IACR Communications in Cryptology
ISSN 3006-5496, Vol. 2, No. 1, 48 pages.

https://doi.org/10.62056/a3wa3z10k

SoK: Privacy-Preserving Signatures

Alishah Chator[1], Matthew Green[2] and Pratyush Ranjan Tiwari[a, 3]

[1] Boston University, USA
[2] Johns Hopkins University, USA
[3] Eternis Labs, USA

Abstract. Modern security systems depend fundamentally on the ability of users to authenticate their communications to other parties in a network. Unfortunately, cryptographic authentication can substantially undermine the privacy of users. One possible solution to this problem is to use privacy-preserving cryptographic authentication. These protocols allow users to authenticate their communications *without* revealing their identity to the verifier. In the non-interactive setting, the most common protocols include blind, ring, and group signatures, each of which has been the subject of enormous research in the security and cryptography literature. These primitives are now being deployed at scale in major applications, including Intel's SGX software attestation framework. The depth of the research literature and the prospect of large-scale deployment motivate us to systematize our understanding of the research in this area. This work provides an overview of these techniques, focusing on applications and efficiency.

1 Introduction

Digital authentication was one of the first key breakthroughs enabled by cryptographic signatures [DH76]. The ability to authenticate that a message was created by a known sender and ensuring its integrity is at the heart of secure communication. Almost all communication on the internet today employs some variant of cryptographic signatures. While this has enabled a massive disruption in financial transactions and e-commerce at scale, digital signatures leave an identifiable digital fingerprint.

Any number of activities — from connecting to a cellular tower to conducting a payment, to browsing a modern website — creates a trail of digital artifacts that can adversely impact a user's privacy. In many cases, this loss of privacy is not a design feature. Rather, it is a side effect of individuals' need to authenticate themselves and their communications to service providers. Finding a way to allow authentication without loss of privacy, has been a major goal of the cryptography and systems research community [Cha85].

Since the early 1980s, the research community has made significant progress in this direction. In particular, researchers have developed several tools and protocols that allow for efficient **privacy-preserving authentication**. Because the most critical element of the authentication toolbox is the **digital signature scheme**, the majority of this work has focused on enhancing signatures with privacy properties. The result of this investigation includes efficient constructions of **blind signatures**, **group signatures**, and **ring signatures** as well as more powerful protocols for developing full-featured **anonymous credential** systems. While much of the early work in this area was conducted in the academic literature, recently the industry has begun to adopt some of these protocols for wide, high-value deployments [TPM14, Pop16, Noe15, H^+14].

E-mail: alishahc@bu.edu (Alishah Chator), mgreen@cs.jhu.edu (Matthew Green), pratyush@eternis.ai (Pratyush Ranjan Tiwari)

[a] Work done as a PhD candidate at JHU

Received: 2025-01-14 Accepted: 2025-03-11

The adoption of privacy-preserving signatures can be a challenge for the industry. Despite the publication of a large number of papers in this area, new security systems are being released with protocols that are inferior to those developed in the literature. Consequently, real security systems fail to benefit from the progress that researchers have accomplished regarding security definitions, constructions, and properties of these protocols. Additionally, the research community itself may be unaware of the challenges and open questions encountered by the industry as it attempts to deploy these technologies.

These developments motivate us to systematize the state of current knowledge regarding privacy-preserving authentication protocols, with a specific focus on digital signature schemes. Our goal is to provide a succinct overview of the state of the art in this field and to provide researchers and practitioners with a guide to which open problems remain. In addition, we examine current efforts to deploy these systems in practice and attempt to identify open problems or areas where the research community can provide assistance. Specifically, our contributions are: (i) We provide an overview of state of the art in privacy-preserving digital signature schemes, including blind (§2), group(§3), and ring (§4) signatures. (ii) We compare the many schemes in the literature and provide a summary that categorizes most existing schemes in terms of both asymptotic and concrete efficiency, as well as their underlying security assumptions. (iii) Our implementation and comparison Tables 4, 5, 6 allow practitioners to pick schemes suitable for their application and Tables 1, 2, 3 provide researchers a simple way to assess the state of existing work as it stands today. (iv) We present an overview of the open research problems and current deployment plans for these protocols. (v) We additionally discuss applications (§6), such as Decentralized Anonymous Attestation (DAA), private cryptocurrencies, and anonymous credential systems.

Classes of protocols. In this work we focus on the following types of signature schemes:

- **Blind signatures.** A blind signature scheme is a digital signature scheme that incorporates a blind signing protocol. This protocol allows a user to obtain a signature on the message from a second party, called the signer, without revealing to the signer either the message and/or the signature obtained. Blind signatures come in several variants, including partially-blind signatures (where the message is partially revealed to the signer), fair blind signatures (where the signature can be provably "unblinded" by user), and restrictive blind signatures (where the message must obey a specific format).

- **Group signatures.** A group signature scheme allows several members of a group to sign a message, such that a normal verifier cannot determine which group member was the signer. A distinguished party called a group manager is responsible for authorizing individual members of the group, and may selectively de-anonymize (or "trace") signatures to identify the signer. Some group signatures provide for static membership of the group, while others offer dynamic membership, in which group members may join and leave (be revoked) periodically.

- **Ring signatures.** Like group signatures, ring signatures allow a party to sign a message on behalf of a group of users – such that no verifier can determine which member issued the signature. Unlike a group signature, there is no single group manager. Rather, ring signature groups are assembled by the signer in an ad hoc fashion and without the requirement of a centralized setup procedure.

Methodology. With the sheer number of digital signature variants in the literature, it is important to be precise with what is captured by the notion of a privacy-preserving signature for this work. First, while there are many signatures with overlapping properties (for example, threshold signatures can have some level of group structure similar to a group signature), we identify blind, group, and ring signatures as the primitives where privacy is an inextricable part of their definitions. While blind signatures focus on hiding message content from signers, group and ring signatures aim to hide signer identity from verifiers while maintaining accountability. While they may be extended beyond just this property, privacy is inherent to their base-level definitions (unlike a threshold signature which may be extended to support privacy). We include an illustrative example instantiation to provide an intuitive sense of how to build each primitive while also highlighting design considerations. Next, we follow the evolution of constructions for each primitive to capture all relevant schemes while not including those whose settings are so different to be incomparable[1]. Similarly, variants of privacy-preserving signatures with additional features will be mentioned when relevant but not included in our analysis unless the underlying privacy-preserving signature is of independent interest. Plain digital signatures used as building blocks for privacy-preserving signatures are mentioned when relevant but are not a primary focus of this work. In our comparisons of schemes, we focus on the *most efficient scheme under each model.* This is necessary as the related works span a period of multiple decades. Additionally, we also present comparisons within the model of schemes with competing merit based on setting, assumption, or other properties. Another goal of our work is to provide researchers and practitioners with a self-contained resource for choosing the right privacy-preserving signature scheme for their applications. Our analysis in Tables 4, 5, 6 allows for this choice to be informed by the functionality and efficiency of existing schemes. We provide an overview of the relevant cryptographic settings, assumptions, and computational models in Appendix A.

Implementations of Privacy-Preserving Signatures. As part of our systematization, we also evaluated several public open-source implementations of privacy-preserving signature schemes. Our findings (§5, Tables 5, 6) provide a list of functional implementations, albeit of research/proof-of-concept code, that can serve others as a reference. Given the wide-variety of applications of these schemes, there have been standardization efforts [DJW23] and libraries[2] released by industry efforts to provide efficient implementations. The implementations we pick for efficiency comparisons are from credible sources and are less likely to be marred by errors and bugs. Thus, providing a high confidence comparison of the best-case efficiency of such schemes.

Outline of this work. In the remainder of this work we separately discuss blind signatures, group signatures, and ring signatures. This raises the question: how should we compare different signature schemes from each class? To compare schemes, we consider the following elements. First, we consider what specialized features the signature scheme offers. Next, we can compare signatures by efficiency, which includes computational efficiency of signing, verification and other operations, as well as signature size (in this work we focus primarily on verification time and signature size). We will be assuming 3072-bit RSA, 256-bit Elliptic curve group elements, 256-bit $\mathbb{G}_1$, 768-bit $\mathbb{G}_2$, and 256-bit $\mathbb{Z}_p$ in our estimations. For lattices and other settings with less common elements and operations, we will provide concrete sizes for comparison where possible. Finally, we consider the cryptographic assumptions and computation model used to prove security of the protocol.

Limitations of current approaches. While much work has been done in this space we see there are still several limitations. Post-quantum schemes are still not overall efficient for both signature size and verification time. Despite the large number of constructions in the academic literature, open-source implementations are hard to come by for many of the schemes. While the theory of privacy-preserving authentication has made great strides, in terms of real-world deployments only a handful of concretely efficient schemes are available, which are overwhelmingly in the ROM setting.

[1] We will still mention these schemes when relevant.

[2] https://github.com/IBM/libgroupsig/wiki/Supported-schemes

2 Blind Signatures

The idea of private signature and authentication schemes began with the question of how to authenticate data without revealing its contents. This led to the development of blind signature schemes. A blind signature is a standard digital signature that contains an additional protocol by which a user may *blindly* obtain a signature from a signer who possesses a signing key sk. Blind signatures enabled the creation of several privacy-preserving authentication technologies, including electronic privacy-preserving cash (e-Cash) [Cha82], electronic voting [Cha04], and one-time anonymous credential systems [Cha85]. Security for a blind signature protocol inherits correctness and unforgeability requirements from digital signatures but also includes a privacy property. Specifically, a blind signature should possess the following properties:

- **Correctness:** An honestly generated blind signature should be considered valid by any verifier.
- **Unforgeability:** In the case of blind signatures, unforgeability is frequently defined using the notion of a "one more forgery" attack. This means that in order for an adversary to have k valid message-signature pairs, it must have participated in k signature generations.
- **Blindness:** If V is the view of the blind signature protocol and (m, σ) its output, then a signer should not be able to go back and link the view to the signing pair. In other words the signer should not know which instance of the protocol involved which message-signature pair.

2.1 Formal Definitions

A blind signature scheme is a tuple of two algorithms (**Gen**, **Verify**) as well as an interactive protocol **BlindSign** that is conducted between a user $\mathcal{U}$ and a signer $\mathcal{S}$. These are defined as follows:

- **Gen**(1^k)**:** Outputs a key pair pk, sk
- **BlindSign**$(\mathcal{U}(m, pk), \mathcal{S}(sk)) \to (\sigma, \perp)$**:** The user supplies a public key pk and a message m, and the signing provides a secret key sk. The protocol returns a signature σ to the user, and produces no output to the signer.
- **Verify**(pk, m, σ)**:** Which takes a message m and a blind signature σ and outputs 1 if the signature is valid and 0 otherwise.

Blind signatures were developed in the early 1980s, and security definitions have closely followed the evolution of provably-secure cryptography itself. The key security properties were informally described by Chaum [Cha82], [Cha83]. With the development of *Provable Security*, it became of interest to evaluate the security of blind signatures in the *Random Oracle Model* (ROM). Pointcheval *et al.* [PS96] formalized the the security of blind signatures into the idea of "one-more" forgery. EUF-CMA does not make sense in a blind signature context as the signer has no knowledge regarding the messages it is providing signatures on and thus the reduction cannot tell whether the message-signature pair output by the adversary is a forgery or a previously issued signature. Rather, a secure blind signature is one where the number of valid signatures obtainable by a user is strictly bounded by the number of interactions with the signing party. Under this definition they constructed a blind signature scheme based on a witness indistinguishable version of the Schnorr scheme from [Oka93] which is secure in the ROM.[3] Chaum's original scheme was

[3] The included scheme was only secure if the number of interactions is bounded polylogarithmically. This was improved to polynomially many interactions in [Poi98]

also found to be secure in the ROM ([MSS98] [BNPS03]), though forgery is possible in an instantiation with a poorly implemented hash function. Juels *et al.* [JLO97] provided game-based definitions of unforgeability and blindness.

Additionally, Juels *et al.* [JLO97] introduced the problem of concurrent security, where unforgeability must hold even when interactions are not sequential. This definition is significantly more difficult to satisfy as the adversary may be running many parallel sessions that are arbitrarily interleaved. This notion became increasingly important as cryptography began to transition away from the random oracle model, and thus the number of protocol rounds increased.[4] To further complicate matters there have been impossibility results on concurrently secure blind signatures in the *Standard Model* (SM) under simulation-based definition via black-box proofs [Lin03], finding security proofs via black box reductions in three round (or fewer) schemes [FS10], and constructing blind signatures (using black-boxes) from *One Way Permutations* ([KSY11]). It is possible to get around these impossibility results by using game-based definitions, interactive assumptions, having inefficient unforgeability reductions, and using non black-box constructions.

Schröder *et al.* [SU12] introduce an additional constraint on unforgeability known as *honest-user unforgeabilty.* An adversary may request a signature on the same message multiple times and thus, obtain more valid signatures than messages it has requested to be signed.

2.2 Illustrative example

We assume the existence of a secure digital signature scheme (**DS.Gen**, **DS.Sign**, **DS.Verify**) as well as a general secure two-party computation scheme $\langle A, B\rangle$ that can securely compute a function $f \rightarrow (z_A, z_B)$ where z_P is the output received by party $P \in \{A, B\}$. These are defined as follows:

- **Gen**(1^k)**:**
  - Run **DS.Gen**$(1^k) \rightarrow (pk, sk)$
  - Output pk to $\mathcal{U}$ and (pk, sk) to $\mathcal{S}$.
- **BlindSign**$(\mathcal{U}(m, pk), \mathcal{S}(sk)) \rightarrow (\sigma, \perp)$**:**
  - Run the two-party protocol $\langle \mathcal{U}, \mathcal{S}\rangle$ that computes the function **DS.Sign**$(sk, m) \rightarrow (\sigma, \perp)$.
- **Verify**(pk, m, σ)**:**
  - Run **DS.Verify**$(pk, m, \sigma) \rightarrow b$
  - Output b.

Here we see that in its most basic form, a blind signature scheme consists of adapting a digital signature scheme to have a two-party computation (2PC) (*e.g.*, [GMW87],[Yao86]) of the signing algorithm with the user supplying the message and the signer supplying the signing key. As this should hopefully illustrate, much of the work in building blind signature schemes focuses on efficient 2PC constructions with minimal round complexity as well suitable signature schemes that perform well in this 2PC setting.

[4] This is because many ROM constructions only had two rounds, a signature request and the signer's response. Two round schemes trivially fulfill concurrent security as an adversary only send one message per session. On the other hand, schemes outside ROM had higher round complexities.

2.3 Evolution of constructions.

The original blind signature construction by Chaum [Cha82, Cha83] was in the RSA setting. Shortly afterwards, a crop of more efficient DL-based schemes were proposed [Cha88, CP92, CPS95]. While practical, many of these schemes had no clear proofs of security. This was worrying as these blind signature schemes were utilized in sensitive applications such as e-Cash [FTY96]. Pointcheval [Poi98] provided the first provably secure blind signature scheme, building the work of [PS96] which only provided security for a logarithmic number of signing queries.

Around the same time, Solms *et al.* [vSN92] detailed how the anonymity provided by blind signatures may lead to the rise of "perfect crimes" where money can no longer be used to track criminals. Fair blind signatures were introduced by Camenisch *et al.* [SPC95] to address this scenario. This introduces a judge that is able to link a signature to the session it was created in. Two works [AO01, HT07] provide a provable framework for developing fair blind signatures in the ROM. There has also been work [FV10, RS10] in search of fair blind signatures in the standard model (SM).

Similarly, it became desirable to provide feature-rich schemes. Signers may only want to give signatures on certain types of messages or add some metadata to the blind signature. Brands' scheme [Bra93b] was a major development on enabling restrictive blind signatures. [AF96] introduced and [AO00a] formalized the idea of a partially blind signature, and [KLX23] provided updated security proofs. In 2003, Boldyreva [Bol03] opened up the world of pairing based blind signatures. This allowed for efficient proofs of knowledge on blinded signatures. Zhang and Kim [ZK02] first introduced the idea of an *identity-based* blind signatures, in which the user's identity is used in place of a public key. The first provably secure construction was by Galindo *et al.* [GHK06].

A key problem is producing efficient and provably secure blind signature schemes. Many efficient schemes are in the ROM, and thus are only secure under trusted assumptions. [CKW04] demonstrates how to build a scheme in the standard model by lifting a digital signature scheme that is provably secure in the standard model into a blind signature scheme through computing the signing algorithm within a two-party computation. Lindell's impossibility results for constructing blind signatures in the SM with black box security proofs motivated the usage of common reference string (CRS). [Fis06] discussed the notion of round optimal blind signatures, where the user and signer only have to transmit one message each, and offered the first construction not in ROM. In order to obtain concurrent security guarantees, recent work has focused on finding efficient round optimal schemes outside ROM [GRS$^+$11, BFPV13, FHKS16, Gha17, BBCF20, KNYY21]. Additionally, Hanzlik [Han23] introduced non-interactive blind signatures for random messages, where the first round message can be reused to save on interaction.

