cryptography

MDPI

Article

A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity

Maharage Nisansala Sevwandi Perera [1,*], Toru Nakamura [2], Masayuki Hashimoto [1], Hiroyuki Yokoyama [1], Chen-Mou Cheng [3] and Kouichi Sakurai [4]

[1] Adaptive Communications Research Laboratories, Advanced Telecommunications Research Institute International (ATR), Kyoto 619-0288, Japan; masayuki.hashimoto@atr.jp (M.H.); hr-yokoyama@atr.jp (H.Y.)
[2] KDDI Research, Inc., Saitama 356-8502, Japan; tr-nakamura@atr.jp
[3] Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa 920-1192, Japan; cheng@se.kanazawa-u.ac.jp
[4] Department of Information Science and Technology, Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819-0395, Japan; sakurai@inf.kyushu-u.ac.jp
* Correspondence: perera.nisansala@atr.jp or mnisansalasperera@gmail.com

Abstract: This survey reviews the two most prominent group-oriented anonymous signature schemes and analyzes the existing approaches for their problem: balancing anonymity against traceability. Group signatures and ring signatures are the two leading competitive signature schemes with a rich body of research. Both group and ring signatures enable user anonymity with group settings. Any group user can produce a signature while hiding his identity in a group. Although group signatures have predefined group settings, ring signatures allow users to form ad-hoc groups. Preserving user identities provided an advantage for group and ring signatures. Thus, presently many applications utilize them. However, standard group signatures enable an authority to freely revoke signers' anonymity. Thus, the authority might weaken the anonymity of innocent users. On the other hand, traditional ring signatures maintain permanent user anonymity, allowing space for malicious user activities; thus achieving the requirements of privacy-preserved traceability in group signatures and controlled anonymity in ring signatures has become desirable. This paper reviews group and ring signatures and explores the existing approaches that address the identification of malicious user activities. We selected many papers that discuss balancing user tracing and anonymity in group and ring signatures. Since this paper scrutinizes both signatures from their basic idea to obstacles including tracing users, it provides readers a broad synthesis of information about two signature schemes with the knowledge of current approaches to balance excessive traceability in group signatures and extreme anonymity in ring signatures. This paper will also shape the future research directions of two critical signature schemes that require more awareness.

Keywords: group signatures; ring signatures; user anonymity; user traceability

Citation: Perera, M.N.S.; Nakamura, T.; Hashimoto, M.; Yokoyama, H.; Cheng, C.-M.; Sakurai, K. A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity. *Cryptography* **2022**, *6*, 3. https://doi.org/10.3390/cryptography6010003

Academic Editors: Seyit A. Camtepe and Josef Pieprzyk

Received: 14 December 2021
Accepted: 11 January 2022
Published: 19 January 2022

1. Introduction

This paper is a survey of two prominent group-oriented digital signatures called group signatures and ring signatures, which support user authentication and anonymity. The purpose of this survey is to point out a challenging problem in both signatures and to present existing approaches. For this purpose, this survey reviews more than 100 existing papers from 1991 to 2020 and presents future research requirements.

Group Signatures and *Ring Signatures* are modern cryptographic primitives that have received significant attention from the cryptographic community and other innovation and manufacturing societies since their introductions due to the privacy preserved authentication feature that they provide. In the digital world, where almost every conceivable product and service are available online, user privacy preservation has become the top requirement to fulfill. Since group signatures and ring signatures are among the leading

candidates that satisfy the necessity of preserving user privacy, many applications employ them. Group signatures were first introduced in 1991 by Chaum and van Heyst [1] and ring signatures were first introduced in 2001 by Rivest, Shamir, and Tauman [2].

Group signatures preserve user privacy by allowing users to get themselves verified while hiding their actual identities in a group. Put differently, a user who belongs to a group can generate a signature by representing the group. Thus the signature verifier can validate the signature against a group verification key, but he cannot identify the precise user (signer). We call this user-identity-hiding feature *user anonymity*. However, to prevent users from misusing the nature of user anonymity, group signatures consist of another property called *user traceability*. Traceability allows an authority called a tracer to revoke the anonymity of signatures. Traceability is introduced to identify dishonest users. Thus, group users can enjoy anonymity until the tracing authority locates them. In most cases, the group owner (the group manager) has the authority to identify group users. Many areas employ group signatures in privacy-preserving applications as e-commerce systems, vehicle safety communication (VSC) [3,4], key-card access systems, and anonymous attestation [5].

In contrast to group signature, ring signatures provide permanent user anonymity. Moreover, in ring signatures, users are not fixed to a group. A signer forms an ad-hoc group with selected users when publishing a message. The signer employs other users' public keys without their consent to hide his identity. Generally speaking, a user adds himself to any set that he chooses and produces a signature. Since there is no group setup, there is also no group manager with a unique key who can revoke user anonymity, as in group signature schemes. Thus, if a user, for instance, a senator, can leak internal information to the media without anxiety, his identity can be traced. Since he employs other senators' public keys, including his own, the message receiver knows the source of the information is a senator. That is, the information is trustworthy. However, nobody can identify the signature's origin. Ring signatures show more solid user anonymity than group signatures. The strong user anonymity of ring signatures supports ring signatures for whistleblowing, e-voting, e-cash, e-bidding, and e-lottery. Recently, ring signatures became a prominent candidate for cryptocurrency uses. For instance, Monero, one of the most popular privacy-centric cryptocurrencies, is based on CryptoNote, which employees (linkable) ring signatures to secure a sender's anonymity.

Even though group signatures provide both user anonymity and traceability and ring signatures provide strong user anonymity, both signatures suffer from balanced security properties. In group signatures tracing authority like group manager can cancel the user anonymity. Even though user-traceability supports identifying malicious users, extreme tracing power that the group manager has allows him to observe innocent users. On the other hand, if tracing authority is corrupted, all the users are in danger. In contrast, ring signatures provide strong user anonymity by preventing identification of users. However, this property allows users to issue bogus messages. For instance, users may vote more than once in e-voting systems that developed based on ring signatures as user actions are hidden. Thus it is required to balance the traceability in group signatures and anonymity in ring signatures.

Addressing this problem, many researchers provided controlled tracing mechanisms for group signatures and methods to prevent malicious user actions in ring signatures. Providing well-balanced tracing and anonymity in group and ring signatures while maintaining other features like efficiency is challenging. Even though numerous approaches have addressed this problem, no perfect solution exists. We believe that the user-tracing mechanism in group signatures must be decentralized, controlled, and held accountable. On the other hand, ring signatures must have a prevention method that provides protection against malicious user actions instead of identifying users. No proposed techniques should affect the efficiency of the schemes or harm their concept. For example, since the ring signature is proposed for protecting the user anonymity, in any case the users should not be identified, but their misbehaviors should be defend.

Contribution. In this paper, we survey two group-oriented signatures, group signatures (GS) and ring signatures (RS), which are dominant in the privacy preservation of users. Thus, this survey paper reviews group signature and ring signature schemes including their syntaxes, security definitions, and the development of the two signatures that answer theoretical and practical challenges. Since both signatures have arguable mechanisms for identifying malicious users and preventing their actions, this paper specifically focuses on imbalanced tracing and anonymity features of group signatures and ring signatures. It provides existing mechanisms that address the extreme tracing power in group signatures and the excessive anonymity in ring signatures methods to balance tracing and anonymity in both group signatures and ring signatures. This paper also presents research directions that require attention to apply group signatures and ring signatures in practice. For instance, in the near future we will experience the quantum era during which most existing cryptosystems will be destroyed, including group signature and ring signature schemes. Thus long-term secured group signatures and ring signature schemes must be developed.

The existing survey papers of Agarwal and Saraswat [6] presented several applications of group signatures, and Meiklejohn [7] compared the basics of group and ring signatures. However, neither paper addressed the problems of imbalanced anonymity and the traceability of group signatures and ring signatures nor offered any current solutions for the problem we review.

Organization. The rest of our paper is constructed as follows. We define group signatures, provide related security notions, and current works in Section 2. Following the same structure of Section 2, in Section 3 we detail ring signatures. Next in Section 4, we present the existing mechanisms in group signatures for tracing signers and the existing methods that address user misuses of anonymity in ring signatures. In Section 5, we compare group and ring signatures, explicitly by their tracing mechanisms, and describe the existing challenges in both signatures that should be addressed to improve future applications. In Section 6, we summarize our paper.

2. Group Signatures: Related Works

In group signature schemes, a group has a single verification key called a group public key **gpk**, which is public and used by outside verifiers to validate the signatures of its users. Each group user has her own secret signing key **gsk** with which she generates an anonymous signature for the group. As explained in Chaum and van Heyst's first group signature schemes [1], a group has a manager that holds a special key called a group manager's secret key **gmsk**. This group manager defines his group, and any user in it can generate an anonymous signature on behalf of the group. Moreover, the group manager wields sufficient authority to revoke user anonymity. Thus a group signature scheme is comprised of at least three parties: a group manager, group members (users), and signature verifiers.

