l} \leftarrow \mathcal{A}()$
5. If $\exists i \in 1 \leq i \leq l$ st. $\mathsf{LkRecov}(m_i, \sigma_i) \neq ID_i$: Return 1
6. Else Return 0

Fig. 9: Security experiment for Identity Traceability IDFBS.

$\mathsf{Exp}^{Sg-Trac}_{\mathsf{IDFBS},\mathcal{U}^*}(\mathfrak{K})$:
1. $((mpk, msk), rk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID_{\mathcal{S}}) \leftarrow \mathcal{A}(mpk)$
3. $sk[ID_{\mathcal{S}}] \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $\{(ID_i, m_i, \sigma_i)\}_{1 \leq i \leq l} \leftarrow \mathcal{A}()$
5. If $\exists i \in 1 \leq i \leq l$ st. $\mathsf{LkRecov}(m_i, \sigma_i) \neq ID_i$: Return 1
6. If $\exists i_0, i_1, j \in 1 \leq i \leq l$ st.
$\mathsf{LkRecov}(Out_j, m_{i_0}, \sigma_{i_0}) = \mathsf{LkRecov}(Out_j, m_{i_1}, \sigma_{i_1}) = 1$ and $i_0 \neq i_1$: Return 1
7. Else Return 0

Fig. 10: Security experiment for Signature Traceability IDFBS.

– *Identity Non-Frameability*: No coalition of issuer, user and tracing authority should be able to provide a signature and a proof that the signature opens to an honest user who did not ask for the signature as we can see in the experiment of Figure 11.

$\mathsf{Exp}^{Id-Fram}_{\mathsf{IDFBS},\mathcal{U}^*}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(ID, m, \sigma) \leftarrow \mathcal{A}(mpk, sk_{\mathcal{P}}, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}})$
3. If $\mathsf{LkRecov}(m, \sigma) = ID$ and $(*, \sigma) \notin Out(\mathcal{O}_{\mathsf{Protocol}}(ID, m))$: Return 1
4. Else Return 0

Fig. 11: Security experiment for Identity Non-Frameability IDFBS.

– *Signature Non-Frameability*: No coalition of issuer, users and tracing authority should be able to provide a transcript that wrongfully opens to an honest signature. Figure 12 is presenting the associated experiment.

A fair blind signature achieve *blindness* if for any PPT adversary $\mathcal{A}$, the following advantage is negligible: $\mathsf{Adv}^{bl}_{\mathsf{IDFBS},\mathcal{A}} = |\mathsf{Exp}^{bl}_{\mathsf{IDFBS},\mathcal{A}}(\mathfrak{K}) - 1/2|$. The remaining security properties are achieved if the corresponding experiment has negligible probability to output 1. To prosper the adversary has access to three oracles during the experiment. $\mathcal{A}$ is able to make any number of queries to each one of them. The previously described $\mathcal{O}_{\mathsf{Extract}}$ and $\mathcal{O}_{\mathsf{S}}$ oracles are available. So does $\mathcal{O}_{\mathsf{LkRecov}}$ associated to the link recovery request to the authority.

Identity-based Forward Security Blind Signature.

$\mathsf{Exp}^{Sg-Fram}_{\mathsf{IDFBS},\mathcal{A}}(\mathfrak{K})$:
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $Out_{\mathcal{S}} \leftarrow \mathcal{A}(mpk, sk_{\mathcal{P}}, m_w, w_{\mathcal{S}\rightarrow\mathcal{P}})$
3. If $Out_{\mathcal{S}} \in Out(\mathcal{O}_{\mathsf{Protocol}_{\mathcal{S}}}(\cdot))$: Return 0
3. If $\mathsf{LkRecov}(Out_{\mathcal{S}}) = (m, \sigma)$ and for some ID, $\mathsf{Verif}(ID, m, \sigma) = 1$: Return 1
4. Else Return 0

Fig. 12: Security experiment for Signature Non-Frameability IDFBS.

These schemes are required to meet two properties *blindness* and *forward secure unforgeability*. Blindness is just as before, note that protocols can now be executed in two different time periods. Let T be the total number of possible key update, let $\mathcal{A}$ be an adversary against forward secure unforgeability playing the role of a user. The property of forward secure unforgeability holds if no PT $\mathcal{A}$ can win the game of Figure 13 with non-negligible advantage $Adv^{fs-uf}_{\mathsf{IDFSBS},\mathcal{A}}(\mathfrak{K}) = Pr[\mathsf{Exp}^{fs-uf}_{\mathsf{IDFSBS},\mathcal{A}}(\mathfrak{K}) = 1]$.

$\mathsf{Exp}^{fs-uf}_{\mathsf{IDBS},\mathcal{A}}(\mathfrak{K})$
1. $(mpk, msk) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $ID_{\mathcal{S}} \leftarrow \mathcal{A}()$
3. $sk[ID_{\mathcal{S}}]_0 \leftarrow \mathsf{Extract}(msk, ID_{\mathcal{S}})$
4. $(m, t^*, \sigma) \leftarrow \mathcal{A}(mpk)$
5. If $t^* < t$ and $\mathsf{Verif}_{ID_{\mathcal{S}}}(m, t^*, \sigma) = 1$: Return 1
6. Else Return 0

Fig. 13: Security Game for Forward Secure Unforgeability of IDFSBS.

During this game $\mathcal{A}$ is able to make queries to four oracles. The adversary can call the first three any number of time, for the last one only on execution is possible.

- **Query of Extraction:** $\mathcal{O}_{\mathsf{Extract}}(ID) \rightarrow sk[ID]$ is the extraction of an unclaimed identity $ID \neq ID_{\mathcal{S}}$.
- **Query of Key Update:** $\mathcal{O}_{\mathsf{KeyUpd}}(t)$ for each update query, if $t < T - 1$, the challenger update its key $sk[ID_{\mathcal{S}}]_t$ to $sk[ID_{\mathcal{S}}]_{t+1}$ and set t to $t + 1$. If $t = T - 1$, $sk[ID_{\mathcal{S}}]_T = \perp$ is returned.
- **Query of Signature:** $\mathcal{O}_{\mathsf{Sign}}(m, t)$ for each query a valid signature for m at time t is returned to $\mathcal{U}^*$, for that he uses key $sk[ID_{\mathcal{S}}]_t$.
- **Query of Revealed key:** $\mathcal{O}_{\mathsf{Reveal}}(t)$ for the break in query (execution only allowed once) the challenger must send the secret key $sk[ID_{\mathcal{S}}]_t$ to the adversary, and he moves the game to the output phase, no more oracle access is allowed.

Weak Identity-based Blind Signature.

Weak blindness allows the signer to link one its view $Out(m')$ of the blind signature protocols with hidden message m' to a revealed message-signature pair (m, σ). Hence, identifying the user at the origin of this message. Formally the game (of Figure 2) remain the same apart from line 6 replaced with $\mathcal{A}$ taking no input: "6. $b^* \leftarrow \mathcal{A}()$".