A recent development impacting the design of the secure blind signatures was the discovery of a polynomial time attack on schemes relying on the hardness of the ROS (Random inhomogeneities in a Overdetermined Solvable system of linear equations) problem [BLL$^+$22]. As described by [Sch01], many DL-based signatures rely this hardness for their concurrent security against "one-more" forgery attacks. Concretely, the attack in [BLL$^+$22] was able to produce a forgery for the Schnorr scheme in a few seconds with 256 concurrent executions (which as they mention is significantly less than the number of concurrent sessions modern web-servers have). The upshot of this attack is that many blind signatures are not suitable for large scale deployments and should only be used sequentially. This vulnerability impacts a number of Schnorr [CP92] and Okamoto-Schnorr [PS00] based schemes. Work by Kastner *et al.* [KLX22] shows that the Abe blind signature is concurrently secure in the algebraic group model (AGM) by avoiding rewinding in their reduction and taking advantage of the scheme's witness indistinguishability. Other recent work looks at boosting [KLR21, CAHL$^+$22, HLW23] to transform linear blind signatures into concurrently secure schemes. These are in the ROM but either require high communication costs or large signatures.

With the prospect of quantum computation on the horizon, there have been works exploring instantiations of blind signatures in other settings such as lattices [HKLN20] and coding theory [BGSS17]. The lattice constructions exist in the SIS-based ROM setting [HKLN20], and improvements to round optimal constructions in the ROM one-more ISIS [AKSY22], MLWE [AAHJ21, LNP22], and QROM [dPK22] settings.

Comparing constructions. Figure 1 provides a comparison of several representative blind signature constructions drawn from the literature.

Takeaways. Despite decades of followups since the original RSA blind signature [Cha82], it remains one of the best existing options for use. While the ROS attack revealed vulnerabilities in some schemes, others that are efficient and secure such as [TZ22, CKM$^+$23] are in the idealized AGM setting. Other schemes in the plain ROM setting remain impractical for now. Outside of ROM schemes, high communication costs or round complexity during signing or large signature sizes limit the deployability of these schemes.

Table 1: A comparison of several blind signature constructions. Schemes marked with a ‡ are vulnerable to the ROS attack. *Setting* and *Assumption* indicate the cryptographic setting and hardness assumptions the scheme's security is based on. *Signature* and *Verification time* represent an approximate estimate (based on the paper) of the signature size in bits and the number of dominant operations ($\mathbb{G}_{exp}$is group exponentiation and p is bilinear pairing) used in signature verification. *Rounds* specifies the number of rounds in the blind signature protocol (where † denotes a reusable first round message), and *Security* indicates the security model. Schemes marked with an asterisk have high communication overhead due to Groth-Sahai (GS) or NIZK proofs [GS08].

Reference	Setting	Assumption	Signature (bits)	Verification	Rounds	Security Model
Chaum82 [Cha82]	RSA	RSA	3072	RSA_{enc}	2	ROM
AO00‡ [AO00b]	DL	DL	1024	$4\mathbb{G}_{exp}$	3	ROM
CKMTZ23 [CKM$^+$23]	DL	DL	768	$3\mathbb{G}_{exp}$	3	ROM+AGM
Hanzlik23 [Han23]	Pairing	DL	1527	$6p$	$1^\dagger$	ROM+GG
HLW23 [HLW23]	Pairing	CDH	45568	$97p$	2	ROM
BFPV13* [BFPV13]	Pairing	CDH+DLIN	512	$3p$	2	SRS
Okamoto06 [Oka06]	Pairing	2SDH	1280	$3\mathbb{G}_{exp}+ 2p$	4	SM
FHKS16* [FHKS16]	Pairing	DDH	1024	$15p$	2	SM
dK22* [dPK22]	Lattice	MSIS+MLWE+DSMR	$\sim$ 80000	-	2	QROM

3 Group Signatures

Where blind signatures focus primarily on hiding the *contents* of an authenticated document from a signer, group signatures [CVH91] are intended to prove membership in a organization. For example in the real world, a company spokesperson might demonstrate their credibility without revealing who they are by using a corporate watermark. These signatures have begun to see widespread adoption, particularly as a component of anonymous credentials [Cha85], *software attestation* protocols for the Trusted Platform Module system [TPM14], and Intel's SGX [BL07].[5]

A group signature scheme is operated by a group of signers, along with a trusted party called the *group manager*. The group manager is responsible for generating a group public key and enrolling signers into the group. Once enrolled, any member of the group can produce a group signature on an arbitrary message. This signature can then be verified using the group public key. To normal verifiers, a group signature reveals nothing beyond the fact that *some* member of a group signed the message. However, to distinguish true

[5] We discuss these applications further in §6.

group signatures from a trivial construction (in which all group members simply share a common secret key), in a true group signature the group manager must be able to *trace* the author of a signature: for example, in the event that abuse is detected by one of the members. To do this, the manager retains a *tracing trapdoor* that allows it to verify the precise authorship of any group signature.[6] Informally, all of the group signature schemes we consider in this work satisfy the following basic properties:

- **Correctness:** Any honestly generated group signature should be considered valid by any verifier.
- **Unforgeability:** A non-signer should have negligible probability of producing a valid group signature.
- **Anonymity:** To a normal verifier (*i.e.,* one who does not have access to a tracing trapdoor or oracle), a group signature should appear equally likely to have been produced by any of the group members (or another group member, if the verifier is also a group member).[7]
- **Exculpability:** No one, including the group manager, should be able to produce group signatures of behalf of another member.
- **Traceability:** If a message is signed by member i, then the opening of this signature by the group manager should output i.
- **Coalition Resistance:** No subset of group members can collude to produce a group signature that cannot be traced back to any of them.
- **Framing:** No subset of group members can collude to produce a group signature that the opening algorithm attributes to a member of the group not in the subset.

3.1 Formal definitions

While there are a broad range of group signature schemes, the literature has largely coalesced around two formal definitions.

The BMW definition. Proposed by Bellare, Micciancio, and Warinschi *et al.* [BMW03] this model captures the above properties into 3 requirements (Which we detail in Appendix B).[8]

A BMW group signature scheme is composed of four algorithms:

- **GKg($1^\lambda, 1^n$):** Which takes a security parameter λ and a group size n, and outputs a group public key gpk, a group manager secret key $gmsk$, and an n-vector of group member secret keys $\boldsymbol{gsk}$ where $\boldsymbol{gsk}[i]$ is the secret key of the i-th group member.
- **GSig($\boldsymbol{gsk}[i], m$):** Which takes a message m and a group member's secret key $\boldsymbol{gsk}[i]$, and outputs a group signature σ.
- **GVf(gpk, m, σ):** Which takes a group public key gpk, message m and a group signature σ and outputs 1 if the signature is valid and 0 otherwise.

[6] In some schemes, the tracing enrollment functions of the group manager may be split across two separate parties.

[7] An equivalent property called *unlinkability* holds that (without an opening oracle) an adversary should not be able to attribute a pair of signatures to the same user.

[8] There is also an additional *Compactness* requirement that group signatures only grow logarithmically with the size of the group rather than polynomially.

- **Open($gmsk, m, \sigma$):** Which takes a group manager's secret key $gmsk$, message m and a group signature σ and (if successful) outputs the identity i that produced this signature, otherwise outputs $\perp$.

Notably, this model only applies to static groups where all signer keys are generated by the group manager. It also makes the somewhat artificial assumption that while the group manager's secret key may be compromised (for traceability), the group manager itself will not be corrupted in the anonymity experiment.

The BSZ definition The BMW definition is limited in some ways, due largely to the fact that it supports only static groups. In 2005, Bellare, Shi and Zhang proposed an updated model that allowed members to *dynamically* join the group. As a secondary factor, the model attempts to minimize the trust required of the group authority. In this BSZ model, the group manager is split into two parties: an opener who can trace signatures, and an issuer who can adaptively add a new member to the group by issuing them a signing key. BSZ signatures are substantially more complex, and are composed of six algorithms and an interactive **Join** protocol run between the group manager and each new member. For space reasons, we leave a description of these algorithms to Appendix B. It is important to note that dynamic group signatures were independently formalized by Kiayias and Yung [KY06]. The [KY06] model is identical to BSZ, except the absence of a judge in their syntax.

While literature on group signatures use a variety of terms to refer to the model used, in this paper static group signatures will be described as in the BMW model and dynamic ones are in the BSZ model. This will assume CCA2-full-anonymity (adversaries having access to the opening oracle before and after the challenge), and weaker notions such as CPA-full-anonymity (adversary cannot query opening oracle) will be denoted as BMW$^-$ or BSZ$^-$. Schemes achieving improved notions of dynamic groups in the vein of [BCC$^+$16a, BHSB19] will be denoted as BSZ$^+$.

3.2 Illustrative Example

We use the ideas of [CS97] to demonstrate a simple group signature scheme. We assume the existence of a one way function f, a secure digital signature scheme (**DS.Gen**, **DS.Sign**,**DS.Verify**), a randomized public key encryption scheme (**PKE.Gen**, **PKE.Enc**, **PKE.Dec**), and a non-interactive zero knowledge proof of knowledge scheme **NIZKPoK**.

- **GKg($1^\lambda, 1^n$):**
  - Run $\textbf{DS.Gen}(1^\lambda) \to (pk_{ds}, sk_{ds})$ and Run $\textbf{PKE.Gen}(1^\lambda) \to (pk_{pke}, sk_{pke})$.
  - Sample $x_1, ..., x_n$ and for all $i \in [n]$ compute $z_i = f(x_i)$ and $v_i = \textbf{DS.Sign}(sk_{ds}, z_i)$.
  - Output $gpk = (pk_{ds}, pk_{pke}, f)$, $gmsk = (sk_{ds}, sk_{pke})$ and $\boldsymbol{gsk}$ where $\boldsymbol{gsk}[i] = (x_i, z_i, v_i)$.
- **GSig($\boldsymbol{gsk}[i], m$):**
  - Randomly sample r and compute $d = \textbf{PKE.Enc}(pk_{pke}, (m, z_i); r)$
  - Use the **NIZKPoK** generate a proof π for the following statement: $\{(x_i, v_i, r) : d = \textbf{PKE.Enc}(pk_{pke}, (m, f(x_i)); r) \wedge \textbf{DS.Verify}(pk_{ds}, f(x_i), v_i) = 1\}$
  - Output $\sigma = (\pi, d)$.
- **GVf(gpk, m, σ):**
  - verify the proof p and output the result.

- **Open**$(gmsk, m, \sigma)$**:**
  - Compute $\mathbf{PKE.Dec}(sk_{pke}, d) = (m', z')$
  - Output i such that $z' \in \boldsymbol{gsk}[i]$

As this example illustrates, moving beyond trivial constructions with a single signing key requires multiple building blocks. In order to have a fixed size group public key, the group manager gives each group member a membership certificate. To sign a message on behalf of the group, a member must prove their group membership in a way that binds the message to sign to the proof (There is a primitive known as a signature of knowledge that generalizes this idea [CL06]). As the signature embeds an encryption of the membership certificate, the group manager can decrypt this to find the identity of the issuer. This example should illustrate that the focus of building group signature schemes has been on minimizing the trust in the group manager, reducing the dependence on expensive public key primitives, and leveraging efficient proof techniques.

3.3 Evolution of constructions

The first group signature schemes were developed by Chaum and van Heyst [CVH91]. Each of the resulting constructions produced a signature size that was dependent on the number of group members N, and some suffered from collusion attacks in which a collection of group members could work together to recover the secret key of a remaining member.[9] Chen and Pedersen [CP94] improved these signature schemes by achieving anonymity even against computationally unbounded adversaries (perfect anonymity). Additionally they demonstrate a general approach to tracing, where the tracing information can verifiably shared such that any subset of the group of size > 2 can identify the signer.

A significant amount of subsequent work went into two separate areas: (1) building strong coalition-resistant group signatures, and (2) developing signature schemes with a signature size and verification time that were small (at least logarithmic) in the number of group members.[10] The latter problem was viewed as particularly important for systems that were intended to be deployed to large organizations.

Camenisch and Stadler [CS97], and subsequently Camenisch and Michels [CM98] and Ateniese *et al.* [ACJT00] addressed both of these problems by proposing efficient signature schemes in which the signature scheme did not depend on the size of the group. The overall approach in these systems is to construct a form of *anonymous* certificate that can be issued to the group member by the group manager, and then provide a protocol by which the member can (non-interactively) prove knowledge of this certificate – either in combination with a proof of knowledge of a signature on a related public key, or by revealing a randomized version of their public key. While such proofs are fairly complex, the underlying witness does not depend on the number of group elements. In the case of schemes in the vein of [ACJT00], the group manager trapdoor is the factorization of an RSA modulus N.

With the advent of pairings, several *short* group signature constructions were proposed. The first of these, by Boneh, Boyen and Shacham [BBS04], allowed for a remarkably small group signature with a size comparable to a standard RSA signature (at the 128-bit security level), with a proof in the random oracle model (Improved security proof from techniques in [TZ23]). Following this, Boyen and Waters [BW06] proposed an efficient group signature scheme that did not rely on random oracles for security. Each of these schemes employed

[9] One solution to this problem was simply to have the group manager also act as a member, and be resistant to collusion.

[10] In practice, since group signatures must reveal to a tracing authority which member signed, they must include at least $log(n)$ bits of information, where n is the size of the group. However, this is likely to be a small value in practice.

zero knowledge proofs to achieve strong security in the BMW or BSZ model. One final notable construction in this vein is the work of Hohenberger *et al.* [ACHDM05], who proposed a very efficient group signature based on a *re-randomizable* certificate, at the cost of losing the ability to achieve BMW security and using an interactive non-falsifiable assumption.[11]

While group signatures were primary constructed in the *sign-encrypt-prove* (SEP) paradigm, there has been interest in building group signatures without directly using public-key encryption as a building block leading to the *sign-randomize-prove* (SRP) paradigm [BCN+10]. The first group signature in the SRP paradigm achieving full BSZ security was by Derler *et al.* [DS18]. Ateniese *et al.* [AdM03] provided an early instantiation of group signatures in the standard model, with Backes *et al.* [BHSB19] providing efficient construction in the fully dynamic group setting. There has also been work by Libert *et al.* [LPY12b, LPY12a] examining the challenges of efficient revocation in the standard model.

At least two constructions took the work above into practice. To support the Trusted Platform Module [TPM14], Brickell *et al.* [BCC04] developed a scheme called Direct Anonymous Attestation. This scheme is a variant of a Strong RSA-based group signature, and allowed TPM devices to attest to the correctness of a software component without revealing the identity of the signing device (see §6 for a more detailed discussion). This system featured a limited revocation system that only operated if the signing key was extracted from the device and published. The second proposal, called Enhance Privacy ID [BL07], was an enhancement of the Boneh *et al.* system of [BBS04] and allowed tracing and revocation on presentation of a valid signature proving abuse. The latter system is now being widely deployed as part of Intel's SGX [sgx16].

There have also been a number of works looking at modifying the functionalities of group signatures. Bifurcated [LNPY21] and multimodal [NGSY22] signatures allow for an adjustable trade-off between accountability and anonymity for group signature style primitives. There have also been a number of works [GL19, FGL21, DL21] looking at different ways users can specify the linkability of their signatures. Threshold dynamic group signatures [CDL+20] split the role of issuer and opener over multiple entities.

Finally, many recent works develop group and ring signatures in new settings, such as the lattice setting [LLLS13, DPLS18, LNPS21, KY19, LNWX18, BDK+23], isogeny setting [BDK+23], and the code-based setting [ELL+15, ELL+20]. While these constructions do not yet compete with pairing and RSA-based signatures on efficiency, they provide a path towards post-quantum security for group signature schemes. Building efficient group signatures in the post-quantum setting, with sizes that are concretely close to the $log(n)$ bits lower bound, remains an open problem.

Comparing constructions. Figure 2 provides a comparison of a selection of representative group signature constructions drawn from the literature.

Takeaways. Despite the expensive cost of pairings and additional reliance on the idealized GGM setting, DS18 [DS18] offers a scheme with practical efficiency, however no public implementation was readily available. BBS04 [BBS04] and PS16 [PS16] have efficient public implementations but are only secure under relaxations of the standard security models. Further investigation of proving existing schemes secure without relaxations of security notions, building efficient group signatures outside of the pairing and ROM settings, and achieving modern notions of fully dynamic security (BSZ$^+$) is needed.