We define the group signature scheme provided by Bellare, Micciancio, and Warinschi [8] for static groups.

Definition 1. *A group signature scheme is a tuple of four polynomial-time (PPT) algorithms: KeyGen, Sign, Verify and Open as in Table 1. The parameters $\lambda \in \mathbb{N}$ is the security parameter and $N \in \mathbb{N}$ is the number of group users (members).*

Table 1. Definition of group signatures.

Algorithm	Purpose	Input	Output
KeyGen	Key Generation	1^λ and 1^N	**gpk**, **gmsk**, **gsk**, where **gsk** = $\{\mathbf{gsk}[i]\}_{i\in\{1,\ldots,N\}}$
Sign	Signature Generation	**gpk**, **gsk**[i], M	a signature Σ
Verify	Signature Verification	**gpk**, M, Σ	1 (valid) or 0 (invalid)
Open	Identifying the Signer	**gmsk**, M, Σ	index i of the signer or $\perp$ if the user cannot be traced

2.1. Security Notions

The group signature scheme of Chaum and van Heyst [1] satisfies user anonymity and traceability.

- *Anonymity* requires that no adversary can recover the user's identity from her signature.
- *Traceability* requires that no adversary can forge a signature that cannot be traced.

Moreover, anonymity ensures that nobody can link that two signatures were generated by the same user (unlinkability).

However, with the development and application of group signatures, more security requirements have been raised. For instance, Ateniese et al. [9] presented unforgeability, which prevents users from producing valid signatures for a message without knowing a valid secret signing key. Chen et al. [10] suggested non-frameability, which avoids a group of users generating a signature that traces back to an innocent user. Bellare et al. [8] subsequently presented two strong security notions, *full anonymity* and *full traceability*, which imply all such previously suggested security notions for group signatures: anonymity [1], unlinkability, unforgeability, collusion resistance [9], exculpability [9], and non-frameability [10].

- *Full Anonymity* requires that no adversary can recover a user's identity from her signature even if the adversary corrupts every group member and can access the outcome of the signature opening (except the challenged signature). In other words, signatures generated by two distinct group users are computationally indistinguishable to an adversary who can corrupt every member (including signature-generating members) and who receives the user indices of the signatures that he formed. He cannot request the revealing of the challenged signature.
- *Full Traceability* requires that no adversary can forge a signature, even one produced by a coalition of group users and the group manager, that cannot be traced back to a member of the coalition.

2.2. Current Works

In 1991, Chaum and van Heyst [1] introduced group signatures. Over the past three decades, numerous group signature schemes have been presented to reduce the barriers for use in real life: based on random oracles [9,11–18], without random oracles [19,20], improving security [8,9,21–27], and efficiency [9,12,13,24,28–30].

In their early stages, group signature schemes [1,10,31] showed a notable disadvantage. Since the group public key (verification key) size and the signature size depended on the number of group members, using group signatures in large group settings was unreliable. Camenisch and Stadler [28] answered the public key and signature sizes problem by presenting a group signature scheme in which the sizes of public keys and signatures are independent from the number of group members. On the other hand, early group signatures [32,33], including Camenisch and Stadler's work [28], were based on strong RSA assumptions. Group signatures were next proposed [11,12] based on Strong Diffie-Hellman and Decision Linear assumptions. Unfortunately, those group signature schemes will not be safe after quantum computers become a reality. Thus, lattice-based [25,34] and code-based [35] quantum-safe group signatures were subsequently presented to secure group signatures in the future.

A strand of works focused on the security of group signatures. Among them, discussing security weaknesses in previous group signature schemes, Ateniese and Tsudik [9] and Ateniese et al. [21] presented proven-secure group signature schemes. Answering different security weaknesses in group signatures several security notions were presented, including collusion resistance [9], framing resistance [10], and exculpability [9]. In 2003, Bellare, Micciancio, and Warinschi [8] proposed a security model with two strong security notions called full anonymity and full traceability for group signatures. We explained these two security notions in Section 2.1. Full anonymity and full traceability cover all the previously suggested security notions for group signatures. Besides, Bellare, Mic-

ciancio, and Warinschi [8] gave a generic construction of a group signature scheme for static groups satisfying the introduced security notions. Their scheme's construction combines digital signatures, IND-CCA secure public-key encryption, and non-interactive zero-knowledge proofs.

Bellare's proposal [8] seems to be a perfect design for group signatures. Both the construction and security model (BMW03 model) of Bellare's scheme proved quite advantageous. Since then the construction of most group signatures [12,24,29,36] follows Bellare's scheme. For instance, the first lattice-based group signature scheme against quantum attacks presented by Gorden et al. [25] employed the outline of Bellare's scheme's construction [8]. However, Gorden's lattice-based group signature scheme is for static group settings. Later dynamic group signatures with member registration [13,15,24,37] employed Bellare's scheme. Other than providing member registration, group signature schemes were also proposed with member revocation [29,38–41]. In dynamic group signatures with member registration [24], the group manager's role is divided between an issuer, who manages new user joining, and a tracer, who is a third party that can revoke the anonymity of signatures. Thus, in dynamic group signatures, achieving full traceability is complicated. However, we can achieve non-frameability with a lower level of trust [24]. In dynamic group settings with user joining, we cannot achieve full traceability if a group has a single authority that manages users and identifies signers. Full traceability [8] allows adversaries to corrupt the group manager. In dynamic group signature schemes, if only a group manager is involved in member joining and tracing signers, then an adversary who corrupts the group manager can generate dummy users and produce untraceable signatures. However, since the dynamic group signatures proposed by Bellare et al. [24] separate the key issuing role from the tracing task, we can achieve traceability with a partially corrupted tracer and non-frameability with fully corrupted tracers and issuers.

In addition to security realization, the dynamic group signature scheme [24] doles out the group manager's authority power. Thus, although the group manager (issuer) deals with user joining (or user registration), the tracer identifies the actual signer of a given signature. Even so, in ordinary group signature schemes, the tracer (or the opener) has extreme privilege because she can freely open any signature. We discuss the extreme tracing power held by the tracing manager in group signature schemes and existing approaches to cope this problem in Section 4.

From the above discussion of the background of group signatures, we observe that in static groups, a trusted party generates keys for both authorities (group manager) and group users other than the verification key (group public key). On the other hand, in dynamic settings, only the authorities (issuer and tracer) get keys from a trusted party, and users have the flexibility to select secret keys. With the demand of group signatures, subsequent variants of group signatures [42] were proposed to suit different real-life applications like Attribute-based Group Signatures, Undeniable Group Signatures, and Revocable Group Signatures. For instance, to control the signers through an access structure, Attribute-based Group Signatures (ABGS) [43,44] were presented. Attribute based group signature requires a signer to satisfy a given policy. In undeniable group signatures [22], the group manager's involvement is necessary for signature verification.

The standard group signatures and variants of group signatures are applicable in diverse privacy-preserving systems [6] like e-commerce systems, English auctions, trust computing group (TCG) [45], vehicle safety communication (VSC) [4,46], and electronic tolls.

Even though group signatures appear to be a perfect solution for preserving privacy, their limitations surface when applied in some applications. For instance, the application of group signatures in e-voting systems risks voter's anonymity because any tracing key holder can identify voters. Thus, a new approach must be developed with a user privacy-preserving method where a tracer cannot revoke user anonymity in such systems. Another requirement of such schemes is anonymously disclosing rumors. In 2001, Rivest et al. [2] introduced ring signatures (RS) to address this requirement.

3. Ring Signatures: Related Works

In contrast to group signature schemes, the ring signature schemes introduced by Rivest et al. [2] are setup-free and unconditionally anonymous. Hence they have no key generation algorithm or a tracing algorithm. A ring signature scheme has only two algorithms: Sign for signature generation and Verify for verification. A user with public key $\mathbf{pk}_s$ and secret key $\mathbf{sk}_s$ generates a signature Σ on a message M using a set of another users' public keys without their awareness. When signing, the user forms a group from the public keys of other users and her public key $\mathbf{pk}_1, \ldots, \mathbf{pk}_s, \ldots, \mathbf{pk}_n$. This newly formed group is called a ring (R). The signer forms a ring to be anonymous and sends his signature with the ring to the verifier who can validate that one of the ring members generated it. Even though other ring members' public keys are used for signing, since they are not practically involved, ordinary ring signatures only involve two parties: signer and verifier.

We provide the ring signature scheme defined by Rivest, Shamir, and Tauman [2].

Definition 2. *A ring signature scheme is a tuple of two polynomial time (PPT) algorithms: Sign and Verify as in Table 2.*

Table 2. Definition of ring signatures.

Algorithm	Purpose	Input	Output
Sign	Signature Generation	$R, \mathbf{sk}_s, M$	Σ
Verify	Signature Verification	R, Σ, M	1 (valid) or 0 (invalid)

While maintaining the concept of original ring signatures, KeyGen algorithm is introduced to ring signatures to ensure that all the users have identical keys [47]. Unlike the KeyGen algorithm in group signatures, this KeyGen algorithm is executed by users who want to get public and secret keys.

Definition 3. *A ring signature scheme is a tuple of three polynomial time (PPT) algorithms: KeyGen, Sign, and Verify [47] as in Table 3.*

Table 3. Definition of ring signatures with key generation.

Algorithm	Purpose	Input	Output
KeyGen	Key Generation	security parameter λ	a public and secret key pair $(\mathbf{pk}, \mathbf{sk})$
Sign	Signature Generation	$R, \mathbf{sk}_s, M$	Σ
Verify	Signature Verification	R, Σ, M	1 (valid) or 0 (invalid)

3.1. Security Notions

The ring signature scheme of Riverst et al. [2] presented two (informal) security notions called anonymity and unforgeability.

- *Anonymity* requires that no adversary can recover the signer's identity from a given signature.
- *Unforgeability* requires that no adversary can output a valid signature using a secret key whose associated public key is not in the presented ring.

In 2006, Bender, Katz, and Morselli [47] formally defined anonymity and unforgeability and showed three possible anonymity levels: basic anonymity, anonymity with respect to adversarially chosen keys, and anonymity against full key exposure attacks. By implying those security notions, in 2007, Shacham and Waters [48] presented two strong security notions: *Anonymity (against full key exposure)* and *Unforgeability*.

- *Anonymity (against full key exposure)* requires even though an adversary gets a set of public keys S and allows to access the signing oracle, with any index i and any $R \not\subset S$,

the adversary cannot distinguish the user from two adaptive indices in the given ring R, where $R \not\subset S$ and those challenging indices were not used for querying the signing oracle.

- *Unforgeability* requires that no adversary with given public key set S and access to signing oracle produce a valid forgery signature $\Sigma^* \leftarrow \mathsf{Sign}(R, \mathbf{sk_i}, M^*)$, where $R \not\subset S$ and i is not used for querying the signing oracle.

3.2. Current Works

With the introduction of ring signatures by Riverst et al. [2], numerous related works (along with the related notion of ring/ad-hoc identification schemes) have been proposed [49–59]. We discuss some of them in this section.

In 2001, Riverst et al. [2] proposed ring signatures, which satisfy user anonymity based on the existence of trapdoor permutation. Subsequently, Bresson et al. [51] showed that Riverst's ring signature scheme holds under weaker security assumptions and improved ring signatures to overcome the security weakness problem. Moreover, they extended their improved scheme into a threshold ring signature scheme. Simultaneously, Abe et al. [49] presented a 1-out-of-n signature scheme with reduced computation and storage cost, and Zhang and Kim [60] proposed ID-based blind signatures and ring signatures from pairings. On the other hand, in 2002, Moni Noar [55] delivered a deniable ring authentication, which merges the ring signature of Riverst et al. [2] and the deniable authentication of Dwork [61]. The presented deniable ring authentication provides a zero-knowledge authentication proof system for ring signatures. In 2004, Xu et al. [56] also delivered an ring signature scheme using bilinear pairings. In 2006, Bender et al. [47] gave much stronger security notions for ring signatures and argued that the previous ring signatures are insecure against chosen public key attacks. As discussed in Section III-A2, Bender et al. [47] presented three-level anonymity: basic anonymity, anonymity with respect to adversarially chosen keys, and anonymity against full key exposure attacks. They also presented three generic constructions. The first construction is inspired by Bellare's static group signature scheme [8], and the other two efficient constructions were based on specific number-theoretic assumptions. Subsequently, Boneh et al. [50] proposed an efficient ring signature scheme secured only in the random oracle model. Shacham and Waters [48] proposed security definitions for anonymity and unforgeability, which are more persuasive than Bender's proposal. For instance, Shacham and Waters showed that Bender's unforgeability is insecure against adversarially generated keys and proposed a more potent version. On the other hand, the ring signature presented by Shacham and Waters is the first efficient ring signature scheme that is secured without random oracles.

While a stream of works solved the security problems in ring signatures, another one discussed efficiency in ring signatures [52,62]. For instance, another concern of original ring signatures [2] is the signature size's growth with the ring size. Dodis et al. [52] presented the first constant-sized ring signature scheme. However, they used random oracle models. In 2007, Chandran et al. [63] delivered a sub-linear-sized ring signature without random oracles and showed some disadvantages regarding the signature size. Ke Gu and Na Wu [62] submitted a traceable constant-sized ring signature without random oracles. Moreover, several certificate-less ring signatures schemes [59,64–66] addressed the key-escrow problem of ring signatures.

Even though permanent anonymity in ring signatures seems advantageous for users, unconditional anonymity leads to critical problems when applied in real-life applications since users can execute breaches. Thus, the complete anonymity of ring signatures became a vital issue in the cryptographic field. We discuss available solutions for this matter in Section 4.

Nevertheless, ring signatures have become popular in many multi-user cryptographic applications, where user anonymity is the main requirement. Typical examples for such applications are e-voting [67–71], e-cash [70–73], and e-lottery [74,75]. Another prominent employment of ring signatures is cryptocurrency. For instance, the most popular cryptocur-

rencies, Monero and Ethereum, employee CryptoNote, which is a linkable ring signature. The application of ring signatures makes Monero a public-private, untraceable cryptocurrency and secures the privacy of transactions. The unrelated nodes on the blockchain can verify that the transaction is from a valid public key, although the transaction's sender cannot be traced.

Various ring signatures have been proposed to fill the gap between the theoretical and practical differences of ordinary ring signatures. In original ring signatures, a single user tries to leak a piece of internal information. A senator leaks a rumor from the White House. Since the user is anonymous, obtaining proof for the message is difficult. Thus the possibility that the receiver of the message will accept its veracity is lowered. Threshold ring signatures, proposed by Bresson et al. [51], require t number of users to sign a message. Thus, a message's receiver is more satisfied with its accuracy. Improvements to threshold ring signatures were eventually presented [76,77]. In e-voting systems with ring signatures, malicious users may vote more than once, because their identity is hidden. Researchers addressed this problem by suggesting linkable-ring signatures [50,70]. Some work improved ring signatures with tracing methods [62,78] (discussed in Section 4). Raylin Tso [79] presented an exciting ring signature called a universal ring signature. In their scheme, the signature holder creates a ring instead of a signature generator. In this case, a user gets a certificate for his information from a signer and can proceed to validate that information with a third party who employs the properties of anonymous credentials. Thus the user creates a ring.

4. Identifying Signers in Group Signatures and Ring Signatures

When analyzing publications on cryptography, many discussions address privacy preservation techniques [80]. As preventing the leakage and the theft of user information emerged as critical problems in the digital world, privacy preservation techniques received more attention, including anonymous signature schemes like group and ring signatures [7]. Even though both are group-oriented and protect user anonymity, group and ring signatures differ in several ways. For instance, although both schemes provide user anonymity, group signature schemes have revocable user anonymity, and ring signatures have non-revocable user anonymity. In group signatures, an authority with a tracing key can identify a signer by revoking a signature's anonymity. On the other hand, ring signatures have permanent user anonymity. Thus, the applicability of group and ring signatures in systems is different. Ring signatures are used in systems like e-voting where anonymity is required permanently instead of bidding systems where group signatures are more suitable since identifying users might sometimes be required. The drawback of tracing ability in group signatures is that the tracing manager can identify any user, including innocent ones. Since ring signatures have no tracing method, users can abuse their uncontrolled anonymity. The extreme power possessed by a tracer in group signatures and the permanent anonymity offered in ring signatures cause these schemes to be impractical to manipulate in the real world. Even though balancing anonymity and traceability in group signature and ring signature schemes is desirable, it seems quiet challenging to achieve. In the following subsections, we describe the existing approaches that addressed imbalanced tracing and anonymity in group and ring signatures.

4.1. User Tracing Methods in Group Signatures

Tracing a signer is essential in group signature schemes for punishing malicious group users. Since group signatures provide anonymity, a user may send a fake message with group signatures. For instance, an employee (user) may exploit the company (group) signature for a personal transaction. Thus to control the misbehavior of group users, their anonymity must be managed. Identifying dishonest users is required to punish them. Another possible requirement is identifying users during a criminal investigation at a housing complex. If a murder occurred, the authorities will want to identify those people who had access (entered) the area at that time. Residents might have to protect their privacy

with an anonymous system like key-card access, which employs group signatures that restrict access. However, since police are looking for a suspect, user anonymity needs to be revoked.

In earlier group signature schemes, the group manager had a tracing privilege. Subsequent tracing authority roles were transferred to a third party. We call the tracing authority (TO) the opening authority (OA) or a tracer. Standard group signature schemes [8,12,21,81], which include lattice-based group signature schemes [34,37], identify a signer by identity escrow. Since the signer escrows his identity to the tracing authority, this mechanism is called *tracing-by-escrow*. Thus the opening authority (OA) opens the given signature to identify the related signer. On the other hand, Wei [82] proposed another method, *tracing-by-linking*. In the group signature scheme with tracing-by-linking method a user who submits the same message twice or more is identified. The tracing-by-linking method, confirms the two or more messages are produced by the same user, and reveals only such users' identities. Thus their proposal is applicable in linkable group signatures [83] and more suitable in ring signatures [84] and e-voting [70,85].