[11] This weakness is due to the fact that without a zero knowledge proof, it is challenging to provide anonymity for a signature even following the theft of a signer's key material.

Table 2: A comparison of several group signature constructions, where n is the group size. *Setting* and *Assumption* indicate the cryptographic setting and hardness assumptions based on which the scheme's security is based. *Signature* and *Verification time* represent an approximate estimate (based on the paper) of the signature size in bits and the number of dominant operations ($\mathbb{G}_{exp}$ is group exponentiation and p is bilinear pairing; Groth-Sahai (GS) is a proof of knowledge) used in signature verification. $>$ indicates verification is lower-bounded by this operation. *Group* indicates whether the groups are static or dynamic, and whether they achieve weaker or stronger notions than BMW/BSZ. *Security* indicates the security model. The security parameter is indicated by λ.

Reference	Setting	Assumption	Signature (bits)	Verification	Group Model	Security Model
BS04 [BS04]	Pairing	q-Strong DH+DLIN	1792	$9{*}\mathbb{G}_{exp}{+}5{*}p$	BMW$^-$	ROM
LLLS13 [LLLS13]	Lattice	SIS+LWE	O(λ^2log(n))	-	BMW	ROM
BDKLP22 [BDK$^+$23]	Lattice	MSIS/MLWE	4000log(n) + 687200	-	BSZ$^+$	ROM
BDKLP22 [BDK$^+$23]	Isogeny	CSIDH-512	4800log(n) + 24000	-	BSZ$^+$	ROM
PS16 [PS16]	Pairing	LRSW + DDH	1024	$3p$+ $2\mathbb{G}_{exp}$	BSZ$^-$	ROM+GG
DS18 [DS18]	Pairing	SXDH+DDH+co-CDHI	3309	$5p$+ $6\mathbb{G}_{exp}$	BSZ	ROM+GG
BW06a [BW06]	Pairing	CDH + Subgroup DH	O(log(n))	(2log(n) + 3)$*p$	BMW	SM
ADM03 [AdM03]	Pairing	Strong LRSW + SXDH + EDH	3072	-	BSZ$^-$	SM
BHS19 [BHSB19]	Pairing	DDH+BDDH	13056	>GSVerify	BSZ$^+$	SRS

4 Ring Signatures

Ring Signatures were first named as a distinct cryptographic primitive by Rivest, Shamir and Tauman [RST01], although similar interactive protocols were described in earlier works (*e.g.,* by Cramer *et al.* [CDS94]). Ring signatures are reminiscent of group signatures, but allow the signer to construct an arbitrary *ad-hoc* group each time she signs a message. Unlike a group signature, ring signatures do not feature a group manager to construct the group, nor do they (canonically) include a tracing capability. Instead, the signer produces a ring signature by first selecting a set of public keys that includes the signer's own public key. She then uses these public keys, together with her secret key, to generate a signature on an arbitrary message. The verifier receives the set of public keys, and should learn only that the the signature was created by one key from the group.

A fundamental property of a ring signature is that a signer can create a signature on behalf of a chosen group *without* coordinating or asking permission of any other party, including the other group members. This facilitates a number of privacy applications. For example, Rivest *et al.* [RST01] proposed using ring signatures to deniably leak secrets from an organization; such a signature would reveal that the message was produced by an organization member, without revealing the precise identity of the leaker. More recently, several cryptocurrencies have sought to use ring signatures to facilitate confidential transactions [Sab13, Noe15] in which the actual signer of a transaction hides herself among a set of possible transaction authors.

There are many ring signature variants, and each offers different features. Informally, all ring signatures are expected to satisfy at least the following properties:

- **Correctness:** Any honestly generated ring signature should be considered valid by any verifier.

- **Unforgeability:** Adversaries should have negligible probability of forging a ring signature. Here forgery is defined as producing a ring signature for a message m and ring R without the signer being a member of R. Unforgeability must hold even when the adversary can adaptively choose messages and groups to obtain ring signatures on.

- **Anonymity:** All adversaries (who may be other ring members) should have at a most negligible advantage in identifying the true signer.

4.1 Formal definitions

A standard ring signature scheme comprises three (possibly) probabilistic algorithms:[12]

- $\mathsf{KeyGen}(1^\lambda)$. On input a security parameter λ, outputs a keypair pk, sk.
- $\mathsf{RSign}((pk_1, \ldots, pk_n), j, sk_j, m)$: Given a set of public keys $(pk_1, \ldots, pk_n)$, a message m and the index j and secret key of the signer sk_j, outputs a ring signature σ.
- $\mathsf{RVerify}((pk_1, \ldots, pk_n), m, \sigma)$: On input a set of public key $(pk_1, \ldots, pk_n)$, a signature σ and a message m, outputs 1 if the signature is valid and 0 otherwise.

The security and correctness definitions for ring signatures have been evolving, despite the fact that they remain relatively simpler than the corresponding definitions for group signatures. We omit formal definitions for unforgeability and correctness, as in most cases definitions are a relatively straightforward adaptation of the corresponding definitions for standard signatures. Rivest *et al.* offered an initial definition for anonymity, termed *basic anonymity.* This definition (formalized by Bender *et al.* [BKM06]) states that the signature itself should reveal no information (or a negligible amount of information) about which signer constructed the message, even when secret keys are available to the adversary – under the condition that all keypairs are honestly generated.[13]

A limitation of the Rivest *et al.* definition is that it holds only in an environment where all members generate their keypairs honestly. Bender *et al.* [BKM06] pointed out that a malicious group member could generate a keypair dishonestly, such that it would be impossible for the group member to be a signer. This is a real possibility in the decentralized ring signature setting, where there is no group manager to check the validity of public keys. To address this, Bender *et al.* proposed stronger definitions that allow an attacker to generate keys according to any (possibly dishonest) key generation algorithm while remaining secure, provided there are at least two honest users in the ring. Bender also proposed security against *attribution attacks*, which consider the possibility that all secret keys for a group (plus all random coins used in signature generation) might be leaked to an adversary. Later Park *et al.* [PS19] provide stronger formalism of repudability and claimability, providing black-box transformations for existing ring signatures and new schemes that meet these definitions.

As pointed out in [Gon19], most ring signatures schemes and definitions do not explicitly consider whether they rely on erasures for unforgeability. This is especially important if the security proof has a NIZK simulator answer all signing queries. Since the challenger cannot efficiently compute randomness that explain the simulated NIZK arguments as real arguments, they may have to pretend the random coins of a corrupted user have been erased in order for the security proof to work out.

4.2 Illustrative Example

We assume the existence of a one way function a secure digital signature scheme (**DS.Gen**, **DS.Sign**,**DS.Verify**), and a non-interactive zero knowledge proof of knowledge scheme **NIZKPoK**.

- $\mathsf{KeyGen}(1^\lambda)$.
  - Output $\mathbf{DS.Gen}(1^\lambda) \to (pk, sk)$.
- $\mathsf{RSign}((pk_1, \ldots, pk_n), j, sk_j, m)$:

[12] Some ring signatures also require a global Setup algorithm that generates a common reference string (CRS). We omit this here.

[13] Although Rivest's construction provided information-theoretic anonymity, computationally secure definitions are also possible.

  - Use the **NIZKPoK** to generate a proof π for the following statement: $\{(pk_j, sk_j) : pk_j \in \{pk_1, ..., pk_n\} \wedge \mathbf{DS.Verify}(pk_j, m, \mathbf{DS.Sign}(sk_j, m)) = 1\}$
  - Output $\sigma = (\pi)$.

- $\mathsf{RVerify}((pk_1, \ldots, pk_n), m, \sigma)$:
  - Verify the proof π and output the result,

As we can see from this example, the essence of a ring signature is a zero knowledge proof that the signer knows a signing key pair whose public key is a member of the provided set of keys. The focus for building ring signatures has been on how to leverage efficient proofs of membership as well as how to prove knowledge of a corresponding secret to some public key. As membership proofs depend on the size of the group, this leads to a focus on minimizing the asymptotic costs of the signature size and verification time.

4.3 Evolution of constructions

Ring signature constructions have developed through several phases. The original paper of Rivest *et al.* [RST01] proposed a general construction based on a *combining function*, which is a family of keyed functions that work to create a dependency on all n public keys of the ring. Any member of the ring should have the ability to properly compute the combining function. The construction of Rivest *et al.* [RST01] can be instantiated with any one-way permutation (and concretely, RSA) while providing perfect anonymity in the basic anonymity model.

The following year, Abe *et al.* [AOS02] proposed *separable ring signatures* in which the signers need not agree on the specific type of signature scheme they use. Abe *et al.*'s construction is based on a disjunction zero knowledge/ witness indistinguishable proof of knowledge of a signature that satisfies an instance of the verification algorithm. Abe *et al.*'s work proposed efficient proofs for both DL-type and RSA signatures. Universal ring signatures [BDW23] extend this notion where the ring signature is compatible with all digital signature schemes.

A major focus of this work is on concrete and asymptotic efficiency, largely measured by the size of a ring signature. Much of the work in this area was realized using bilinear pairings. For example, Boneh *et al.* [BGLS03] proposed an efficient short ring signature scheme (though with a signature linear in the ring size), and several related and improved linear-size constructions were proposed subsequently [BKM06, CLWY06, Boy07, SS10]. Notable among these constructions are some that provide security without relying on the random oracle model, such as the work of [CLWY06] and Shacham and Waters [SW07], among others [SS10].

Some more recent work has focused on reducing the size of a ring signature to be sublinear in the number of group members. A common approach to this task is to use an *accumulator* to collect the set of all public keys, and to use a zero knowledge (or witness indistinguishable) proof system to prove knowledge of a membership witness in this accumulator. The efficiency of this construction depends on the accumulator and proof system. This paradigm led to the first constant-sized ring signature construction by Dodis *et al.* [DKNS04], which relied on a specific RSA-based accumulator and proof (due to Camenisch and Lysyanskaya [CL02a]) that rely on the random oracle model for security. Using a new proof system in the discrete log setting, Groth and Kohlweiss's later realized a concretely efficient technique with $log(n)$-sized signatures [GK15] (though also in the random oracle model). Later work [LPQ18] improves on their proofs with a tighter reduction.

Without the use of random oracles, results have been more limited. Chandran *et al.* realized a $O(\sqrt{N})$-sized signature in 2007 [CGS07]; Gonzalez improved this signature size to $O(\sqrt[3]{n})$ [Gon19]. Most recently, Malavolta and Schröder proposed an efficient *constant-sized* group signature in the CRS model based on zkSNARKs [MS17], with a standard model construction relying on the non-falsifiable L-KEA assumption. Backes *et al.* [BHKS18, BDH$^+$19] builds the $log(n)$-sized signatures in the standard model without non-falsifiable assumptions. Haque *et al.* [HKSS22] constructs the first $log(n)$-sized threshold ring signatures in standard model.

A related line of work has sought to apply ring signatures to concrete applications. While these new ring signatures repeat many earlier ideas, they seek to develop optimized constructions that fit to specific applications, such as *confidential transactions* for cryptocurrency systems. These signatures include the CryptoNote protocol [Sab13, Noe15] as well as the "Borromean" ring signatures of Maxwell and Poelstra [MP15], in which the statement proven is a monotone boolean function of the signing keys. Triptych [NG20] builds on this to construct $log(n)$-sized linkable ring signatures for use in RingCT style systems. Similarly, Liu *et al.* [LNY$^+$19] introduce the notion of linkable ring signatures with stealth addresses.

Finally, several recent works have developed lattice-based ring signatures. For example, Brakerski and Kalai laid the groundwork for lattice-based ring signatures [BK10], and more recently Libert *et al.* developed an much more efficient $log(n)$-sized ring signature based on an efficient hash-based accumulator [LLNW16]. While still far from concretely efficient, there is a great deal of followup work for post-quantum ring signatures in the lattice [EZS$^+$19, ESZ22, ESLL19, CCLM22, CGH$^+$21, YEL$^+$21, LNS21], code-based [ZLC07, BM19, BM18], isogeny [BKP20], and symmetric key [KKW18, DRS18, GGHAK22] settings. Chatterjee *et al.* [CCLM22] adapts the post-quantum security notion for plain signatures, blind-unforgeability, for the ring signature setting.

Comparing constructions. Figure 3 compares many representative ring signature constructions drawn from the literature.

Takeaways. To date the most examined, deployed, and accessible ring signature schemes are the ROM constructions with signature size linear in the ring size in the vein of [Sab13, Noe15, LWW04]. For large ring sizes, the log-sized Dualring [YEL$^+$21] ring signatures may be preferable. Other efficient schemes in the setting such as AOS02 [AOS02] require accessible implementations. Linear verification times, even for schemes with sublinear signature sizes, continue to be a roadblock. Many ring signatures with sublinear signature sizes have large overheads hurting their concrete efficiency.

5 Implementations of Privacy-Preserving Signatures

As part of our systematization, we evaluated several public open-source implementations of privacy-preserving signature schemes. This process is necessarily more limited than we desire because many implementations were not functional or were incompatible with newer hardware and operating systems. We present our findings here and in Tables 5, 6 so that a list of functional implementations, albeit of research/proof-of-concept code, can serve others as a reference.

For blind signature scheme variants, we've used the IRTF's RSA Blind Signature draft [DJW23] and accompanying code[14] and an implementation[15] of [LWW04]. For group signatures, a library from IBM[16] offered us a variety of recent schemes, from which we could select two variants albeit it did not compile out-of-the-box and we had to use a modified fork of the code[17]. Ring signatures had a lot of available implementations. We

[14] https://github.com/cfrg/draft-irtf-cfrg-blind-signatures
[15] https://github.com/rot256/pblind
[16] https://github.com/IBM/libgroupsig/wiki/Supported-schemes
[17] https://github.com/n1ckl0sk0rtge/libgroupsig

Table 3: A comparison of several ring signature constructions, where n is the size of the ring. *Setting* and *Assumption* indicate the cryptographic setting and hardness assumptions the scheme's security is based on. *Signature* and *Verification time* represent an approximate estimate (based on the paper) of the signature size in bits and the number of dominant operations ($\mathbb{G}_{exp}$ is group exponentiation, p is bilinear pairing; ZAP, Groth-Sahai (GS), NIZK, NIWI, and SNARKS (SK) are proofs of knowledge) used in signature verification. Schemes marked with an asterisk have addition assumptions and costs due to the use of a proof system. $>$ indicates verification is lower-bounded by this operation. *Security* indicates the security model. While we found all of the schemes listed here did not require erasures, only schemes marked with a † explicitly discuss erasures.

Reference	Setting	Assumption	Signature (bits)	Verification	Security Model
AOS02 [AOS02]	DL	DL	256*n + 256	$\mathbb{G}_{exp}$*n*5/4	ROM
YELAD21 [YEL+21]	DL	DL	1024 + 512log(n)	(n + 2log n + 1)$\mathbb{G}_{exp}$	ROM
DKNS04 [DKNS04]	RSA	RSA+DL	38400	21*RSA_{enc}	ROM
BGLS03 [BGLS03]	Pairing	CDH	256*n	p*(n + 1)	ROM
BKP20 [BKP20]	Lattice	M-LWE+M-SIS	4,000log(n) + 232000	-	ROM
LNS21 [LNS21]	Lattice	Ex-M-LWE+ M-SIS	2320log(n) + 118000	-	ROM
GGHK22 [GGHAK22]	Symmetric-key	OWF	348000 + log(n)	NIZK.verify	ROM
ZLC07 [ZLC07]	Code-based	SD	144 + 126n	(n+1)h	ROM
BKP20 [BKP20]	Isogeny	CSIDH-512	log(n) + 21600	-	ROM
SW07 [SW07]	Pairing	CDH+SubD	512*n + 512	p*(2*n + 3)	SRS
MS17 [MS17]	Pairing	q-SDH+SXDH+SQROOT	3072	2*p+ $\mathbb{G}_{exp}$+ SK_{Verify}	SRS
González19 [Gon19]	Pairing	SXDH	$5031\sqrt[3]{n} + 4608$	$(8n^{2/3} + 122*\sqrt[3]{n} + 94)p$	SRS†
BDHKS19 [BDH+19]	DL*	DDH*	$512\log(n)^2 + 512\log(n) + 1024 + \pi_{NIWI}$	>NIWI.verifiy	SM
BKM06 [BKM06]	Trapdoor	Trapdoor	$3072*n^2$ + ZAP	ZAP_{verify}	SM
BKM06* [BKM06]	Pairing	CDH	512	3*p	SM
YELAD21 [YEL+21]	Lattice	M-LWE+M-SIS	36288 + 208n	-	SM

decided to utilize one implementing Monero's [Noe15] scheme[18][19] and one for [LWW04][20].