In the dynamic group signature scheme of Bellare et al. [24], which employed *tracing-by-escrow*, a signer encrypts his id in the signature using the tracing manager's public key (**tpk**), which is available in the group public key. As a result, only the tracing authority with the related secret key (**tsk**) can decrypt the signature and identify the signer, confirming that no outsider other than the tracing manager can identify the signature originator. Such simple encryption and decryption make the tracing mechanism efficient and straightforward. The underlying non-interactive zero-knowledge (NIZK) protocols [86,87] employed by group signature schemes ensure that ciphertext C in given signature Σ is the correct encryption of signer's id d. NIZK is a method that convinces an outsider (verifier) that the given statement is true without disclosing any information beyond the statement's validity and without interacting with the statement verifier. It requires only sending a message once with a statement to the verifier to satisfy a standard common string.

On the other hand, group signature schemes with an efficient revocation method called verifier-local revocation (VLR) [88] showed a different tracing method. In group signature schemes with verifier-local revocation [29,39,41,89], a token determines the users' revocation status. Thus the signature verifier can validate the signature against a revocation token list provided by the group manager. Using the same technique, considering each user as a revoked user, the tracing authority (the group manager in this case) can identify the signer. We call this *implicit tracing*. The tracing method in group signature schemes with verifier-local revocation seems inefficient because the tracing authority requires that each user be checked until the signer is found.

Recall that in the standard group signature schemes only a single tracing manager can identify the signers. The context of ordinary group signature schemes relies on a centralized trusted tracing authority. As discussed above, while such a tracing mechanism is required to punish malicious users and control user anonymity, it grants extreme privilege to the tracing authority. Even though the tracing mechanism is proposed to controls user disputes in group signatures, the tracing party can also identify innocent group users. Thus it greatly violates user anonymity. The tracing authority possesses dominance for maintaining user anonymity. He can cancel any user anonymity whenever he wants. If the tracing manager is corrupted, users' anonymity is vulnerable. Moreover, the tracing manager is not held accountable for his behavior. No mechanism is discussed in standard group signature schemes [8,24] to control the tracing authority. Thus standard group signatures are comprised of imbalanced tracing and anonymity.

Well-balanced group signatures are desirable to apply to group signatures in practice. For instance, extreme tracing in imbalanced traditional group signatures violates user rights because it also allows tracers to cancel the anonymity of innocent users. Such complications are mainly caused by uncontrolled tracing ability and centralized tracing power. Another problem is the lack of accountability of tracers in traditional group signatures.

In 2004, Kiayias et al. [90] proposed a controlled tracing mechanism scheme in which the tracing authority can identify only a particular user and the messages signed by her. Kiayias et al. [90] focused on situations requiring that the messages signed by an identified malicious user be recognized. For instance, in an investigation, if the group manager finds an action by a malicious user, she may want to identify the transactions done by the malicious user to fix them. In standard group signatures, all the signatures must be opened, even those issued by innocent users to solve this problem. In Kiayias's method, other users' anonymity is preserved. When a trusted party sends the details about a suspected user to the group manager, she outputs a user-based trapdoor to the tracing authority. Thus the tracing manager can only open user-related messages. Kiayias' tracing method is a *user-dependent opening*. However, on the other hand, the tracer can open all the messages of the targeted user.

In 2012, Sakai et al. [26] proposed a *message-dependent opening* (MDO) for group signatures to limit the tracing capability to message-related openings. Their tracing method helps identify signers based on messages, like anonymous auctions. For instance, when the highest bid is awarded, the opener can only identify the highest bidder. Their proposal controls the tracer's ability based on the message. Sakai used a straightforward and appealing method to control the tracer's extreme power. Another authority, called an admitter in their scheme, issues a token based on a message, probably for inappropriate messages. Thus a tracer with a token can only identify the user/users related to that message. For instance, to identify the users who accessed our system during a specific time period, taking the particular period as a message, we can identify the users for that period. Thus the anonymity of other users is preserved. At the signing time, a user first encrypts his id with the tracing manager's public key and encrypts the obtained ciphertext with the message. Thus, the tracer can identify the signer by first decrypting the signature with the token received from the admitter related to the message. Libert et al. [91] eventually constructed this idea from lattice cryptography. However, message-dependent opening proposal is somewhat centralized.

Eliminating the centralized tracing power in group signatures, Manulis [92] presented another attractive tracing solution, *decentralized tracing*, based on democratic group signatures. However, the proposed model is too strong because it requires the unlinkability of issued group signatures. Subsequently, Manulis, Sadeghi, and Schwenk [93] presented a linkable version of the previous idea. We refer to the second scheme, which is practical in real life. In their Linkable Democratic Group Signature (LDGS) scheme, user anonymity is preserved only against outsiders. Thus group users can identify a signer, but non-members cannot. Outsiders can only validate the signatures as in standard group signatures. The tracing role can be done by any user. At the setup stage, the group establishes sets of ids ID and pseudonyms PS as public parameters and secret keys for each user. The signature verifiers can validate a signature using the publicly available pseudonym set PS. On the other hand, only inside members can identify the signer using a trapdoor related to the user's secret key. However, outsiders can validate the linkability of signatures. Thus Manulis's linkable democratic group signature scheme shares some properties with ring signatures. Although they delivered acceptable properties that eliminated centralized management and granted tracing power to each member of the group, trusting that no group member will disclose the signer's identity is unrealistic. Ibrahim [94] extended Manulis's linkable democratic group signature idea by addressing the problem of group members being traitors. Their scheme requires a majority of the users to join and identify the signer. Zheng et al. [95] extended Manulis's [92] democratic group signature scheme with threshold traceability where t group members must collude to trace signers (t is the threshold value).

Ghadafi [96] presented a group signature scheme with *distributed tracing*, where the centralized tracing authority in previous group signature schemes is distributed to an n-tracing party. Unless all the n-tracing authorities agree to disclose a signer, user anonymity is protected. Each tracing party must share its traced share, which will later be verified and

combined to identify the signer. Ghadafi also discussed threshold-distributed tracing with a tag-based encryption scheme. Blömer et al. [97] achieved a similar tracing method with a threshold protocol and presented short group signatures. They modified Boneh's short group signature scheme [12] with a tracing mechanism that requires that (t, n) threshold requirement be satisfied. Gennaro et al. [98] extended the threshold-based tracing idea by distributing the tracing authority and proposed a fully distributed group signature scheme by scattering the membership issuance authorization among multiple issuing managers who deal with user joining. Thus user joining is managed by a threshold protocol.

In 2015, Kohlweiss and Miers [99] presented the notion of *accountable tracing* (AT) in a scheme that addresses the problem in standard group signature schemes: no mechanism keeps the tracer accountable for his action. In the *accountable tracing* scheme, the tracing authority and the group manager are identical, and there are two kinds of users: traceable and nontraceable. Although traceable users are detected like traditional group signatures, nontraceable users cannot be traced by any authority. During an investigation, the group manager can treat suspected users as traceable and identify them. On the other hand, the group manager must also reveal which users are traceable. Thus it enables tracer accountability. Ling et al. [100] used the lattice hardness problems, and presented a quantum-safe *accountable tracing* group signature scheme.

In 2015, Ishida et al. [101] described the notion of *deniable group signatures*. In their scheme, they discussed real-life situations where a third party, like the police, needs to check whether a suspect was in the crime area when it was committed. In deniable group signatures, the tracing party can confirm the relation between the given signature against the suspected user without opening the innocent users' signatures. If the given signature does not belong to the suspected user, then the tracing party will output proof confirming it. Moreover, he cannot output the original signer of the given signature. Even though their scheme does not discuss reducing the tracing authority's centralized privilege, they showed how to control the data revealed by the tracing authority to the outside.

Benjumea et al. [102] proposed fair traceable multi-group signatures, where user traceability is discussed when multiple groups are involved: multi-group signatures. Their idea combines the group and traceable signatures of Kiayias et al. [90]. Moreover, their tracing method requires that traces cooperate with another party called fairness authorities to trace users. Recently, Lu et al. [103] presented a work that resembles that of Benjumea with a shorter signature size.

4.2. Preventing Malicious User Actions in Ring Signatures

Ring signatures are a simplified version of group signatures. Compared to group signature schemes, the ring signature scheme presented by Riverst et al. [2] provides permanent anonymity for users. On the other hand, there are no interactive communications like a user joining in group signatures, in which the group manager's requirement also arises. Thus users in ring signatures enjoy much flexibility with setup freeness. Even though ring signatures deliver the advantages of perfect anonymity and flexibility, ring signers are vulnerable to user attacks since they can abuse their signing rights. For instance, standard ring signatures [2,47] only provide user anonymity and unforgeability. The former ensures that no one can identify a signature's originator from the signature itself. Unforgeability ensures that the signer-submitted ring (set of public keys) has the signer's public key. No authority can identify the signer. Thus, users can double-submit a message for the same event. One possible application for ring signatures is e-voting. Users (voters) can submit their ballots while remaining anonymous due to ring signatures. Since ring signatures provide non-traceability, no authority can identify the dishonest voters and their malicious actions like voting more than once. Signature verifiers or another trusted authority must be given the power to recognize such malicious actions. The verifier should not accept signatures that have already been received for the same event by the same signer.

The above discussion shows that perfect anonymity in ring signature is questionable. On the other hand, we cannot cancel the anonymity of users like in group signature schemes

because it violates the principles of ring signatures. It is desirable to trace or prevent user disputes while protecting user anonymity in ring signatures.

Recall that the Riverst's ring signature scheme [2] has only two algorithms, signing and verifying, and their security notions of anonymity and unforgeability rely on the existence of trapdoor permutations. Note that subsequent ring signature schemes have a KeyGen algorithm to ensure that all the user keys are the same type. No mechanism identifies malicious users or prevents their actions because traditional ring signatures provided permanent anonymity to protect users and their behaviors. The problem of users' dishonesty was mainly caused by the absence of a mechanism to identify the relations between signatures and signatures with users.

The *accountable ring signature* (ARS) scheme by Xu and Yung [104] is the first known ring signature scheme that identifies users. While allowing them to choose a ring, accountable ring signatures force them to include a tag with the signature, allowing an authority to identify them. Accountable ring signatures bridge the gap between ring and group signatures. However, they show more suitability in applications where either group signatures or ring signatures are inapplicable. Bootle et al. [57] created a short accountable ring signature from random oracles, based on the decisional Diffie-Hellman assumption. Users have the flexibility to choose a ring and a tracer at the time of signing.

On the other hand, Liu et al. [54] presented the first *linkable ring signatures* (LRS) in a scheme for group signatures from ad-hoc groups. Their proposal satisfies three properties: anonymity, linkability, and spontaneity. Anonymity ensures the signer's indistinguishability. Linkability ensures that two signatures by identical signers can be linked. Spontaneity means setup freedom: no group-related key like in group signatures and no group manager role. Moreover, their ring signature scheme satisfied another notion: claimability. Using claimability, a user can claim responsibility for his violations by presenting proof for the signature. Thus, Liu's scheme delivered several noticeable improvements and advantages for ring signatures, resulting in their scheme being selected for such applications as one-round e-voting. They also presented the threshold version of their scheme. Subsequently, employing Liu's techniques [54] and Dodis' short constant-sized ring signature scheme [52], Tsang and Wei [70] delivered a short linkable ring signature scheme. Linkable ring signatures seem reasonable for applications like e-voting, which must protect user identities (required to protect user anonymity) and prevent users from abusing their anonymous signing privilege. Jeong et al. [105] presented a ring signature scheme with weak linkability. Recently, Torres et al. [106] and Lu et al. [107] extended Liu's [54] linkable ring signatures to more secured and practical linkable ring signatures from lattices (quantum-safe). Simultaneously, Boyen and Haines [108] delivered a linkable ring signature (LRS) scheme based on n-times multi-linear mappings. Baum et al. [109] also submitted a onetime linkable ring signature scheme from lattices.

Parallel to Liu's work on linkable ring signatures [54], Wei [82] presented a tracing technique for group signatures by linking called tracing-by-linking. This approach identifies a double signer's public key. In contrast, tracing-by-escrow in standard group signatures identifies the signer's identity. Enhancing the tracing-by-linking technique, in 2007, Fujisaki and Suzuki [78] presented *traceable ring signatures*, which restrict excessive anonymity. To achieve mild anonymity, they borrowed two notions, 'one-more unforgeability' from the context of the blind signature scheme [110] and 'double-spending traceability' from the context of the restricted blind signature scheme [111].

In contrast to group signatures in blind signatures, the signer does not know the message's content, and the message owner is different from the signer. Blind signatures act as a signature placed on a carbon copy envelope. For example, in an e-voting system, a voter (user) places his vote inside an envelope with a piece of carbon paper and gets the authority's signature on the envelope without disclosing his vote. The signer might know the user but not the content of the message inside the envelope. Once the user gets the authority's signature, he removes the vote from the envelope and submits it to the ballot system. The user anonymously proves his eligibility to vote to the ballot system with

the authority's signature. After the user removes his vote with the authority's signature from the envelope, it becomes nontraceable. Neither the ballot system nor the signing authority can identify the user. However, a user who already obtained a blind signature cannot generate a new one, that is, one-more unforgeable [110]. On the other hand, double-spending traceability in restricted blind signatures [111], which is presented for e-cash, tracks a user who used a signature twice [73,112,113].

Using both the 'one-more unforgeability' and 'double-spending traceability' properties used in blind signatures, Fujisaki and Suzuki [78] presented *traceable ring signatures*. Since the double-spending traceability of blind signatures does not trace honest users, honest user anonymity is protected in blind signatures and also in the application of traceable ring signatures. Traceable ring signatures use a tag to manage the linkability and the traceability of the signatures. Tag L consists of the event (issue) for which the signature was produced and a ring. For instance, in an election, its id is the event (issue), and the user-selected ad-hoc group (the public key list) is the ring. As explained in Fujisaki's scheme, a user produces a signature on a message using her secret signing key and tag $L = (issue, R)$, where R is the set of valid public keys or ring members, including the signer's public key. Thus the signature verifier, who cannot know the signer, validates the received signature for the given message and tag. If the signer outputs a signature for a message she already signed, everyone can identify the linkability of the two signatures. If the signer outputs a new signature for a new message but with the same tag, she is traceable. A malicious signer's public key is output by a tracing algorithm.

Traceable ring signatures have a tracing algorithm that anyone can execute and outputs one of three outputs for the given two message-signature pairs. If the given inputs are independent of each other, it outputs 'indep.' If they are linkable, it outputs 'linked.' If the signer is traced, it outputs the signer's public key. Moreover, Fujisaki's scheme satisfies three security notions: tag-linkability, anonymity and exculpability. Through traceable ring signatures, we can prevent excessive user anonymity. Recently, Fujisaki and Suzuki's traceable ring signature scheme [78] was extended to constant-sized traceable signatures without random oracles [62] and to quantum-safe schemes [114] with practical applications like VANET [115].

5. Discussion

Group and ring signatures are very influential in anonymous authenticating systems like e-commerce schemes and vehicle safety communication (VSC). In the future when constructing systems with post-quantum primitives, group- and ring-signature-based systems will be more convenient than the other current systems. For instance, at present, most VSC systems use short-lived pseudonyms to secure privacy. Since the vehicles cannot frequently request new pseudonyms from the authority, vehicles carry a stack of pseudonyms that last for a few years. However, when those systems are constructed in post-quantum primitives, the size becomes too large and reduces VSC system's efficiency and impacts its bandwidth usage. Thus, employing group and ring signatures instead of pseudonyms is an optimum solution. Other than user anonymity, group and ring signatures simplify construction and provide maintenance advantages.

5.1. Comparison of Group Signatures and Ring Signatures

Both group and ring signatures provide user anonymity based on group orientation. However, an important advantage of ring signatures over group signatures is the freeness of the pre-defined group of users (ring). Ring signatures are a generalization of group signatures because they offer more flexibility for users. In ring signatures, users are responsible for their own anonymity because they select a group when signing. In group signatures, to generate signatures users must have a group membership. That is, the group members are fixed for the group. Accordingly dynamic group signatures consist of user joining interactive protocols for new user registration and revocation mechanisms to punish misbehaving users. In group signatures, each group has a manager who governs the users

and identifies the signers. The tracing ability provided in group signatures limits user anonymity. In contrast, in ring signatures, users can generate signatures while enjoying permanent anonymity. Users are bound to no group or group manager; they can choose an ad-hoc group when they sign up to hide their identity. Moreover, ring signatures' settings exclude user joining and revoking methods and user-tracing mechanisms. Thus while group signatures are suitable in applications like key-card access, ring signatures are suitable in applications like e-voting. However, since the tracing manager in group signatures can detect any user (including innocent ones) and the honesty of the tracing manager is responsible for the user anonymity, the extreme tracing power invested in group signatures is a serious issue for user anonymity. On the other hand, since ring signatures provide permanent anonymity for users, they can more easily misuse their privilege. ring signatures provide extended anonymity for users. Thus excessive anonymity in ring signatures is a significant challenge that must be addressed.

5.2. Identifying User-Misbehaviors in Group Signatures and Ring Signatures

In contrast to ring signatures, group signatures have revocable anonymity. Although group signatures have extreme tracing authority, ring signatures have excessive anonymity. Thus, research work related to tracing (identifying) users of the two schemes has chosen different directions. In group signatures, the extreme power held by the tracing manager must be controlled. In contrast, in ring signatures, the excessive anonymity held by the users must be generalized. In Tables 4 and 5, we conclude the existing tracing methods in group and ring signatures.