We could not compile the following implementations (not necessarily by the authors of the schemes) even after much effort: (i) For blind signatures, this[21] implementation of [TZ22] and this[22] implementation of [HLW23]. (ii) For ring signatures, this [23] implementation of Abe-Ohkubo-Suzuki's [AOS02] linkable ring signatures.

Some cryptographic accumulator variants, such as schemes with the zero-knowledge property can be viewed as a way to privately authenticate identity, much like anonymous credentials. While zero-knowledge accumulators are fast for private authentication, most of them require a trusted party for setup, making it an unfair comparison.

Overall, it's clear that while there are many open-source options, these resources require careful evaluation and, at times, substantial modification to function appropriately.

6 Deploying in Practice

Privacy-preserving authentication has a number of applications. In this section, we discuss several current or potential applications that use or are suitable for these primitives. The focus of this section is primarily on applications that are currently receiving industry attention or seeing large-scale deployment.

6.1 Software Attestation

Many trusted hardware applications have begun to deploy *anonymous software attestation* primitives as a means to authenticate messages sent by an application running within trusted hardware. A software attestation scheme allows an application to issue a signed

[18] https://github.com/noot/ring-go
[19] Monero recently upgraded to using the CLSAG signatures of [GNB19]
[20] https://github.com/fernandolobato/ecc_linkable_ring_signatures
[21] https://github.com/codahale/blind
[22] https://github.com/b-wagn/Raichoo
[23] https://github.com/sdiehl/aos-signature

Table 4: Functionality Reference Table: The properties these various primitives achieve. See Appendix D for detailed explanations of the properties and comparisons. *Note:* These properties are not mutually exclusive and there exist schemes that combine multiple properties, such as the linkable threshold ring signatures of [GN18]. ●: Yes, ○: No.

Primitive	Variant	Schemes	Link	Revoke	Restrict	Repudiate	Trace
Blind Signatures	Plain	Table 1	○	○	○	○	○
	Fair	[SPC95, AO01, HT07, FV10, RS10]	●	●	○	○	●
	Partial	[AF96, AO00a, KLX23]	○	○	●	○	●
	Restrictive	[Bra93b]	○	○	●	○	○
Group Signatures	Plain	Table 2	●	●	○	○	●
	Selective-linkability	[GL19, FGL21, DL21]	●	○	○	○	○
	Threshold	[CDL$^+$20]	●	●	●	○	●
Ring Signatures	Plain	Table 3	○	○	○	○	○
	Linkable	[LWW04, Noe15, NG20, LNY$^+$19]	●	○	○	○	○
	Threshold	[BSS02, HKSS22, HS20, AHAN$^+$22, ABF23]	○	○	●	○	○
	Accountable/ Revocable	[XY04, BCC$^+$16b, FLL$^+$21]	○	●	○	○	●
	Deniable/ Repudiable	[Nao02, KOSK06, PS19, LW22]	○	○	○	●	○

Table 5: Experiments on Privacy-preserving Authentication: We ran the following experiment using existing, working implementations of group and ring signature schemes: *i*) Take groups of size $2^5, 2^{10}, 2^{15}, 2^{20}$ *ii*) Use the signature scheme to set up the group and sign as one of the members *iii*) Compare Setup, Signing, Verification times, Size of Signature, and Public keys. Setup time refers to the scheme dependent one-time cost of generating the scheme parameters, which we include here for completeness to give a thorough overview of practical efficiency of these schemes. As this is a one time cost it was not included as a important point of comparison for tables 1 to 3. We note that the techniques of [CG18] can be used to compress the public key size for the ring signature schemes in certain settings. None of the schemes here require a trusted setup. err denotes that the experiment failed with a memory error. Experiments run on an Apple M1 Pro machine, 16GB RAM.

Group Size	Scheme Variant	Setup Time (ms)	Signing Time (ms)	Verification Time (ms)	Signature Size (Bytes)	Key Size (Bytes)
2^5	GS_1 [BBS04]	4.81	2.26	3.17	2984	17200
	GS_2 [PS16]	1.61	1.52	3.38	1416	2832
	RS_1 [Noe15]	0.67	6.74	6.40	2144	1024
	RS_2 [LWW04]	2264.23	2269.12	2296.75	1028	2048
2^{10}	GS_1 [BBS04]	4.88	2.26	3.16	2984	17200
	GS_2 [PS16]	1.62	1.53	3.38	1416	2832
	RS_1 [Noe15]	16.24	205.75	204.30	65632	32768
	RS_2 [LWW04]	76945.15	76924.15	77231.88	8856	65536
2^{15}	GS_1 [BBS04]	4.91	2.26	3.16	2984	17200
	GS_2 [PS16]	1.75	1.53	3.41	1416	2832
	RS_1 [Noe15]	521.61	6601.28	6552.50	2086752	1048576
	RS_2 [LWW04]	3154590	3201831	3299360	252374	2097152
2^{20}	GS_1 [BBS04]	4.93	2.26	3.18	2984	17200
	GS_2 [PS16]	1.76	1.53	3.39	1416	2832
	RS_1 [Noe15]	15005.48	188362.08	187881.13	66787064	33554432
	RS_2 [LWW04]	~hours	~hours	~hours	err	67108864

message that asserts to the following: (1) the message attested to by the application is authentic (signed), (2) the application is a legitimate instance of a specific application running within a trusted hardware module, and (3) that various other conditions of the software are met.

Anonymous attestation extends the above scheme by requiring that the identity of the attesting device should not be discernible from an attestation signature. This use-case is compelling to manufacturers, who are concerned about the possibility that an

Table 6: Comparing the efficiency of an RSA based vs EC based blind signature scheme.

Scheme	Setup Time (ms)	Signing (ms)	Verification (ms)	Signature Size (Bytes)	Key Size (Bytes)
BS_1 [DJW23] (RSA)	6146	119.1	1.4	384	384
BS_2 [AO00a] (EC based)	0.10	0.34	0.12	128	32

attestation key might be used as a form of hardware identifier – allowing software to cryptographically "fingerprint" the hardware that it runs on. To address this concern, manufacturers have deployed two anonymous attestation schemes in products: Direct Anonymous Attestation (DAA) [BL07], which was included in the Trusted Platform Module 2.0 specification [TPM14]; and Intel's Enhanced Privacy ID (EPID) system [BL07], which is deployed in Intel's Software Guard Extensions (SGX) platform [sgx16].

Each of these systems implements what is effectively an anonymous credential system. In DAA, the machine owners configure the group manager, while in EPID the Intel Corporation acts as the group manager. DAA provides for revocation, but only in the event that a TPM private key is extracted and published widely. By contrast, the EPID system operates as a group signature scheme based on the Boneh *et al.* construction [BBS04]: an authorized tracing authority can recover the identity of a signer given only a valid attestation signature. SGX's implementation of EPID also provides an optional *linkable* mode for the signature, wherein two distinct signatures from the same device can be compared and detected [sgx16]. EPID, as described in the academic publication of [BL07], also provides *verifier local revocation.*

Open problems. A key limitation of the current EPID design is that revocation of individual devices appears to be somewhat costly. The exact details of Intel's system are difficult to determine, as there have been unspecified changes from the published version of EPID [BL07] to the deployed version in SGX. However, this published version indicates that for an r-sized revocation list the EPID signatures will have an $O(r)$ size and verification time. Perhaps because this is not scalable to a worldwide deployment, Intel appears to have settled on a centralized client-server revocation system in which attestations are made to an Intel server, which performs an (efficient) revocation check and then forwards a signature. Given the importance of remote attestation systems, we believe that analyzing and improving this system are important future directions for researchers.

6.2 Anonymity in Cryptocurrency

The introduction of Bitcoin [Nak12] has inspired a significant amount of privacy research. This work is motivated by cryptocurrencies typically employing a public ledger called a *blockchain* to store transactions between participants. Because the ledger contents are world-readable, the transaction graph can be analyzed, and information about payments may be extracted. Many commercial enterprises have developed tools to identify transactions and payment flows in Bitcoin and other currencies [Ell13, Blo14, Cha15].

One proposed approach to anonymizing cryptocurrencies is to use ring signatures to authenticate new transactions [MGGR13, Sab13, Noe15]. The overall approach is as follows. To spend the output of a previous transaction using sk, the transaction author gathers together a collection of k "cover" transaction outputs (from many different transactions). The transaction author now uses a ring signature to prove that the new transaction contains a signature on sk or one of the other secret keys associated with the cover transactions. This provides a form of k-anonymity for transactions. In systems such as Zerocoin and Zerocash [MGGR13, SCG$^+$14], the size of k is set to include all previous transactions (with constant-sized transaction size), while in systems such as CryptoNote [Sab13, Noe15] with linear-size signatures the size is much smaller. Inputs of different values are handled by either mixing equal-value tokens, or by using commitments and zero-knowledge proofs to hide the value from outside parties.

Open problems. There are several open problems in this area. Protocols such as Zerocoin and Zerocash provide constant-sized transactions with a maximal k, but require a *trusted setup* phase that develops a complex (non-random) common reference string. It remains an open problem to construct practical and sublinear-size ring signatures that do not require trusted setup and use standard assumptions. Additionally, while there are multiple, reportedly efficient, proof systems [BBHR18, GLS+20, COS20] that are post-quantum secure, there is no notable effort to implement them towards enhancing and future-proofing anonymity in cryptocurrencies.

6.3 Anonymous identification systems

A number of private efforts are underway to develop and deploy anonymous credential systems. U-Prove [PZ11] is a commercial anonymous credential system currently being developed by Microsoft. U-Prove uses a protocol developed by Brands to produce lightweight, single-show anonymous credential that can be used for identity management applications. U-Prove has an API available to developers, though it has struggled to find any adoption [Bri10]. Additionally, Baldimtsi and Lysyanskaya [BL13b] demonstrated that the underlying blind signature of U-Prove [Bra93a] could not be proven unforgeable in the random oracle model, though in [BL13a] they introduce a similarly efficient anonymous identification protocols with provable security.

Open problems. Unfortunately many anonymous credential schemes used in practice continue to lack provable security guarantees. This includes an ad-hoc anonymous credential scheme using an anonymity set of Ethereum addresses and proof of knowledge of signatures [Tiw23] used by many privacy-focused blockchain applications today. To the best of our knowledge, in blockchain applications, the ad-hoc schemes are deployed without consideration for cryptographic proofs of security. Notably, multiple proof of knowledge of signature schemes will heuristically use hash functions as random oracles in a non-black box fashion. Efforts to formalize security proofs in this direction can attempt to utilize new formalizations such as the arithmetized [CCG+23] or pseudo-random [JLLW23] oracle models to prove security.

6.4 Vehicle-to-vehicle communications

Vehicle-to-Vehicle (V2V) communication technology allows cars, trucks and motorcycles to communicate via short-range wireless radio. V2V promises to dramatically improve safety by providing detailed information about nearby vehicles, including the exact position and speed of each vehicle on a roadway. By monitoring this information, communications-enabled cars can notify the driver of a dangerous condition and/or take automated action to avoid a crash.[24]

Deployment of V2V technology raises concerns related to security, privacy and driver safety. Critical among these is the resilience of V2V systems to *malicious* transmissions, including the broadcasting of erroneous messages designed to harm drivers or create unsafe traffic conditions. In tandem with these security concerns, V2V designers must also address potential concerns regarding driver privacy: specifically that V2V transmissions could be used to uniquely identify and track vehicles, either individually or at large scale.

In 2014 the U.S. National Highway Traffic Safety Administration (NHTSA) proposed a framework called the Security Credential Management System (SCMS) [H+14]. SCMS is a projected \$4 billion USD identity management system that uses digital signatures to authenticate V2V messages, and suggests techniques for protecting vehicle privacy. The

[24] A related technology known as Vehicle-to-Infrastructure (V2I) allows a similar form of communication with infrastructure such as traffic lights and toll systems.

technology is rapidly proceeding to deployment: General Motors has begun to include V2V technology in 2017 Cadillac sedans [Ple17].

The SCMS system can be viewed as a weak anonymous credential system that incorporates many engineering design tradeoffs. Instead of using a multi-show credential system, users must be provisioned with several thousand individual X.509 certificates. Rather than use a blind signature protocol, SCMS breaks the public key infrastructure into two distinct authorities in the SCMS backend, the Pseudonym Certificate Authority and the Registration Authority. Pseudonym Certificate Authority will only know that a vehicle is requesting certificates, but not what those certificates look like. Registration Authority knows what the individual certificates look like, but has no idea which certificates belong to which vehicle. Provided that both components do not collude, this protects the users from being tracked by insiders. SCMS also mandates a verifier-local revocation system: because each user has many certificates that must all be revoked, the deployed system defines a complex system based on hash chains: this allows revocation of a large number vehicle certificates using a single short seed, which introduces storage cost considerations for revocation data. In the worst case, if vehicles do not have enough storage to hold the expanded revocation data they will incur a a verification time linear in the number of revocations. Most critically from a privacy perspective, because the number of certificates obtained is low, users must *re-use* certificates for many distinct authentications – providing for the possibility that they will be linked.

Open problems. The large-scale deployment of anonymous credentials to a vehicle communication network is an important practical development. However, the choice of primitives for the SCMS system indicates that industry does not view the current credential literature as efficient enough, in terms of signature size, verification time, and revocation cost, for deployment at scale. This motivates the development of anonymous credential systems that can compete favorably on concrete runtime and bandwidth cost.

6.5 Revocation

As revocation is a crucial property of privacy-preserving authentication, we briefly cover state-of-the-art approaches for revocation (and direct readers to [KMPQ23] for a more detailed treatment). *Signature lists* approaches [NFHF10, LV09, LPY12a, LPY12b] involve a publicized revocation list that a signer can prove they are not listed on. While these approaches can be expensive for the prover and introduce revocation lists, [AEHS14] introduces an scheme with constant size revocation lists. *Verifier-local revocation* [BS04, LV09] has been a popular approach for offloading costs to the verifier, leading to extremely efficient revocation though still requiring revocation lists and well as weaker privacy guarantees. One benefit is these schemes avoid membership proofs that are bound to the current state of a changing list. Finally, *Accumulator* approaches to revocation [CL02b] allow for efficient and extremely compressed membership proofs. A drawback of this approach was the need to update the witness whenever the revocation list changed. However, recent work [BCD$^+$17] improves on this with a scheme that only requires witness updates on deletions (which are likely far rarer than additions for revocation lists).

7 Future directions in research

In this work, we have attempted to survey and systematize the research around privacy-preserving authentication. While this work is by no means complete, we provided a taxonomy of authentication schemes as well as an overview of the security properties of these protocols. The research in this area leaves a number of open questions. Chief among these are questions related to practice, which we discussed in §6: in particular, problems related to signing efficiency in applications such as cryptocurrency, and revocation efficiency for applications such as software attestation and vehicle-to-vehicle communications. . Additionally, open-source implementations only are available for a small fraction of schemes, primarily older schemes in the ROM setting. Finally, while the adoption of these technologies is promising, the development of practical quantum computing poses a threat to most of the existing "efficient" constructions of these schemes, particularly ring and group signatures. This motivates the development of efficient signatures based in quantum-resistant settings. Unfortunately, at present all of these techniques produces signatures that are orders of magnitude larger than the most efficient pairing-based constructions. Resolving this efficiency differential so that we may continue to support current applications is a well-motivated open problem.

Acknowledgements

Alishah Chator was supported in part by a project with the Massachusetts Executive Office of Labor and Workforce Development. Pratyush Ranjan Tiwari was supported by the Ethereum Foundation's grant FY23-1087, and partly supported by a Security and Privacy research gift from Google, a research gift from Cisco. The authors would like to additionally acknowledge support from the NSF under awards CNS-2209194, CNS-1955172, CNS-1653110, and CNS-1801479 and DARPA under Contract No. HR001120C0084, a Security and Privacy research award from Google. Any opinions, views, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government, DARPA, or its affiliates, or other sponsors.

References

[AAHJ21] Nabil Alkeilani Alkadri, Patrick Harasser, and Christian Janson. Blindor: an efficient lattice-based blind signature scheme from or-proofs. In *Cryptology and Network Security: 20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings 20*, pages 95–115. Springer, 2021. doi:10.1007/978-3-030-92548-2_6.

[ABC22] Arasu Arun, Joseph Bonneau, and Jeremy Clark. Short-lived zero-knowledge proofs and signatures. In *ASIACRYPT*, 2022. doi:10.1007/978-3-031-22969-5_17.