Table 4 presents more methods presented than in Table 5 because compared to the ring signatures, group signatures has a long history, and based on the various applications that the group signatures are applied, controlling of the group manager's tracing power is discussed presenting different tracing methods.

Table 4. Notable tracing methods in group signatures.

Tracing Approach	Level of User Privacy/Traceability	Application Example
Standard tracing [8]	Suspected users: traceable Innocent users: traceable	In key-card access system, group manager can track user activities.
User dependent opening [90]	Suspected users: traceable Innocent users: non traceable	When highest bidder in an auction refuses to pay, authority can cancel any other bids by same user without revealing other users.
Decentralized tracing [93]	Suspected users: traceable Innocent users: traceable User anonymity is only safe from outsiders	When a panel member wants to discuss a fellow (anonymous) member's submitted paper, he can identify him/her.
Message-dependent opening [26]	Suspected message related users: traceable Innocent users (not related to the message): non traceable	Identifying users who entered a park at a particular time at which a crime happened in it.
Distributed tracing [96]	Suspected users: traceable Innocent users: traceable	Shareholders agree to find a malicious employee.
Accountable tracing [99]	Suspected users: traceable Innocent users: non traceable	Police request a housing complex owner to narrow down surveillance control to suspected list.

Table 5. Notable tracing methods in ring signatures.

Tracing Approach	Level of User Privacy/Traceability	Application Example
Accountable ring signature scheme [104]	Users are traceable only to their tracer	Users post in any online forums without registering. However, a forum owner can identify a user who violated conduct code.
Linkable ring signatures [54]	User anonymity is safe. Only linkability of signatures is identified	This prevents voting again during e-voting without identifying user.
Traceable ring signatures [78]	Dishonest users' public keys are traced	Unclonable group identification without group manager: honest user can prove his membership anonymously, but user clones are detected.

Even though as in Table 4 several approaches address the extreme tracing power wielded by the tracing manager in group signatures, we cannot say that any candidate solution is ideal. Well-balanced tracing and anonymity in group signatures should consist of a controlled, decentralized, and accountable user-tracing mechanism. The existing approaches provide reasonable tracing mechanisms, which are ideal for the applications being considered. For instance, Sakai's message-dependent opening approach [26] is suitable for controlling the tracing power based on message content. On the other hand, since accountable tracing [99] enables just tracking users who were selected in advance, it is useful when only the tracing party gets the suspected list beforehand. However, neither of these proposals provide decentralized tracing. If the tracing party is dishonest, all the anonymity of the accessible users is threatened. On the other hand, in decentralized tracing from Manulis et al. [93], if the tracing group (users) agrees, then it can revoke the anonymity of any group signature. However, tracing parties are not limited to what they can access. We note that each tracing approach proposed in the group signatures has advantages for the concerned applications. Selecting a suitable tracing mechanism for an actual system is the responsibility of the system owners. On the other hand, the systems will face some problems on user anonymity because the given solutions fail to satisfy all the aspects of balanced traceability.

Among approaches suggested in Table 5 for ring signatures, linkable ring signatures are appropriate in e-cash and e-voting because they prevent resubmissions. Note that signatures are linkable only when they are produced for the same event. Thus the same signer who creates signatures for different events is unlinkable. Moreover, the traceable ring signature has a characteristic that balances anonymity and traceability. Since traceable ring signatures provide restricted anonymity and traceability, they are more advantageous than other approaches. However, ring signatures may face efficiency issues like ring size problem. Even though Gu and Wu [62] presented constant-size traceable ring signatures still they are not quantum safe. Well-balanced anonymity and traceability, which is the prevention of malicious user attacks while securing user anonymity, should not affect the efficiency of ring signatures and should be secured long term.

5.3. Main Challenges and Future Research Trends in Group Signatures and Ring Signatures

In this section we highlight some research areas of group and ring signatures that require more future discussion (including the well balance traceability and anonymity discussed above).

- *Balancing Traceability and Anonymity while Achieving Other Features*
  Privacy is a right possessed by every user. On the other hand, traceability is required to prevent user attacks. We need well-balanced signature schemes.
  Although numerous group and ring signatures address the extreme tracing power in group signatures and excessive anonymity in ring signatures, no clear winner has emerged with a perfect tracing method that balances user anonymity and traceability. Each approach provides a specific solution ideal for a particular scenario. This is reasonable since the requirements of practical scenarios differ. However, an ideal tracing

method for group signatures must satisfy the following criteria: it must decentralize the tracing authority without requiring the involvement of another centralized authority; it must protect innocent users' anonymity; it must control the data that the tracer can access and hold the tracer accountable. Providing the best tracing solution for group signatures (while maintaining other features like efficient member revocation) is challenging. For instance, the existing group signatures with verifier-local revocation schemes [29,39,41,89] that present efficient member revocation have inefficient tracing mechanism. Even though we can obtain efficient tracing by an identity-escrow technique, still other authority like issuer who supports member registration can trace users based on their revocation tokens. On the other hand, the existing approaches that tried to provide privacy-preserved traceability failed to satisfy such requirements as decentralized tracing, accountability, and efficiency. Moreover, we identified a lack of discussion in tracking malicious tracers. The behavior of the tracers must be accountable to protect the long-term privacy of users. Ring signatures also have problems, including the growth of the ring size in notable tracing approaches.
Providing well-balanced, privacy-preserved traceability or preventing user attacks while maintaining features like flexibility and efficiency is necessary when applying group signatures and ring signatures in real life. Thus researchers should consider the impact on those features when proposing solutions that balance traceability and anonymity in both group and ring signatures.

- *Long Term Security for Group Signatures and Ring Signatures*
Quantum computing and the security of current cryptographic systems against quantum attacks have become a hot topic in the cryptoworld.
Most available group signature and ring signature schemes are not safe against quantum attacks. Since Peter Shor [116] showed that many number-theoretical problems are vulnerable to quantum attacks, researchers tend to construct schemes from quantum-safe cryptographic primitives like lattice cryptography and code-based cryptography. However, due to simple construction and high efficiency most of the presented proposals are still based on number-theoretical hardness assumptions. Recently, the National Institute of Standards and Technology (NIST) published post-quantum public key cryptosystems and digital signatures that were selected as the third-round finalist in their standardization project for post-quantum cryptosystems (https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization, accessed on 10 January 2022). In the future, the constructors of group and ring signatures should focus on schemes that satisfy standards like provided by NIST to protect their systems from quantum attacks. At the same time, some research groups, including that of Professor Johannes Buchmann, TU Darmstadt, Germany (https://longtermsecurity.org/, accessed on 10 January 2022), provide a platform for researchers to discuss the challenges of achieving long-lived systems and proposing theoretical and practical solutions. Projects like PQCrypto H2020 (www.pqcrypto.eu.org, accessed on 10 January 2022) are devoted to post-quantum and long-term security. Those projects show the importance of such security to conduct more researches. Recently, Grontas et al. [117] proposed a security model for long-lived e-voting systems. One research direction is taking Grontas' proposal as a starting point and conducting research on long-lived applications of group and ring signatures.
- *Preventing Implementation Hindrances in Group Signatures and Ring Signatures*
Group and ring signature proposals should be realistically administered in real-world applications and secured in actual systems.
The first group and ring signatures introduced were not applicable for real applications due to efficiency and security problems. For instance, the size of the first group and ring signatures grew linearly with the number of group users. This linear problem was later solved in both signature schemes. However, we still face difficulties when applying group signatures and ring signatures schemes that were proposed in the theoretical

world in the real world. For instance, the security model proposed in theoretical group signature and ring signature schemes did not capture all the side-channel attacks that happened after implementing them in actual situations. An attacker can observe the time consumptions taken for signing messages of different sizes and capture some of the signing key's information. Attacks on practical systems done by observing leakages like consumption of time, power, and electro magnetic radiation for a system process known as side-channel attacks. Studying side-channel attacks and proposing leakage-resilient signatures is another interesting research area. Since the proposals of group and ring signatures are eventually employed in physical, privacy-preserving applications like vehicle safety communications, e-cash, and e-voting, we have to be concerned with potential efficiency and security hindrances during their implementations. Recently, Huang et al. [118] presented three new black-box constructions of a leakage-resilient group signature.

Few research works have discussed the above hindrances in group and ring signatures. However, the research works we discussed above might be instantiated in future research trends.

6. Conclusions

This paper detailed two prominent signature schemes, group and ring signatures, which provide user anonymity by masking user identity in a group. Group signatures enable user anonymity by a predefined group, and it is revocable. On the other hand, ring signatures enable permanent anonymity by an ad-hoc group setting. Even though both signatures provide user anonymity, the extreme tracing power in group signatures and the permanent anonymity in ring signatures make them challenging for real-life applications. This paper analyzed and presented the existing strategies adopted addressing the imbalanced traceability and anonymity in both signatures. Although the tracing approaches in group signatures tried to distribute centralized tracing power or limit the user details to which the tracing authority has access, the strategies in ring signatures attempted to identify the malicious actions of users without harming their anonymity. However, since each existing tracing approach in the group and ring signatures provides matching solutions limiting to the concerning scenarios without answering all the aspects of balanced tracing, delivering an ideal tracing mechanism remains an open problem in both signature schemes. In addition, some notable hindrances in both prevent employing them in practice, such as security against quantum and side-channel attacks. Thus, more research is required, especially for security concerns, to make group and ring signatures in practice. Finally, this paper showed some hindrances as future research trends in group and ring signatures.

Throughout this survey, we realized that achieving privacy-preserved traceability for group signatures and controlled anonymity for ring signatures is not impossible. We need more research to provide ideal solutions and must focus on other aspects such as efficiency as well as the aspects that occur in practical applications.

Author Contributions: Conceptualization, M.N.S.P.; methodology, M.N.S.P.; writing—original draft preparation, M.N.S.P.; writing—review and editing, M.N.S.P., T.N. and M.H.; supervision, C.-M.C. and K.S.; project administration, H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chaum, D.; Van Heyst, E. Group signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1991; Volume 547, pp. 257–265.
2. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001; Volume 2248, pp. 552–565.
3. Chaurasia, B.K.; Verma, S.; Bhasker, S. Message broadcast in VANETs using group signature. In Proceedings of the 2008 Fourth International Conference on Wireless Communication and Sensor Networks, Indore, India, 12–14 October 2008; pp. 131–136.
4. Emura, K.; Hayashi, T. Road-to-vehicle communications with time-dependent anonymity: A lightweight construction and its experimental results. *IEEE Trans. Veh. Technol.* **2017**, *67*, 1582–1597. [CrossRef]
5. Brickell, E.; Camenisch, J.; Chen, L. Direct anonymous attestation. In Proceedings of the 11th ACM conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 132–145.
6. Agarwal, A.; Saraswat, R. A survey of group signature technique, its applications and attacks. *Int. J. Eng. Innov. Technol. (IJEIT)* **2013**, *2*, 28–35.
7. Meiklejohn, S. An Exploration of Group and Ring Signatures. 2011. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.308.8751&rep=rep1&type=pdf (accessed on 2 March 2021).
8. Bellare, M.; Micciancio, D.; Warinschi, B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003; Volume 2656, pp. 614–629.
9. Ateniese, G.; Tsudik, G. Group signatures á la carte. In *SODA*; SIAM: Philadelphia, PA, USA, 1999; Volume 17, pp. 848–849.
10. Chen, L.; Pedersen, T.P. New group signature schemes. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; Volume 950, pp. 171–181.
11. Camenisch, J.; Lysyanskaya, A. Signature schemes and anonymous credentials from bilinear maps. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; Volume 3152, pp. 56–72.
12. Boneh, D.; Boyen, X.; Shacham, H. Short group signatures. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; Volume 3152, pp. 41–55.
13. Kiayias, A.; Yung, M. Group signatures with efficient concurrent join. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005; Volume 3494, pp. 198–214.
14. Furukawa, J.; Imai, H. An efficient group signature scheme from bilinear maps. In Proceedings of the Australasian Conference on Information Security and Privacy, Brisbane, Australia, 4–6 July 2005; Volume 3574, pp. 455–467.
15. Delerablée, C.; Pointcheval, D. Dynamic fully anonymous short group signatures. In Proceedings of the International Conference on Cryptology in Vietnam, Hanoi, Vietnam, 25–28 September 2006; Volume 4341, pp. 193–210.
16. Bichsel, P.; Camenisch, J.; Neven, G.; Smart, N.P.; Warinschi, B. Get shorty via group signatures without encryption. In Proceedings of the International Conference on Security and Cryptography for Networks, Amalfi, Italy, 13–15 September 2010; Volume 6280, pp. 381–398.
17. Pointcheval, D.; Sanders, O. Short randomizable signatures. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 29 February–4 March 2016; Volume 9610, pp. 111–126.
18. Libert, B.; Mouhartem, F.; Peters, T.; Yung, M. Practical "signatures with efficient protocols" from simple assumptions. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 511–522.
19. Ateniese, G.; Camenisch, J.; Hohenberger, S.; De Medeiros, B. Practical Group Signatures without Random Oracles. *IACR Cryptol. EPrint Arch.* **2005**, *2005*, 385.
20. Boyen, X.; Waters, B. Compact group signatures without random oracles. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, 8 May–1 June 2006; Volume 4004, pp. 427–444.
21. Ateniese, G.; Camenisch, J.; Joye, M.; Tsudik, G. A practical and provably secure coalition-resistant group signature scheme. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2000; Volume 1880, pp. 255–270.
22. Lyuu, Y.D.; Wu, M.L. Convertible group undeniable signatures. In Proceedings of the Conference on the Theory and Application of Cryptography, Amsterdam, The Netherlands, 28 April 28–2 May 2002; Volume 2587, pp. 48–61.
23. Kiayias, A.; Yung, M. Extracting group signatures from traitor tracing schemes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003; Volume 2656, pp. 630–648.
24. Bellare, M.; Shi, H.; Zhang, C. Foundations of group signatures: The case of dynamic groups. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 14–18 February 2005; Volume 3376, pp. 136–153.
25. Gordon, S.D.; Katz, J.; Vaikuntanathan, V. A group signature scheme from lattice assumptions. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 5–9 December 2010; Volume 6477, pp. 395–412.
26. Sakai, Y.; Emura, K.; Hanaoka, G.; Kawai, Y.; Matsuda, T.; Omote, K. Group Signatures with Message-Dependent Opening. In Proceedings of the International Conference on Pairing-Based Cryptography, Cologne, Germany, 16–18 May 2012; Volume 7708, pp. 270–294.

27. Krenn, S.; Samelin, K.; Striecks, C. Practical group-signatures with privacy-friendly openings. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10.
28. Camenisch, J.; Stadler, M. Efficient group signature schemes for large groups. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997; Volume 1294, pp. 410–424.
29. Boneh, D.; Shacham, H. Group signatures with verifier-local revocation. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 168–177.
30. Bootle, J.; Cerulli, A.; Chaidos, P.; Ghadafi, E.; Groth, J. Foundations of fully dynamic group signatures. In Proceedings of the International Conference on Applied Cryptography and Network Security, Guildford, UK, 19–22 June 2016; Volume 9696, pp. 117–136.
31. Camenisch, J. Efficient and generalized group signatures. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997; Volume 1233, pp. 465–479.
32. Barić, N.; Pfitzmann, B. Collision-free accumulators and fail-stop signature schemes without trees. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997; Volume 1233, pp. 480–494.
33. Fujisaki, E.; Okamoto, T. Statistical Zero-Knowledge Protocols to Prove Modular Polynomial Relations. *IEICE TRANSACTIONS Fundam. Electron. Commun. Comput. Sci.* **1999**, *82*, 81–92.
34. Ling, S.; Nguyen, K.; Wang, H. Group signatures from lattices: Simpler, tighter, shorter, ring-based. In Proceedings of the IACR International Workshop on Public Key Cryptography, Gaithersburg, MD, USA, 30 March–1 April 2015; Volume 9020, pp. 427–449.
35. Alamélou, Q.; Blazy, O.; Cauchie, S.; Gaborit, P. A code-based group signature scheme. *Des. Codes Cryptogr.* **2017**, *82*, 469–493. [CrossRef]
36. Groth, J. Fully anonymous group signatures without random oracles. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007; Volume 4833, pp. 164–180.
37. Libert, B.; Ling, S.; Mouhartem, F.; Nguyen, K.; Wang, H. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; Volume 10032, pp. 373–403.
38. Ateniese, G.; Song, D.; Tsudik, G. Quasi-efficient revocation of group signatures. In Proceedings of the International Conference on Financial Cryptography, Southampton, Bermuda, 11–14 March 2002; Volume 2357, pp. 183–197.
39. Nakanishi, T.; Funabiki, N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, 4–8 December 2005; Volume 3788, pp. 533–548.
40. Nakanishi, T.; Fujii, H.; Hira, Y.; Funabiki, N. Revocable group signature schemes with constant costs for signing and verifying. In Proceedings of the International Workshop on Public Key Cryptography, Irvine, CA, USA, 18–20 March 2009; Volume 3788, pp. 463–480.
41. Langlois, A.; Ling, S.; Nguyen, K.; Wang, H. Lattice-Based Group Signature Scheme with Verifier-Local Revocation. In Proceedings of the International Workshop on Public Key Cryptography, Buenos Aires, Argentina, 26–28 March 2014; Volume 8383, pp. 345–361.
42. Garms, L. Variants of Group Signatures and Their Applications. 2020. Available online: https://pure.royalholloway.ac.uk/portal/files/38498511/2020garmslhphd.pdf (accessed on 10 March 2021).
43. Khader, D. Attribute Based Group Signatures. *IACR Cryptol. EPrint Arch.* **2007**, *2007*, 159.
44. Kuchta, V.; Sahu, R.A.; Sharma, G.; Markowitch, O. On new zero-knowledge arguments for attribute-based group signatures from lattices. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 29 November–1 December 2017; Volume 10779, pp. 284–309.
45. Camenisch, J.; Groth, J. Group signatures: Better efficiency and new theoretical aspects. In Proceedings of the International Conference on Security in Communication Networks, Amalfi, Italy, 8–10 September 2004; Volume 3352, pp. 120–133.
46. Guo, J.; Baugh, J.P.; Wang, S. A group signature based secure and privacy-preserving vehicular communication framework. In Proceedings of the 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 11 May 2007; pp. 103–108.
47. Bender, A.; Katz, J.; Morselli, R. Ring signatures: Stronger definitions, and constructions without random oracles. In *Theory of Cryptography Conference*; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3876, pp. 60–79.
48. Shacham, H.; Waters, B. Efficient ring signatures without random oracles. In Proceedings of the International Workshop on Public Key Cryptography, Beijing, China, 16–20 April 2007; Volume 4450, pp. 166–180.
49. Abe, M.; Ohkubo, M.; Suzuki, K. 1-out-of-n signatures from a variety of keys. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002; Volume 2501, pp. 415–432.
50. Boneh, D.; Gentry, C.; Lynn, B.; Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. In Proceedings of the International conference on the theory and applications of cryptographic techniques, Warsaw, Poland, 4–8 May 2003; Volume 2656, pp. 416–432.
51. Bresson, E.; Stern, J.; Szydlo, M. Threshold ring signatures and applications to ad-hoc groups. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002; Volume 2442, pp. 465–480.