[ABF23] Gennaro Avitabile, Vincenzo Botta, and Dario Fiore. Extendable threshold ring signatures with enhanced anonymity. In *Public-Key Cryptography–PKC 2023: 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7–10, 2023, Proceedings, Part I*, pages 281–311. Springer, 2023. doi:10.1007/978-3-031-31368-4_11.

[ACHDM05] Giuseppe Ateniese, Jan Camenisch, Susan Hohenberger, and Breno De Medeiros. Practical group signatures without random oracles. *Cryptology ePrint Archive*, 2005. URL: https://eprint.iacr.org/2005/385.

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *CRYPTO '00*, 2000. doi:10.1007/3-540-44598-6_16.

[AdM03] Giuseppe Ateniese and Breno de Medeiros. Efficient group signatures without trapdoors. In *ASIACRYPT '03*, 2003. doi:10.1007/978-3-540-40061-5_15.

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In *Advances in Cryptology—EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28–May 2, 2002 Proceedings 21*, pages 83–107. Springer, 2002. doi:10.1007/3-540-46035-7_6.

[AEHS14] Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai. A revocable group signature scheme from identity-based revocation techniques: Achieving constant-size revocation list. In *Applied Cryptography and Network Security: 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings 12*, pages 419–437. Springer, 2014. doi:10.1007/978-3-319-07536-5_25.

[AF96] Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, 1996. doi:10.1007/bfb0034851.

[AHAN$^+$22] Diego F Aranha, Mathias Hall-Andersen, Anca Nitulescu, Elena Pagnin, and Sophia Yakoubov. Count me in! extendability for threshold ring signatures. In *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, pages 379–406. Springer, 2022. doi:10.1007/978-3-030-97131-1_13.

[AKSY22] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. Practical, round-optimal lattice-based blind signatures. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 39–53, 2022. doi:10.1145/3548606.3560650.

[AO00a] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, 2000. doi:10.1007/3-540-44598-6_17.

[AO00b] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings 20*, pages 271–286. Springer, 2000. doi:10.1007/3-540-44598-6_17.

[AO01] Masayuki Abe and Miyako Ohkubo. Provably secure fair blind signatures with tight revocation. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, 2001. doi:10.1007/3-540-45682-1_34.

[AOS02] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, 2002. doi:10.1007/3-540-36178-2_26.

[AW04] Michel Abdalla and Bogdan Warinschi. On the minimal assumptions of group signature schemes. In *Information and Communications Security: 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004.*

Proceedings 6, pages 1–13. Springer, 2004. doi:10.1007/978-3-540-30191-2_1.

[BBCF20] Olivier Blazy, Laura Brouilhet, Céline Chevalier, and Neals Fournaise. Round-optimal constant-size blind signatures. In *ICETE (2)*, pages 213–224, 2020. doi:10.5220/0009888702130224.

[BBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.*, 2018. https://eprint.iacr.org/2018/046.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *CRYPTO '04*, volume 3152 of LNCS, pages 45–55, 2004. doi:10.1007/978-3-540-28628-8_3.

[BCC04] Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004. doi:10.1145/1030083.1030103.

[BCC$^+$09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In *CRYPTO*, 2009. doi:10.1007/978-3-642-03356-8_7.

[BCC$^+$16a] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth. Foundations of fully dynamic group signatures. In *Applied Cryptography and Network Security: 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, pages 117–136. Springer, 2016. doi:10.1007/978-3-319-39555-5_7.

[BCC$^+$16b] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on ddh. In *Computer Security–ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, pages 243–265. Springer, 2016. doi:10.1007/978-3-319-24174-6_13.

[BCD$^+$17] Foteini Baldimtsi, Jan Camenisch, Maria Dubovitskaya, Anna Lysyanskaya, Leonid Reyzin, Kai Samelin, and Sophia Yakoubov. Accumulators with applications to anonymity-preserving revocation. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 301–315. IEEE, 2017. doi:10.1109/eurosp.2017.13.

[BCG$^+$23] Gabrielle Beck, Arka Rai Choudhuri, Matthew Green, Abhishek Jain, and Pratyush Ranjan Tiwari. Time-deniable signatures. *Proc. Priv. Enhancing Technol.*, 2023(3):79–102, 2023. doi:10.56553/popets-2023-0071.

[BCN$^+$10] Patrik Bichsel, Jan Camenisch, Gregory Neven, Nigel P Smart, and Bogdan Warinschi. Get shorty via group signatures without encryption. In *Security and Cryptography for Networks: 7th International Conference, SCN*, 2010. doi:10.1007/978-3-642-15317-4_24.

[BD19] Nir Bitansky and Akshay Degwekar. On the complexity of collision resistant hash functions: New and old black-box separations. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I 17*, pages 422–450. Springer, 2019. doi:10.1007/978-3-030-36030-6_17.

[BDF$^+$11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology–ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings 17*, pages 41–69. Springer, 2011. doi:10.1007/978-3-642-25385-0_3.

[BDH$^+$19] Michael Backes, Nico Döttling, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Ring signatures: logarithmic-size, no setup—from standard assumptions. In *Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38*, pages 281–311. Springer, 2019. doi:10.1007/978-3-030-17659-4_10.

[BDK$^+$23] Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: generic, simple, and efficient. *Designs, Codes and Cryptography*, pages 1–60, 2023. doi:10.1007/s10623-023-01192-x.

[BDW23] Pedro Branco, Nico Döttling, and Stella Wohnig. Universal ring signatures in the standard model. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*, pages 249–278. Springer, 2023. doi:10.1007/978-3-031-22972-5_9.

[BFM19] Manuel Blum, Paul Feldman, and Silvio Micali. *Non-interactive zero-knowledge and its applications*, page 329–349. Association for Computing Machinery, New York, NY, USA, 2019. doi:10.1145/3335741.3335757.

[BFPV13] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Short blind signatures. In *Journal of Computer Security*, 2013. doi:10.3233/jcs-130477.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *Proceedings of Eurocrypt '03*, volume 2656 of LNCS, pages 416–432, 2003. doi:10.1007/3-540-39200-9_26.

[BGSS17] O. Blazy, P. Gaborit, J. Schrek, and N. Sendrier. A code-based blind signature. In *2017 IEEE International Symposium on Information Theory (ISIT)*, 2017. doi:10.1109/isit.2017.8007023.

[BHKS18] Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Signatures with flexible public key: Introducing equivalence classes for public keys. In *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part II*, pages 405–434. Springer, 2018. doi:10.1007/978-3-030-03329-3_14.

[BHSB19] Michael Backes, Lucjan Hanzlik, and Jonas Schneider-Bensch. Membership privacy for fully dynamic group signatures. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2181–2198, 2019. doi:10.1145/3319535.3354257.

[BK10] Zvika Brakerski and Yael Tauman Kalai. A framework for efficient signatures, ring signatures and identity based encryption in the standard model. *IACR*

Cryptol. ePrint Arch., page 86, 2010. URL: http://eprint.iacr.org/2010/086.

[BKM06] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. *Theory of Cryptography, Third Theory of Cryptography Conference, TCC*, 2006. doi:10.1007/11681878_4.

[BKP20] Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II*, pages 464–492. Springer, 2020. doi:10.1007/978-3-030-64834-3_16.

[BL07] Ernie Brickell and Jiangtao Li. Enhanced privacy ID: A Direct Anonymous Attestation scheme with enhanced revocation capabilities. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, 2007. doi:10.1109/tdsc.2011.63.

[BL13a] Foteini Baldimtsi and Anna Lysyanskaya. Anonymous credentials light. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1087–1098, 2013. doi:10.1145/2508859.2516687.

[BL13b] Foteini Baldimtsi and Anna Lysyanskaya. On the security of one-witness blind signature schemes. In *ASIACRYPT*, 2013. doi:10.1007/978-3-642-42045-0_5.

[BLL$^+$22] Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova. On the (in) security of ros. *Journal of Cryptology*, 35(4):25, 2022. doi:10.1007/s00145-022-09436-0.

[Blo14] Blockchain Analysis. Chainalysis. http://www.chainanalysis.com/, 2014.

[BM18] Pedro Branco and Paulo Mateus. A code-based linkable ring signature scheme. In *Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings 12*, pages 203–219. Springer, 2018. doi:10.1007/978-3-030-01446-9_12.

[BM19] Pedro Branco and Paulo Mateus. A traceable ring signature scheme based on coding theory. In *Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers 10*, pages 387–403. Springer, 2019. doi:10.1007/978-3-030-25510-7_21.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT 2003*, 2003. doi:10.1007/3-540-39200-9_38.

[BN05] Paulo SLM Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *International Workshop on Selected Areas in Cryptography*. Springer, 2005. doi:10.1007/11693383_22.

[BNPS03] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The one-more-rsa-inversion problems and the security of chaum's blind signature scheme. In *Journal of Cryptology*, volume 16, 2003. doi:10.1007/s00145-002-0120-1.

[Bol03] Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography PKC*, 2003. doi:10.1007/3-540-36288-6_3.

[Bow17] Sean Bowe. Switch from bn254 to bls12-381. GitHub issue, 2017. Available at: https://github.com/zcash/zcash/issues/2502.

[Boy07] Xavier Boyen. Mesh signatures: How to leak a secret with unwitting and unwilling participants. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 210–227. Springer, 2007. doi:10.1007/978-3-540-72540-4_12.

[BP97] Niko Barić and Birgit Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In *EUROCRYPT '97*, volume 1233 of LNCS, pages 480–494, 1997. doi:10.1007/3-540-69053-0_33.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93. ACM, 1993. doi:http://doi.acm.org/10.1145/168588.168596.

[Bra83] Gilles Brassard. Relativized cryptography. *IEEE Transactions on Information Theory*, 29(6):877–894, 1983. doi:10.1109/tit.1983.1056754.

[Bra93a] Stefan Brands. An efficient on-line electronic cash system based on the representation problem. Technical report, CWI, 1993. URL: https://dl.acm.org/doi/10.5555/869454.

[Bra93b] Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, 1993. doi:10.1007/3-540-48329-2_26.

[Bra00] Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, USA, 2000. doi:10.7551/mitpress/5931.001.0001.

[Bri10] Peter Bright. Microsoft open-sources clever U-Prove identity framework. Available at https://arstechnica.com/information-technology/2010/03/microsoft-open-sources-clever-u-prove-identity-framework/, March 2010.

[BS04] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *CCS*, pages 168–177, 2004. doi:10.1145/1030083.1030106.

[BSS02] Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold ring signatures and applications to ad-hoc groups. In *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings*, pages 465–480. Springer, 2002. doi:10.1007/3-540-45708-9_30.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The case of dynamic groups. In *CT-RSA '05*, 2005. doi:10.1007/978-3-540-30574-3_11.

[BW06] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In *EUROCRYPT '06*, 2006. doi:10.1007/11761679_26.

[CAHL+22] Rutchathon Chairattana-Apirom, Lucjan Hanzlik, Julian Loss, Anna Lysyanskaya, and Benedikt Wagner. Pi-cut-choo and friends: Compact blind signatures via parallel instance cut-and-choose and more. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part III*, pages 3–31. Springer, 2022. doi:10.1007/978-3-031-15982-4_1.

[CCG+23] Megan Chen, Alessandro Chiesa, Tom Gur, Jack O'Connor, and Nicholas Spooner. Proof-carrying data from arithmetized random oracles. In *Advances in Cryptology - EUROCRYPT*, 2023. doi:10.1007/978-3-031-30617-4_13.

[CCLM22] Rohit Chatterjee, Kai-Min Chung, Xiao Liang, and Giulio Malavolta. A note on the post-quantum security of (ring) signatures. In *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, pages 407–436. Springer, 2022. doi:10.1007/978-3-030-97131-1_14.

[CCRR18] Ran Canetti, Yilei Chen, Leonid Reyzin, and Ron D Rothblum. Fiat-shamir and correlation intractability from strong kdm-secure encryption. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part I 37*, pages 91–122. Springer, 2018. doi:10.1007/978-3-319-78381-9_4.

[CDH16] Jan Camenisch, Manu Drijvers, and Jan Hajny. Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, 2016. doi:10.1145/2994620.2994625.

[CDL+20] Jan Camenisch, Manu Drijvers, Anja Lehmann, Gregory Neven, and Patrick Towa. Short threshold dynamic group signatures. In *Security and Cryptography for Networks: 12th International Conference, SCN 2020, Amalfi, Italy, September 14–16, 2020, Proceedings*, pages 401–423. Springer, 2020. doi:10.1007/978-3-030-57990-6_20.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO '94*, volume 839 of LNCS, pages 174–187, 1994. doi:10.1007/3-540-48658-5_19.

[CE87] David Chaum and Jan-Hendrik Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In *Advances in Cryptology — CRYPTO' 86: Proceedings*, 1987. doi:10.1007/3-540-47721-7_10.

[CeA10] Jan Camenisch and et Al. Specification of the identity mixer cryptographic library. Technical report, IBM Research - Zurich, 2010. URL: https://dominoweb.draco.res.ibm.com/eeb54ff3b91c1d648525759b004fbbb1.html.

[CG18] Alishah Chator and Matthew Green. How to squeeze a crowd: reducing bandwidth in mixing cryptocurrencies. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 40–49. IEEE, 2018. doi:10.1109/eurospw.2018.00012.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 2004. doi:10.1145/1008731.1008734.

[CGH$^+$21] Rohit Chatterjee, Sanjam Garg, Mohammad Hajiabadi, Dakshita Khurana, Xiao Liang, Giulio Malavolta, Omkant Pandey, and Sina Shiehian. Compact ring signatures from learning with errors. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 282–312. Springer, 2021. doi:10.1007/978-3-030-84242-0_11.

[CGS07] Nishanth Chandran, Jens Groth, and Amit Sahai. Ring signatures of sublinear size without random oracles. In *Automata, Languages and Programming, 34th International Colloquium, ICALP 2007, Wroclaw, Poland, July 9-13, 2007, Proceedings*, 2007. doi:10.1007/978-3-540-73420-8_38.

[Cha82] David Chaum. Blind signatures for untraceable payments. In *CRYPTO '82*, pages 199–203. Plenum Press, 1982. doi:10.1007/978-1-4757-0602-4_18.

[Cha83] David Chaum. Blind signature system. In *Advances in Cryptology: Proceedings of CRYPTO*, 1983. doi:10.1007/978-1-4684-4730-9_14.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 1985. doi:10.1145/4372.4373.

[Cha88] David Chaum. Blinding for unanticipated signatures. In *EUROCRYPT' 87*, 1988. doi:10.1007/3-540-39118-5_21.

[Cha04] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, 2:38–47, 2004. doi:10.1109/msecp.2004.1264852.

[Cha15] Chainalysis. Chainalysis inc. https://chainalysis.com/, 2015.

[CKM$^+$23] Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. Snowblind: A threshold blind signature in pairing-free groups. In *Annual International Cryptology Conference*, pages 710–742. Springer, 2023. doi:10.1007/978-3-031-38557-5_23.

[CKW04] Jan Camenisch, Maciej Koprowski, and Bogdan Warinschi. Efficient blind signatures without random oracles. In *SCN '04*, volume 3352 of LNCS, pages 134–148, 2004. doi:10.1007/978-3-540-30598-9_10.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT '01*, volume 2045 of LCNS, pages 93–118, 2001. doi:10.1007/3-540-44987-6_7.

[CL02a] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *CRYPTO '02*, 2002. Extended Abstract. URL: http://cs.brown.edu/~anna/papers/camlys02.pdf, doi:10.1007/3-540-45708-9_5.

[CL02b] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *CRYPTO '02*, pages 61–76, 2002. doi:10.1007/3-540-45708-9_5.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Advances in Cryptology – CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings*, 2004. doi:10.1007/978-3-540-28628-8_4.

[CL06] Melissa Chase and Anna Lysyanskaya. On signatures of knowledge. In *Advances in Cryptology-CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings 26*, pages 78–96. Springer, 2006. doi:10.1007/11818175_5.

[CLWY06] Sherman S. M. Chow, Joseph K. Liu, Victor K. Wei, and Tsz Hon Yuen. Ring signatures without random oracles. *ASIACCS*, 2006. doi:10.1145/1128817.1128861.

[CM98] Jan Camenisch and Markus Michels. A group signature scheme with improved efficiency. In *ASIACRYPT '98*. Springer Berlin Heidelberg, 1998. doi:10.1007/3-540-49649-1_14.

[COS20] Alessandro Chiesa, Dev Ojha, and Nicholas Spooner. Fractal: Post-quantum and transparent recursive proofs from holography. In *Advances in Cryptology - EUROCRYPT 2020*, 2020. doi:10.1007/978-3-030-45721-1_27.

[CP92] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In *CRYPTO '92*, volume 740 of LNCS, pages 89–105, 1992. doi:10.1007/3-540-48071-4_7.

[CP94] Lidong Chen and Torben P. Pedersen. New group signature schemes (extended abstract). In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, 1994. doi:10.1007/BFb0053433.

[CPS95] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology — EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings*, 1995. doi:10.1007/bfb0053458.

[CPS07] Ran Canetti, Rafael Pass, and Abhi Shelat. Cryptography from sunspots: How to use an imperfect reference string. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 249–259. IEEE, 2007. doi:10.1109/focs.2007.70.

[CS97] Jan Camenisch and M. Stadler. Efficient group signature schemes for large groups. In *CRYPTO '97*, volume 1296 of LNCS, pages 410–424, 1997. doi:10.1007/bfb0052252.

[CVH91] David Chaum and Eugène Van Heyst. Group signatures. In *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, 1991. doi:10.1007/3-540-46416-6_22.

[Den02] Alexander W Dent. Adapting the weaknesses of the random oracle model to the generic group model. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 100–109. Springer, 2002. doi:10.1007/3-540-36178-2_6.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976. doi:10.1109/tit.1976.1055638.

[DJW23] Frank Denis, Frederic Jacobs, and Christopher A. Wood. RSA Blind Signatures. Internet-Draft draft-irtf-cfrg-rsa-blind-signatures-12, Internet Engineering Task Force, 2023. Work in Progress. URL: https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/12/, doi:10.17487/rfc9474.

[DKNS04] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, 2004. doi:10.1007/978-3-540-24676-3_36.

[DL21] Jesus Diaz and Anja Lehmann. Group signatures with user-controlled and sequential linkability. In *Public-Key Cryptography–PKC 2021: 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10–13, 2021, Proceedings, Part I*, pages 360–388. Springer, 2021. doi:10.1007/978-3-030-75245-3_14.

[dPK22] Rafael del Pino and Shuichi Katsumata. A new framework for more efficient round-optimal lattice-based (partially) blind signature via trapdoor sampling. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, pages 306–336. Springer, 2022. doi:10.1007/978-3-031-15979-4_11.

[DPLS18] Rafaël Del Pino, Vadim Lyubashevsky, and Gregor Seiler. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 574–591, 2018. doi:10.1145/3243734.3243852.

[DRS18] David Derler, Sebastian Ramacher, and Daniel Slamanig. Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives. In *Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings 9*, pages 419–440. Springer, 2018. doi:10.1007/978-3-319-79063-3_20.

[DS18] David Derler and Daniel Slamanig. Highly-efficient fully-anonymous dynamic group signatures. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 551–565, 2018. doi:10.1145/3196494.3196507.

[Ell13] Elliptic. Elliptic enterprises limited. https://www.elliptic.co/, 2013.

[ELL$^+$15] Martianus Frederic Ezerman, Hyung Tae Lee, San Ling, Khoa Nguyen, and Huaxiong Wang. A provably secure group signature scheme from code-based assumptions. In *ASIACRYPT '15*, 2015. doi:10.1007/978-3-662-48797-6_12.

[ELL$^+$20] Martianus Frederic Ezerman, Hyung Tae Lee, San Ling, Khoa Nguyen, and Huaxiong Wang. Provably secure group signature schemes from code-based assumptions. *IEEE Transactions on Information Theory*, 66(9):5754–5773, 2020. doi:10.1109/tit.2020.2976073.

[ESLL19] Muhammed F Esgin, Ron Steinfeld, Joseph K Liu, and Dongxi Liu. Lattice-based zero-knowledge proofs: new techniques for shorter and faster constructions and applications. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I*, pages 115–146. Springer, 2019. doi:10.1007/978-3-030-26948-7_5.

[ESZ22] Muhammed F Esgin, Ron Steinfeld, and Raymond K Zhao. Matrict+: More efficient post-quantum private blockchain payments. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1281–1298. IEEE, 2022. doi:10.1109/sp46214.2022.9833655.

[EZS+19] Muhammed F Esgin, Raymond K Zhao, Ron Steinfeld, Joseph K Liu, and Dongxi Liu. Matrict: efficient, scalable and post-quantum blockchain confidential transactions protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 567–584, 2019. doi:10.1145/3319535.3354200.

[FGL21] Ashley Fraser, Lydia Garms, and Anja Lehmann. Selectively linkable group signatures—stronger security and preserved verifiability. In *Cryptology and Network Security: 20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings*, pages 200–221. Springer, 2021. doi:10.1007/978-3-030-92548-2_11.

[FHKS16] Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model from weaker assumptions. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, 2016. doi:10.1007/978-3-319-44618-9_21.

[Fis06] Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In *Advances in Cryptology - CRYPTO*, 2006. doi:10.1007/11818175_4.

[FKL18] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part II 38*, pages 33–62. Springer, 2018. doi:10.1007/978-3-319-96881-0_2.

[FLL+21] Hanwen Feng, Jianwei Liu, Dawei Li, Ya-Nan Li, and Qianhong Wu. Traceable ring signatures: general framework and post-quantum security. *Designs, Codes and Cryptography*, 89:1111–1145, 2021. doi:10.1007/s10623-021-00863-x.

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *CRYPTO '97*, volume 1294 of LNCS, pages 16–30, 1997. doi:10.1007/bfb0052225.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986. doi:10.1007/3-540-47721-7_12.

[FS10] Marc Fischlin and Dominique Schröder. On the impossibility of three-move blind signature schemes. In *Advances in Cryptology – EUROCRYPT*, 2010. doi:10.1007/978-3-642-13190-5_10.

[FTY96] Yair Frankel, Yiannis Tsiounis, and Moti Yung. "indirect discourse proof": Achieving efficient fair off-line e-cash. In *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, 1996. doi:10.1007/bfb0034855.

[FV10] Georg Fuchsbauer and Damien Vergnaud. Fair blind signatures without random oracles. In *AFRICACRYPT*, 2010. doi:10.1007/978-3-642-12678-9_2.

[GGHAK22] Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk. Efficient set membership proofs using mpc-in-the-head. *Proceedings on Privacy Enhancing Technologies*, 2022(2):304–324, 2022. doi:10.2478/popets-2022-0047.

[GGM14] Christina Garman, Matthew Green, and Ian Miers. Decentralized anonymous credentials. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*, 2014. URL: http://www.internetsociety.org/doc/decentralized-anonymous-credentials, doi:10.14722/ndss.2014.23253.

[Gha17] Essam Ghadafi. Efficient round-optimal blind signatures in the standard model. In *Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*, pages 455–473. Springer, 2017. doi:10.1007/978-3-319-70972-7_26.

[GHK06] David Galindo, Javier Herranz, and Eike Kiltz. On the generic construction of identity-based signatures with additional properties. In *Advances in Cryptology – ASIACRYPT 2006*, 2006. doi:10.1007/11935230_12.

[GK15] Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, 2015. doi:10.1007/978-3-662-46803-6_9.

[GL19] Lydia Garms and Anja Lehmann. Group signatures with selective linkability. In *Public-Key Cryptography–PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I 22*, pages 190–220. Springer, 2019. doi:10.1007/978-3-030-17253-4_7.

[GLS$^+$20] Alexander Golovnev, Jonathan Lee, Srinath T. V. Setty, Justin Thaler, and Riad S. Wahby. Brakedown: Linear-time and post-quantum snarks for R1CS. In *Advances in Cryptology - CRYPTO 2023*, 2020. doi:10.1007/978-3-031-38545-2_7.

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing*, 17(2):281–308, 1988. doi:10.1137/0217017.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC '87*, pages 218–229, 1987. doi:10.1145/3335741.3335755.

[GN18] Brandon Goodell and Sarang Noether. Thring signatures and their applications to spender-ambiguous digital currencies. Cryptology ePrint Archive, Paper 2018/774, 2018. URL: https://eprint.iacr.org/2018/774.

[GNB19] Brandon Goodell, Sarang Noether, and Arthur Blue. Concise linkable ring signatures and forgery against adversarial keys. Cryptology ePrint Archive, Paper 2019/654, 2019. URL: https://eprint.iacr.org/2019/654.

[Gon19] Alonso González. Shorter ring signatures from standard assumptions. In *Public-Key Cryptography–PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I*, pages 99–126. Springer, 2019. doi:10.1007/978-3-030-17253-4_4.

[GPS08] Steven D Galbraith, Kenneth G Paterson, and Nigel P Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008. doi:10.1016/j.dam.2007.12.010.

[GRS+11] Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh. Round optimal blind signatures. In *CRYPTO*, 2011. doi:10.1007/978-3-642-22792-9_36.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT '08*, volume 4965 of LNCS, pages 415–432, 2008. doi:10.1007/978-3-540-78967-3_24.

[H+14] Thorsten Hehn et al. Vehicle safety communications security studies: Technical design of the security credential management system. Final report, Crash Avoidance Metrics Partnership and National Highway Traffic Safety Administration (NHTSA), 2014. URL: https://downloads.regulations.gov/NHTSA-2015-0060-0004/attachment_2.pdf.

[Han23] Lucjan Hanzlik. Non-interactive blind signatures for random messages. In *Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, pages 722–752. Springer, 2023. doi:10.1007/978-3-031-30589-4_25.

[HKLN20] Eduard Hauck, Eike Kiltz, Julian Loss, and Ngoc Khanh Nguyen. Lattice-based blind signatures, revisited. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40*, pages 500–529. Springer, 2020. doi:10.1007/978-3-030-56880-1_18.

[HKSS22] Abida Haque, Stephan Krenn, Daniel Slamanig, and Christoph Striecks. Logarithmic-size (linkable) threshold ring signatures in the plain model. In *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, pages 437–467. Springer, 2022. doi:10.1007/978-3-030-97131-1_15.

[HLW23] Lucjan Hanzlik, Julian Loss, and Benedikt Wagner. Rai-choo! evolving blind signatures to the next level. In *Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, pages 753–783. Springer, 2023. doi:10.1007/978-3-031-30589-4_26.

[HS20] Abida Haque and Alessandra Scafuro. Threshold ring signatures: new definitions and post-quantum security. In *Public-Key Cryptography–PKC 2020: 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4–7, 2020, Proceedings, Part II 23*, pages 423–452. Springer, 2020. doi:10.1007/978-3-030-45388-6_15.

[HT07] Emeline Hufschmitt and Jacques Traoré. Fair blind signatures revisited. In *Pairing-Based Cryptography - Pairing 2007, First International Conference, Tokyo, Japan, July 2-4, 2007, Proceedings*, 2007. doi:10.1007/978-3-540-73489-5_14.

[HW21] Andreas Hülsing and Florian Weber. Epochal signatures for deniable group chats. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 1677–1695, 2021. doi:10.1109/sp40001.2021.00058.

[Imp95] Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147. IEEE, 1995. doi:10.1109/sct.1995.514853.

[JLLW23] Aayush Jain, Huijia Lin, Ji Luo, and Daniel Wichs. The pseudorandom oracle model and ideal obfuscation. In *Advances in Cryptology - CRYPTO*, 2023. doi:10.1007/978-3-031-38551-3_8.

[JLO97] Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures (extended abstract). In *CRYPTO '97*, volume 1294 of LNCS, pages 150–164, 1997. doi:10.1007/bfb0052233.

[Jou04] Antoine Joux. A one round protocol for tripartite diffie-hellman. *J. Cryptol.*, 17(4):263–276, 2004. doi:10.1007/s00145-004-0312-y.

[KB16] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In *Advances in Cryptology - CRYPTO*, 2016. doi:10.1007/978-3-662-53018-4_20.

[KKW18] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 525–537, 2018. doi:10.1145/3243734.3243805.

[KLR21] Jonathan Katz, Julian Loss, and Michael Rosenberg. Boosting the security of blind signature schemes. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27*, pages 468–492. Springer, 2021. doi:10.1007/978-3-030-92068-5_16.

[KLX22] Julia Kastner, Julian Loss, and Jiayu Xu. On pairing-free blind signature schemes in the algebraic group model. In *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, pages 468–497. Springer, 2022. doi:10.1007/978-3-030-97131-1_16.

[KLX23] Julia Kastner, Julian Loss, and Jiayu Xu. The Abe-Okamoto partially blind signature scheme revisited. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*, pages 279–309. Springer, 2023. doi:10.1007/978-3-031-22972-5_10.

[KMPQ23] Saqib A. Kakvi, Keith M. Martin, Colin Putman, and Elizabeth A. Quaglia. Sok: Anonymous credentials. In *Security Standardisation Research- SSR*, 2023. doi:10.1007/978-3-031-30731-7_6.

[KNYY21] Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Round-optimal blind signatures in the plain model from classical and quantum standard assumptions. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I 40*, pages 404–434. Springer, 2021. doi:10.1007/978-3-030-77870-5_15.

[KOSK06] Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, and Shinichi Kawamura. Toward the fair anonymous signatures: Deniable ring signatures. In *Topics in Cryptology–CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2005. Proceedings*, pages 174–191. Springer, 2006. doi:10.1007/11605805_12.

[KSY11] Jonathan Katz, Dominique Schröder, and Arkady Yerukhimovich. Impossibility of blind signatures from one-way permutations. In *Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, 2011. doi:10.1007/978-3-642-19571-6_37.

[KY06] Aggelos Kiayias and Moti Yung. Secure scalable group signature with dynamic joins and separable authorities. *Int. J. Secur. Networks*, 1(1/2):24–45, 2006. doi:10.1504/ijsn.2006.010821.

[KY19] Shuichi Katsumata and Shota Yamada. Group signatures without nizk: from lattices in the standard model. In *Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38*, pages 312–344. Springer, 2019. doi:10.1007/978-3-030-17659-4_11.

[Lin03] Yehuda Lindell. Bounded-concurrent secure two-party computation without setup assumptions. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*, 2003. doi:10.1145/780542.780641.

[LLLS13] Fabien Laguillaumie, Adeline Langlois, Benoît Libert, and Damien Stehlé. Lattice-based group signatures with logarithmic signature size. In *ASIACRYPT '13*, 2013. doi:10.1007/978-3-642-42045-0_3.

[LLNW16] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In *EUROCRYPT*, 2016. doi:10.1007/978-3-662-49896-5_1.

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. Efficient lattice-based blind signatures via gaussian one-time signatures. In *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, pages 498–527. Springer, 2022. doi:10.1007/978-3-030-97131-1_17.

[LNPS21] Vadim Lyubashevsky, Ngoc Khanh Nguyen, Maxime Plancon, and Gregor Seiler. Shorter lattice-based group signatures via “almost free” encryption and other optimizations. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27*, pages 218–248. Springer, 2021. doi:10.1007/978-3-030-92068-5_8.

[LNPY21] Benoît Libert, Khoa Nguyen, Thomas Peters, and Moti Yung. Bifurcated signatures: folding the accountability vs. anonymity dilemma into a single private signing scheme. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part III*, pages 521–552. Springer, 2021. doi:10.1007/978-3-030-77883-5_18.

[LNS21] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. Smile: set membership from ideal lattices with applications to ring signatures and confidential transactions. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II*, pages 611–640. Springer, 2021. doi:10.1007/978-3-030-84245-1_21.

[LNWX18] San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Constant-size group signatures from lattices. In *Public-Key Cryptography–PKC 2018: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II 21*, pages 58–88. Springer, 2018. doi:10.1007/978-3-319-76581-5_3.

[LNY$^+$19] Zhen Liu, Khoa Nguyen, Guomin Yang, Huaxiong Wang, and Duncan S Wong. A lattice-based linkable ring signature supporting stealth addresses. In *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24*, pages 726–746. Springer, 2019. doi:10.1007/978-3-030-29959-0_35.

[LPQ18] Benoît Libert, Thomas Peters, and Chen Qian. Logarithmic-size ring signatures with tight security from the ddh assumption. In *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, September 3-7, 2018, Proceedings, Part II 23*, pages 288–308. Springer, 2018. doi:10.1007/978-3-319-98989-1_15.

[LPY12a] Benoît Libert, Thomas Peters, and Moti Yung. Group signatures with almost-for-free revocation. In *Advances in Cryptology–CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, pages 571–589. Springer, 2012. doi:10.1007/978-3-642-32009-5_34.

[LPY12b] Benoît Libert, Thomas Peters, and Moti Yung. Scalable group signatures with revocation. In *Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31*, pages 609–627. Springer, 2012. doi:10.1007/978-3-642-29011-4_36.

[LRSW00] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym systems. In *Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography*, SAC ’99. Springer-Verlag,

2000. URL: http://dl.acm.org/citation.cfm?id=646555.694598, doi:10.1007/3-540-46513-8_14.

[LV09] Benoît Libert and Damien Vergnaud. Group signatures with verifier-local revocation and backward unlinkability in the standard model. In *Cryptology and Network Security: 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings 8*, pages 498–517. Springer, 2009. doi:10.1007/978-3-642-10433-6_34.

[LW22] Hao Lin and Mingqiang Wang. Repudiable ring signature: Stronger security and logarithmic-size. *Computer Standards & Interfaces*, 80:103562, 2022. doi:10.1016/j.csi.2021.103562.

[LWW04] Joseph K Liu, Victor K Wei, and Duncan S Wong. Linkable spontaneous anonymous group signature for ad hoc groups. In *ACISP*, volume 4, pages 325–335. Springer, 2004. doi:10.1007/978-3-540-27800-9_28.

[Mau05] Ueli Maurer. Abstract models of computation in cryptography. In *Cryptography and Coding: 10th IMA International Conference, Cirencester, UK, December 19-21, 2005. Proceedings 10*, pages 1–12. Springer, 2005. doi:10.1007/11586821_1.

[Mer79] Ralph Charles Merkle. *Secrecy, authentication, and public key systems.* Stanford university, 1979. ISBN: 978-0835713849.

[Mer17] Jeremy B. Merrill. Authenticating email using dkim and arc, or how we analyzed the kasowitz emails. https://www.propublica.org/nerds/authenticating-email-using-dkim-and-arc-or-how-we-analyzed-the-kasowitz-emails, 2017.

[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, SP '13, pages 397–411, 2013. doi:10.1109/sp.2013.34.

[MP15] Greg Maxwell and Andrew Poelstra. Borromean ring signatures. Available at https://github.com/Blockstream/borromean_paper, 2015.

[MS17] Giulio Malavolta and Dominique Schröder. Efficient ring signatures in the standard model. In ASIACRYPT '17, 2017. doi:10.1007/978-3-319-70697-9_5.

[MSS98] Markus Michels, Markus Stadler, and Hung-Min Sun. On the security of some variants of the RSA signature scheme. In *Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, September 16-18, 1998, Proceedings*, 1998. doi:10.1007/bfb0055857.

[Nak12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009, 2012. URL: http://www.bitcoin.org/bitcoin.pdf.

[Nao02] Moni Naor. Deniable ring authentication. In *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22*, pages 481–498. Springer, 2002. doi:10.1007/3-540-45708-9_31.

[NFHF10] Toru Nakanishi, Hiroki Fujii, Yuta Hira, and Nobuo Funabiki. Revocable group signature schemes with constant costs for signing and verifying. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 93(1):50–62, 2010. doi:10.1587/transfun.e93.a.50.

[NG20] Sarang Noether and Brandon Goodell. Triptych: logarithmic-sized linkable ring signatures with applications. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2020 International Workshops, DPM 2020 and CBT 2020, Guildford, UK, September 17–18, 2020, Revised Selected Papers 15*, pages 337–354. Springer, 2020. doi:10.1007/978-3-030-66172-4_22.

[NGSY22] Khoa Nguyen, Fuchun Guo, Willy Susilo, and Guomin Yang. Multimodal private signatures. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, pages 792–822. Springer, 2022. doi:10.1007/978-3-031-15979-4_27.

[Noe15] Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptology ePrint Archive*, 2015. URL: https://eprint.iacr.org/2015/1098.

[Oka93] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *Advances in Cryptology — CRYPTO' 92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992 Proceedings*, 1993. doi:10.1007/3-540-48071-4_3.

[Oka06] Tatsuaki Okamoto. Efficient blind and partially blind signatures without random oracles. In *Theory of Cryptography (TCC)*, volume 3876 of LNCS, pages 80–99, 2006. doi:10.1007/11681878_5.

[Ple17] Kelly Pleskot. 2017 Cadillac CTS Now Standard With V2V Technology. Available at http://www.motortrend.com/news/2017-cadillac-cts-now-standard-v2v-technology/, March 2017.

[Poi98] David Pointcheval. Strengthened security for blind signatures. In *Advances in Cryptology — EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques Espoo, Finland, May 31 – June 4, 1998 Proceedings*, 1998. doi:10.1007/bfb0054141.

[Pop16] Nathaniel Popper. Zcash, a Harder-to-Trace Virtual Currency, Generates Price Frenzy. *The New York Times*, 2016. Available at https://www.nytimes.com/2016/11/01/business/dealbook/zcash-a-harder-to-trace-virtual-currency-generates-price-frenzy.html.

[PS96] David Pointcheval and Jacques Stern. Provably secure blind signature schemes. In *ASIACRYPT '96*, volume 1163 of LNCS, pages 252–265, 1996. doi:10.1007/bfb0034852.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000. doi:10.1007/s001450010003.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. In *Topics in Cryptology-CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29-March 4, 2016, Proceedings*, pages 111–126. Springer, 2016. doi:10.1007/978-3-319-29485-8_7.

[PS19] Sunoo Park and Adam Sealfon. It wasn't me! repudiability and claimability of ring signatures. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III 39*, pages 159–190. Springer, 2019. doi:10.1007/978-3-030-26954-8_6.

[PZ11] Christian Paquin and Greg Zaverucha. U-prove cryptographic specification v1. 1, 2011. URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Cryptographic20Specification20V1.1.pdf.

[RS10] Markus Rückert and Dominique Schröder. Fair partially blind signatures. In *Progress in Cryptology – AFRICACRYPT 2010: Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, May 3-6, 2010. Proceedings*, 2010. doi:10.1007/978-3-642-12678-9_3.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, 2001. doi:10.1007/3-540-45682-1_32.

[Sab13] Nicolas van Saberhagen. Cryptonote v 2.0, 2013. URL: https://cryptonote.org/whitepaper.pdf.

[Sat18] Raphael Satter. Emails: Lawyer who met trump jr. tied to russian officials. https://apnews.com/article/4946c3cfaea04ce69a7e5bf2344c4a7a, 2018.

[SCG⁺14] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *IEEE Security and Privacy*, 2014. doi:10.1109/sp.2014.36.

[Sch01] Claus Peter Schnorr. Security of blind discrete log signatures against interactive attacks. In *International Conference on Information and Communications Security*, pages 1–12. Springer, 2001. doi:10.1007/3-540-45600-7_1.

[sgx16] Intel® Software Guard Extensions Remote Attestation End-to-End Example, July 2016. Available at https://software.intel.com/en-us/articles/intel-software-guard-extensions-remote-attestation-end-to-end-example.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology—EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings 16*, pages 256–266. Springer, 1997. doi:10.1007/3-540-69053-0_18.

[SPC95] Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch. Fair blind signatures. In *Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, 1995. doi:10.1007/3-540-49264-x_17.

[SS10] Sven Schäge and Jörg Schwenk. A cdh-based ring signature scheme with short signatures and public keys. In *Financial Cryptography and Data Security: 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers*, 2010. doi:10.1007/978-3-642-14577-3_12.

[SU12] Dominique Schröder and Dominique Unruh. Security of blind signatures revisited. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, 2012. doi:10.1007/978-3-642-30057-8_39.

[SW07] Hovav Shacham and Brent Waters. Efficient ring signatures without random oracles. In *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*, 2007. doi:10.1007/978-3-540-71677-8_12.

[Tiw23] Pratyush Ranjan Tiwari. Private ECDSA verification using zk: Motivation, optimizations & security. Blogpost, 2023. https://blog.bigwhalelabs.com/private-ecdsa-verification-using-zk/.

[TPM14] TPM. TPM Library Specification, October 2014. Available at https://trustedcomputinggroup.org/tpm-library-specification/.

[TVH22] Craig Timberg, Matt Viser, and Tom Hamburger. Here's how the post analyzed hunter biden's laptop. https://www.washingtonpost.com/technology/2022/03/30/hunter-biden-laptop-data-examined/, 2022.

[TZ22] Stefano Tessaro and Chenzhi Zhu. Short pairing-free blind signatures with exponential security. In *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part II*, pages 782–811. Springer, 2022. doi:10.1007/978-3-031-07085-3_27.

[TZ23] Stefano Tessaro and Chenzhi Zhu. Revisiting bbs signatures. In *Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, pages 691–721. Springer, 2023. doi:10.1007/978-3-031-30589-4_24.

[vSN92] Sebastiaan H. von Solms and David Naccache. On blind signatures and perfect crimes. *Comput. Secur.*, 1992. doi:10.1016/0167-4048(92)90193-U.

[XY04] Shouhuai Xu and Moti Yung. Accountable ring signatures: A smart card approach. In *Smart Card Research and Advanced Applications VI: IFIP 18th World Computer Congress TC8/WG8. 8 & TC11/WG11. 2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS) 22–27 August 2004 Toulouse, France*, pages 271–286. Springer, 2004. doi:10.1007/1-4020-8147-2_18.

[Yao86] Andrew Yao. How to generate and exchange secrets. In *FOCS '86*, pages 162–167, 1986. doi:10.1109/sfcs.1986.25.

[YEL+21] Tsz Hon Yuen, Muhammed F Esgin, Joseph K Liu, Man Ho Au, and Zhimin Ding. Dualring: generic construction of ring signatures with efficient instantiations. In *Advances in Cryptology–CRYPTO 2021: 41st*

Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41, pages 251–281. Springer, 2021. doi:10.1007/978-3-030-84242-0_10.

[ZK02] Fangguo Zhang and Kwangjo Kim. Id-based blind signature and ring signature from pairings. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT*, 2002. doi:10.1007/3-540-36178-2_33.

[ZLC07] Dong Zheng, Xiangxue Li, and Kefei Chen. Code-based ring signature scheme. *Int. J. Netw. Secur.*, 5(2):154–157, 2007. URL: http://ijns.jalaxy.com.tw/contents/ijns-v5-n2/ijns-2007-v5-n2-p154-157.pdf.

A Cryptographic Background

A.1 Cryptographic Settings

The schemes in this paper use various cryptographic settings. In the following section we describe these settings at a high level, and then proceed to discuss cryptographic hardness assumptions in these settings.

The RSA Setting. A number of the schemes in discussed in this work are set in a ring of integers modulo $N = pq$, where p and q are prime. While not all of these schemes explicitly use the RSA function, we will generally refer to this class of schemes as the *RSA setting*. Schemes in this setting employ a number of underlying hardness assumptions, including the RSA assumption, quadratic residuosity, factoring, and the Strong RSA assumption [BP97, FO97]. In our estimates of signature size, we will generally consider an RSA ring with $|N| = 3,072$ bits, which at current estimates of security strength, provides approximately 128-bit equivalent security against factorization.

Discrete Logarithm Setting. Some of the schemes we discuss are set in a cyclic group $\mathbb{G}$, typically of prime order q, in which the discrete logarithm problem is assumed to be hard. Except where explicitly noted we will assume that this group $\mathbb{G}$ can be instantiated as either (1) a subgroup within a finite field where, given some modulus p the group operation is defined as modular multiplication, or (2) by instantiating the group as a subgroup of an elliptic curve. Except where explicitly noted, our estimates of signature size will consider the latter setting: specifically a subgroup of order q in a curve over F_p where $|p| = 256$ bits. Appropriately-structured curves of this size are thought to provide 128-bit security against (EC) discrete logarithm attacks. Schemes in this setting employ a number of underlying hardness assumptions, including the (elliptic curve) discrete logarithm and Diffie-Hellman assumptions.

Bilinear Groups Several of the schemes in this work are set in bilinear groups. This setting consist of three (possibly distinct) groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ where g_1 generates $\mathbb{G}_1$, g_2 generates $\mathbb{G}_2$, the groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ each have prime order q, and there exists a *bilinear map* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Bilinear groups have three common instantiations [GPS08, Jou04]. Schemes in the various bilinear settings may rely on various hardness assumptions, ranging from common assumptions such as (computational) Diffie-Hellman to more complex dynamic assumptions. Pairing-friendly curves offer a good balance between security and efficiency. The security of these curves is well-studied [BN05] and is considered to be high enough for practical purposes. Recent optimizations [KB16] of the number field sieve (NFS) algorithm has lowered the concrete security of BN254, resulting in a switch to the BLS12-381 curve for multiple applications [Bow17].

Other settings. While this work is primarily focused on the three efficient settings above, some more recent literature considers alternative settings, such as lattice or coding-based settings. While these settings offer a number of benefits, at present the majority of privacy-preserving schemes in these settings are impractical when compared to the settings above. Where applicable, we discuss these settings; although we do not in all cases provide concrete signature size or verification time estimates for these works. Verification time in particular is difficult to compare for assumptions relying on non-standard cryptographic operations, and in these cases we prioritize providing concrete signature sizes as these tend to be the primary deployment constraint for most of these schemes. The post-quantum cryptography (PQC) setting is also rapidly evolving and it remains to be seen which assumptions stay relevant in the long-term.

Comparing settings. One of the most challenging aspect of comparing different private signature schemes is the variety of different settings that they are constructed in. These settings make use of different cryptographic and mathematical operations and it can feel like comparing apples to oranges. When possible, we try to standardize the comparisons by providing size comparisons in terms of bits and runtime comparisons in terms of common operations like group exponentiation. However, the runtime cost of group exponentiation also depends on the group in question and some schemes use non-standard groups. Additionally, other schemes use operations that can not be cleanly expressed in terms of common operations. In these cases, we note the operation being performed so the reader can decide whether that operation makes sense for their setting. While it is not feasible to do a full overview of comparing the costs of different cryptographic operations in this work, we can briefly outline a hierarchy of efficiency. Generally, elliptic curve group exponentiations are considered cheaper than pairing operations or RSA operations. Schemes requiring NIZK, NIWI, ZAP, SNARK, or Groth-Sahai proofs are considered to have a high communication cost.

Models of computation. Separate to the mathematical setting, many of the schemes discussed in this work include security proofs in various computing models. We now briefly review these models. In the *standard model* (SM) [Bra83], we assume that the adversary is limited in computing time. Several schemes are proven secure in the Random Oracle Model (ROM) [BR93], which assumes the existence of an ideal random (hash) function that can be efficiently evaluated. While proofs in this model provide a useful heuristic, use of this model has been challenged by results showing that schemes proven secure in the random oracle model may be *insecure* when instantiated with concrete functions [CGH04]. In order to account for quantum adversaries the Quantum Random Oracle Model (QROM) [BDF$^+$11] was introduced, where the adversary can query the oracle on quantum states. Another common idealized model is the Generic Group Model (GGM) [Sho97, Mau05], where the adversary is given access to a randomly selected encoding of a group and to an oracle that performs the group operation. However, this model was found to have a similar issue to the random oracle model, where schemes proven secure in GGM may be insecure when the random encoding function for the group is replaced with a specific encoding function [Den02]. The Algebraic Group Model (AGM) [FKL18] was introduced to account for these limitations, allowing for exploitation of the algebraic structure of groups while still limiting how new group elements can be derived. This model is seen as a middle ground between the GGM and SM, where there is currently no evidence it suffers from the same issue as other idealized models like GGM and ROM. A final class of schemes is secure in the Common Reference String (or Common Random String) (CRS) model [BFM19, CPS07], where there exists a trusted reference string generated by a trusted party. We distinguish between the models that use a string sampled uniformly at random (URS) and those that must have some structure based on secret random coins and the secret must be discarded after generation (SRS). The SRS model is more powerful but SRS generation an inherently trusted process. Constructions in the ROM, GGM, AGM, and CRS models are often much more efficient than in the standard model, however it is at the cost of additional assumptions of idealized functionalities or trusted parties. The GGM and AGM additionally do not have the same wide applicability as the ROM or CRS model, as they focus on group-specific algorithms. We identify these models when we discuss specific protocols in this work.

Signatures in Different Security Models. The random oracle model is perhaps the most straightforward model for designing privacy-preserving signatures. This is due to the Fiat-Shamir transform [FS86] enabling the conversion of interactive public-coin proofs into non-interactive proofs. Then, this random oracle can be replaced with a hash function when constructing the scheme. As plain signatures (which can be thought of as a non-interactive proof of identity) and NIZKs are core building blocks for privacy-preserving signatures, this simple approach can yield efficient and easy to analyze schemes.

Designing schemes in the CRS involve finding efficient non-interactive proofs that do not rely on random oracles. These proof systems, such as Groth-Sahai proofs [GS08], tend to be in the pairing setting. Similar to the CRS model, building privacy-preserving signatures in the standard model involves finding efficient non-interactive proofs that are secure in the SM. While there may be generic ways to convert signatures from one model to the others, generally due to the added complexity of proof systems in the SM and CRS models these schemes are often designed and optimized specifically for their settings. However, work on correlation-intractable hash functions [CCRR18] seeks to find ways to instantiate the Fiat-Shamir transform without the need of random oracles, which would open the door to directly lifting some ROM schemes to be secure in the standard model.

A.2 Cryptographic Constructs for Privacy-Preserving Signatures.

The core cryptographic constructs used to build schemes are one-way functions (OWF), one-way permutations (OWP), pseudorandom generators (PRG), pseudorandom functions (PRF), and pseudorandom permutations (PRP). Of note is the fact that one-way functions can be directly used to build these other constructs. There are a variety of cryptographic schemes we can build from just these constructs, the exceptions being public key cryptographic primitives which we only know how to build with the use of additional mathematical assumptions. In the terminology of [Imp95] we refer to set of cryptographic schemes that only require the existence of OWFs as being in *Minicrypt* and those also requiring the existence of public key cryptography as being in *Cryptomania* (where Minicrypt is a subset of Cryptomania).

Plain digital signatures are known to be in Minicrypt, that is they can be built given only the existence of one-way functions. This can be seen through the hash-based Merkle signatures [Mer79], as hash functions are within Minicrypt[25]. However, these schemes are not efficient and as a result most digital signatures use public key primitives in their design. This led to an interest in exploring whether extensions to digital signatures, such as privacy-preserving signatures, can be built purely from one-way functions and its family of constructs.

Existing literature on the topic seems to indicate that privacy-preserving signatures do require additional public key assumptions beyond their plain counterparts. In the case of blind signatures, it was found that they could not be constructed from one-way functions in a black-box way [KSY11]. Group signatures were found to imply the existence of public key encryption [AW04], making the likelihood of basing them solely on one-way functions unlikely. Unlike the other privacy-preserving signatures, ring signatures have neither been found to imply public key encryption nor have had black-box constructions from one-way functions ruled out. However, all existing schemes require assumptions beyond just one-way functions.

[25] Note that Collision Resistant Hash functions are unlikely to be in Minicrypt [BD19]

A.3 Unforgeability and Threat Models

The security of digital signature schemes has a long history of study. In particular, the key threats to these schemes are either *total breaks*, where the secret trapdoor information can be computed, or *forgery attacks*, where valid signatures can be produced without knowledge of the signer's secret information [GMR88]. Additionally, there are a variety of attack settings considered which provide the adversary with differing amounts of power and access. The canonical security notion is *Existential Unforgeability under Adaptive Chosen Message Attacks* (EUF-CMA) [GMR88]. This definition requires that an adversary is unable to produce a valid signature on a message it has not seen a signature for yet, even if it is adaptively able to ask for signatures on messages. There is also a variant of this definition known as *Strong Existential Unforgeability under Adaptive Chosen Message Attacks* (sEUF-CMA) [ADR02], which requires that even if the adversary obtained a signature on a message it still should not be able to produce any other valid signatures for that message.

Privacy-preserving signatures intuitively follow this same notion of security, adversaries should not be able to produce valid signatures without knowledge of the proper secret information. However, the privacy properties of these schemes make the notion of what should be considered a forgery somewhat more involved.

In the case of blind signatures, the standard notion of EUF-CMA does not apply. Blind signature schemes require that the signer does not learn what messages it is producing signatures on. However, for EUF-CMA this information is necessary in order for the reduction to detect if the signature provided by the adversary was a previously issued signature. Instead, blind signatures schemes demonstrate security in terms of *One More Unforgeability* [PS96], where an adversary should not be able to produce $l+1$ valid signatures given l interactions with the signer. Concretely, this enforces that any valid signatures must have originated from the signer. Since blind signature schemes are interactive protocols, unlike plain digital signatures, there is also an additional consideration of concurrent security. Recent work has found that achieving concurrent security against "one more forgery" attacks is nontrivial and that many existing schemes only offer sequential security due to their reliance on the hardness of the ROS (Random inhomogeneities in an Overdetermined Solvable system of linear equations) problem [BLL$^+$22].

As group and ring signatures do not hide which messages are being signed, EUF-CMA applies more directly in these cases, though their privacy properties still require additional security considerations.

Intuitively, EUF-CMA for group signatures requires that an adversary who is not a member of the group (and thus does not know the relevant secret information) cannot produce a valid signature for the group on a message it has not seen a signature on yet. However due to the fundamental requirement that group signatures can be traced to the group member that generated them, there are other attacks to account for. Meaningful unforgeability for group signatures requires that all valid signatures are *traceable*, so an adversary cannot produce a signature whose origin cannot be determined. Relatedly, group signatures must be *non-frameable*, so an adversary cannot produce a valid group signature that traces back to a group member it has not corrupted. Finally, there is an *anonymity* requirement that the adversary should not be able to identify which honest group member generated the group signature. More details about these requirements are provided in Appendix B.

The ad hoc nature of ring signatures creates a slightly different set of considerations compared to group signatures. The EUF-CMA security is required to hold against *insider corruptions* [BKM06]. This requires that even if the adversary can adaptively choose messages and sets of parties to obtain ring signatures on, they should not be able to produce a valid signature for a message with respect to a ring of uncorrupted parties. This avoids trivial attacks where the adversary controls one of the parties in the ring.

An implicit assumption some schemes make is that of *secure erasures* [Gon19], where security against adaptive corruptions only holds if the previous random coins of a corrupted party were erased prior to corruption. Similar to group signatures, ring signatures have an *anonymity* requirement that the adversary cannot determine which party in the ring created a honestly generated ring signature.

B Additional definitions for Group Signatures

The BMW scheme formalized the desired properties of group signatures into the following 3 requirements:

- **Correctness:** Any honestly generated group signature should verify correctly, and should trace correctly.
- **Full-Anonymity:** Even with access to all group member signing keys, an adversary cannot distinguish between the signatures produced by any pair of group members for a chosen message.
- **Full-Traceability:** Any coalition set of forgers (including the group manager) should be unable to produce a signature that does not trace to a member of the coalition.

The BSZ scheme formalized the desired properties of group signatures into 4 requirements:

- **Correctness:** Any honestly generated group signature should be considered valid by any verifier. An honestly generated group signature will open to the identity of the signer. The opener's proof should be accepted by the Judge algorithm (Discussed below). Correctness must hold regardless of when an honest user joins the group.
- **Anonymity:** An adversary cannot distinguish between the signatures produced by any pair of group members for a chosen challenge message without being able to open these signatures.
- **Traceability:** An adversary is unable to produce a valid signature that does not open to their identity without at least partially corrupting the issuer or fully corrupting the opener.
- **Non-frameability:** An adversary is unable to produce an acceptable proof that an honest user produced a group signature unless the user actually did produce it.

The BSZ definition [BSZ05] defines a group signature using the following algorithms and protocols:

- **GKg(1^λ):** Which takes a security parameter λ, and outputs a group public key gpk, an issuer key ik, and an opener key ok.
- **UKg(1^λ):** Which takes a security parameter λ, and outputs a personal public and private key pair $\boldsymbol{upk}[i], \boldsymbol{usk}[i]$ where the vector $\boldsymbol{upk}$ is publicly accessible. All users must run UKg prior to joining the group.
- Join, Iss → $(\boldsymbol{gsk}[i], \boldsymbol{reg}[i])$: An interactive protocol between a user running Join and an Issuer running Iss. If the protocol successfully completes then Join ouputs the user's signing key $\boldsymbol{gsk}[i]$ and Iss makes an entry $\boldsymbol{reg}[i]$) in its table of registered users.
- **GSig(gsk$[i], m$):** Which takes a message m and a group member's secret key $\mathbf{gsk}[i]$, and outputs a group signature σ.

- **GVf(ok, m, σ):** Which takes an opener key ok, message m and a group signature σ and outputs 1 if the signature is valid and 0 otherwise.
- **Open(ok, m, σ):** Which takes a group managers secret key $gmsk$, message m and a group signature σ and uses these plus its read access of the registration table $\boldsymbol{reg}$ to trace the signer. If successful outputs the identity i that produced this signature on this message and a proof of this claim τ, else ouputs $(0, \perp)$.
- **Judge($gpk, j, \boldsymbol{upk}[j], m, \sigma, \tau$):** Which takes a group public key gpk, an identity j, the public key of this entity $\boldsymbol{upk}[j]$, message m a group signature σ, and a proof τ and outputs 1 if τ is a proof that j produced this signature on this message and 0 otherwise.

The division of the group manager into an opener and issuer allows for them to have differing levels of trust. However, this definition can still be applied to a scheme with a single group manager if security requirements are relaxed.

C Anonymous Credentials

Related to the concept of ring and group signatures is a third concept, known generally as an *anonymous credential* system. Anonymous credentials provide a token that a holder can use to demonstrate some property of the holder, without completely revealing their identity. In this sense, they are quite similar to group signatures but offer a more powerful set of functions.

Definition 1 (Anonymous Credentials)**.** An anonymous credential scheme consists of authorized issuer(s)/auditors $\mathcal{I} = \{I_1, \ldots, I_n\}$ and a set of admissible attributes $\mathsf{Att} = \{\mathsf{att}_1, \ldots, \mathsf{att}_L\}$. Each user u obtains a set of attribute values $\mathsf{Att}^u = \{\mathsf{att}_1^u, \ldots, \mathsf{att}_L^u\}$ such that att_i^u is the value of att_i for user u. The following PPT algorithms define an anonymous credential scheme:

- $\mathsf{Setup}(\mathcal{I}, \mathsf{Att}) \rightarrow \mathsf{pp}$: The setup algorithm takes as input the set of authorized issuer(s)/auditors $\mathcal{I}$, a set of admissible attributes Att and outputs the public parameters pp.
- $\mathsf{CredGen}(\mathsf{pp}, \mathsf{Att}^u, \mathcal{P}) \rightarrow \pi_{\mathsf{cred}/\perp}^{\mathcal{P}}$: The credential generation algorithm takes as input the public parameters pp, user attributes Att^u and a policy P and outputs a valid credential $\pi_{\mathsf{cred}}^{\mathcal{P}}$ if the user attributes satisfy the policy, else it outputs $\perp$.
- $\mathsf{CredVerify}(\mathsf{pp}, \mathcal{P}, \pi_{\mathsf{cred}}^{\mathsf{P}}) \rightarrow 0/1$: The credential verification algorithm takes as input the public parameters pp, a credential $\pi_{\mathsf{cred}}^{\mathcal{P}}$ and outputs either 1 if the credential is a valid one, otherwise it outputs 0.

Anonymous credentials were first proposed by Chaum [Cha85, CE87]. In his work, Chaum laid out a method to exchange credentials between organizations without creating a link between the credentials used in different organizations. The original scheme was based on a blind signature protocol, and required a trusted third party. Chaum and Pedersen [CP92] subsequently introduced the idea of a “wallet with observer" to refer to a device that manages credentials in a privacy-preserving way.

This idea was formalized into the notion of a pseudonym system by Lysyanskaya *et al.* [LRSW00]. This notion added important ideas preventing credential sharing among users and limiting the role of the trusted party to initial enrollment. Brands [Bra00] further develops this idea with the separation of credentials into multi-show, linkable (pseudonyms) and limited-show, potentially unlinkable (these are anonymous credentials if only one use, using more than limit will expose secret key) credentials. He also introduced the idea of a certificate blacklist to revoke all credentials of a user.

Credential technology advanced significantly in 2001, when Camenisch and Lysyanskaya [CL01] proposed the first construction of an anonymous credential system with an *unlinkable multi-show credential* as well as a revocation feature. This allowed a user to apply a credential multiple times without revocation, except when abuse was detected and a group manager revoked the user (the underlying primitive is based on group signatures). This idea was generalized to allow for efficient proofs of knowledge on arbitrary signed messages by Camenisch and Lysanskaya [CL04]. The first significant practical application of these anonymous credentials was Direct Anonymous Attestation [BCC04] with usage in Trusted Platform Modules.

Finally, using randomizable zero knowledge, Belenkiy *et al.* [BCC$^+$09] introduced an efficient scheme that allows users to delegate their credentials to others. Garman *et al.* [GGM14] proposed the removal of the trusted issuer by utilizing blockchains. Recently there have been efforts in industry [CeA10, PZ11] to provide feature-rich, practical anonymous credential systems. However, revocation is a significant burden on these systems, and making revocation scalable is currently an area of active research [CDH16]. We refrain from discussing the details of the different variants of anonymous credentials and their security definitions as a recent systematization of knowledge paper [KMPQ23] covers them.

D Overview of Additional Properties

Beyond the plain variants of privacy-preserving signatures, there have been a number of schemes that promise additional properties. Many of these properties serve as a check on the privacy and anonymity guarantees of the underlying primitive in order to stop "Perfect Crimes" as put by [vSN92]. In the following, the *initiator* refers to the party that initiates the generation of the signature (which would be the user for blind signatures and the same as the signer for ring/group signatures). We provide generalized terms for each party as there is some variablilty in the terms used in the literature. *Link*: Linkability refers to the ability to determine whether two signatures had the same initiator involved in their generation. *Revoke*: Revocability is the ability to revoke the initiator's ability generate signatures. *Restrict*: Restrictivity references to the ability to restrict the signature generation in some way (who the initiators are, what messages are allowed, format of the signature). *Repudiate*: Repudiate allows a party to provably deny being the initiator for a specific signature. *Deny*: Deniability allows the initiator to deny involvement in generating a specific signature. *Trace*: Traceability refers to the ability to trace a signature back to the initiator. *Note:* These properties are not mutually exclusive and there exist schemes that combine multiple properties, such as the linkable threshold ring signatures of [GN18].

- **Fair Blind Signatures:** Fair blind signatures involve a judge that is able to link a message-signature pair to the blind signing protocol that generated it (Trace). This linking protocol can be further used to see if two signatures had the same initiator (Link) and disallow that initiator from further blind signing (Revoke).

- **Partial Blind Signatures:** Partial Blind Signatures allow the signer to partially see the message that is being signed (or embed some additional information onto the signature), such as an expiration date or transaction ID. Depending on what this information is, this may allow for limiting the validity of the signature (Restrict) or a mechanism for connecting a signature to a particular blind signing protocol instance (Trace).

- **Restrictive Blind Signatures:** Restrictive Blind Signatures require the message that is being blind signed to follow a specific format. This allows for limits on what types of messages can have blind signatures (Restrict).

- **Plain Group Signatures:** The group management and opening functionality of group signatures means that there are built in mechanisms for tracing the initiator of signatures, revoking group members, and linking signatures from the same initiator.
- **Group Signatures with Selective Linkability:** Selective Linkability restricts the powers of the group manager/other group members, reducing their ability to trace the initiator of a signature to only being able to link multiple signatures that had the same initiator.
- **Threshold Group Signatures:** While Threshold Group Signatures help reduce the dependence on a central authority by converting key generation and opening into distributed protocols, this change in trust model also weakens the anonymity guarantees of these schemes (Restrict).
- **Linkable Ring Signatures:** Linkable Ring Signatures allow one to detect whether multiple signatures were generated by the same initiator (Link).
- **Threshold Ring Signatures:** t-out-of-n Threshold Ring Signatures add a restriction that of the n parties included in the ring signature, at least t of them must be involved in the signature generation. This limits the ability of the initiator to produce signatures without additional approval (Restrict).
- **Accountable/Revocable Ring Signatures:** Accountable/Revocable Ring Signatures include a third-party or some other mechanism to reveal who the initiator of the ring signature was ((Trace). Additionally, once this identity is found, its keys can be revoked (Revoke).
- **Deniable/Repudiable Ring Signatures:** Deniable/Repudiable Ring Signatures have additional capabilities to allow a party to produce a proof that they were not involved in the generation of a signature. Typically, these schemes focus on repudiablilty for parties that were not the initiator but had their public keys included in the ring (Repudiate). However [Nao02] describes a stronger mechanism where authentication can only happen interactively, thus the receiver in the protocol cannot convince anyone else that a member of the ring was involved in the signature generation.

E On deniable signatures.

Another aspect of privacy in digital signatures is that of deniability. The property of cryptographic deniability in this context, allows the signer to disavow authorship of messages, e.g., in the event that they have been leaked or stolen. Digital signatures with a time-deniability property were introduced due to the misuse of email authentication protocols like DKIM. These authentication protocols were introduced to ensure that the receiver can authenticate the identity of the sender. However, they are now being misused as a way to identify and authenticate the sender by a third party. For example, news organizations routinely verify the authenticity of leaked or stolen email collections using DKIM signatures [Sat18, Mer17, TVH22]. To fix these issues a recent line of work [HW21, BCG^{+}23, ABC22] proposed constructions of signature schemes where there is a notion of time-deniability and after a certain amount of time has elapsed, the signature can no longer be attributed to the original signer. These works capture a very important aspect of privacy but are tangential to our systematization on signing without revealing identity or data at any point.