52. Dodis, Y.; Kiayias, A.; Nicolosi, A.; Shoup, V. Anonymous identification in ad hoc groups. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; Volume 3027, pp. 609–626.
53. Herranz, J.; Sáez, G. Forking lemmas for ring signature schemes. In Proceedings of the International Conference on Cryptology in India, New Delhi, India, 8–10 December 2003; Volume 2904, pp. 266–279.
54. Liu, J.K.; Wei, V.K.; Wong, D.S. Linkable spontaneous anonymous group signature for ad hoc groups. In Proceedings of the Information Security and Privacy: 9th Australasian Conference, Sydney, Australia, 13–15 July 2004; Volume 3108, pp. 325–335.
55. Naor, M. Deniable ring authentication. In Proceedings of the 22nd Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002; Volume 2442, pp. 481–498.
56. Xu, J.; Zhang, Z.; Feng, D. A ring signature scheme using bilinear pairings. In Proceedings of the Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, 23–25 August 2004; Volume 3325, pp. 160–169.
57. Bootle, J.; Cerulli, A.; Chaidos, P.; Ghadafi, E.; Groth, J.; Petit, C. Short accountable ring signatures based on DDH. In Proceedings of the 20th European Symposium on Research in Computer Security, Vienna, Austria, 21–25 September 2015; Volume 9326, pp. 243–265.
58. Huang, J.; Huang, Q.; Susilo, W. Leakage-resilient ring signature schemes. *Theor. Comput. Sci.* **2019**, *759*, 1–13. [CrossRef]
59. Deng, L.; Shi, H.; Gao, Y. Certificateless Linkable Ring Signature Scheme. *IEEE Access* **2020**, *8*, 54641–54651. [CrossRef]
60. Zhang, F.; Kim, K. ID-based blind signature and ring signature from pairings. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002; Volume 2501, pp. 533–547.
61. Dwork, C.; Naor, M.; Sahai, A. Concurrent zero-knowledge. *J. ACM (JACM)* **2004**, *51*, 851–898. [CrossRef]
62. Gu, K.; Wu, N. Constant Size Traceable Ring Signature Scheme without Random Oracles. *IACR Cryptol EPrint Arch.* **2018**, *2018*, 288.
63. Chandran, N.; Groth, J.; Sahai, A. Ring signatures of sub-linear size without random oracles. In Proceedings of the International Colloquium on Automata, Languages, and Programming, Wroclaw, Poland, 9–13 July 2007; Volume 4596, pp. 423–434.
64. Chow, S.S.; Yap, W.S. Certificateless Ring Signatures. *IACR Cryptol EPrint Arch.* **2007**, *2007*, 236.
65. Zhang, L.; Zhang, F.; Wu, W. A provably secure ring signature scheme in certificateless cryptography. In Proceedings of the First International Conference, Wollongong, Australia, 1–2 November 2007; Volume 4784, pp. 103–121.
66. Chang, S.; Wong, D.S.; Mu, Y.; Zhang, Z. Certificateless threshold ring signature. *Inf. Sci.* **2009**, *179*, 3685–3696. [CrossRef]
67. Baudron, O.; Fouque, P.A.; Pointcheval, D.; Stern, J.; Poupard, G. Practical multi-candidate election system. In Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing, Newport, RI, USA, 26–29 August 2001; pp. 274–283.
68. Cramer, R.; Franklin, M.; Schoenmakers, B.; Yung, M. *Multi-Authority Secret-Ballot Elections with Linear Work*; EUROCRYPT 1996; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1070, pp. 72–83.
69. Wu, Y. An e-Voting System Based on Blockchain and Ring Signature. 2017. Available online: https://dgalindo.es/mscprojects/yifan.pdf (accessed on 14 March 2021).
70. Tsang, P.P.; Wei, V.K. Short linkable ring signatures for e-voting, e-cash and attestation. In Proceedings of the First international conference on Information Security Practice and Experience, Singapore, 11–14 April 2005; Volume 3439, pp. 48–60.
71. Malina, L.; Hajny, J.; Dzurenda, P.; Ricci, S. Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions. In Proceedings of the 15th International Joint Conference, ICETE 2018, Porto, Portugal, 26–28 July 2018; pp. 692–697.
72. Chaum, D.; Pedersen, T.P. Wallet databases with observers. In Proceedings of the 12th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992; Volume 740, pp. 89–105.
73. Brands, S. Untraceable off-line cash in wallet with observers. In Proceedings of the 3th Annual International Cryptology Conference, Santa Barbara, CA, USA, 22–26 August 1993; Volume 773, pp. 302–318.
74. Goldschlag, D.M.; Stubblebine, S.G. Publicly verifiable lotteries: Applications of delaying functions. In Proceedings of the International Conference on Financial Cryptography, Anguilla, British West Indies, 23–25 February 1998; Volume 1465, pp. 214–226.
75. Kushilevitz, E.; Rabin, T. Fair e-lotteries and e-casinos. In Proceedings of the Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, 8–12 April 2001; Volume 2020, pp. 100–109.
76. Chow, S.S.; Hui, L.C.; Yiu, S.M. Identity based threshold ring signature. In Proceedings of the 7th International Conference, Seoul, Korea, 2–3 December 2004; Volume 25, pp. 218–232.
77. Melchor, C.A.; Cayrel, P.L.; Gaborit, P.; Laguillaumie, F. A new efficient threshold ring signature scheme based on coding theory. *IEEE Trans. Inf. Theory* **2011**, *57*, 4833–4842. [CrossRef]
78. Fujisaki, E.; Suzuki, K. Traceable ring signature. In Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 16–20 April 2007; Volume 4450, pp. 181–200.
79. Tso, R. A new way to generate a ring: Universal ring signature. *Comput. Math. Appl.* **2013**, *65*, 1350–1359. [CrossRef]
80. bin Abdullah, N.; Muftic, S. Security protocols with privacy and anonymity of users. *Univers. J. Commun. Netw.* **2015**, *3*, 89–98. [CrossRef]
81. Camenisch, J.; Lysyanskaya, A. A signature scheme with efficient protocols. In Proceedings of the Third International Conference, SCN 2002, Amalfi, Italy, 11–13 September 2002; Volume 2576, pp. 268–289.

82. Wei, V.K. Tracing-by-linking group signatures. In Proceedings of the 8th International Conference, ISC 2005, Singapore, 20–23 September 2005; Volume 3650, pp. 149–163.
83. Hwang, J.Y.; Chen, L.; Cho, H.S.; Nyang, D. Short dynamic group signature scheme supporting controllable linkability. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1109–1124. [CrossRef]
84. Au, M.H.; Liu, J.K.; Susilo, W.; Yuen, T.H. Constant-size ID-based linkable and revocable-iff-linked ring signature. In Proceedings of the 7th International Conference on Cryptology in India, Kolkata, India, 11–13 December 2006; Volume 4329, pp. 364–378.
85. Li, P.; Lai, J. LaT-Voting: Traceable Anonymous E-Voting on Blockchain. In Proceedings of the 13th International Conference, NSS 2019, Sapporo, Japan, 15–18 December 2019; Volume 11928, pp. 234–254.
86. Feige, U.; Lapidot, D.; Shamir, A. Multiple non-interactive zero knowledge proofs based on a single random string. In Proceedings of the [1990] 31st Annual Symposium on Foundations of Computer Science, St. Louis, MO, USA, 22–24 October 1990; pp. 308–317.
87. Blum, M.; De Santis, A.; Micali, S.; Persiano, G. Noninteractive zero-knowledge. *SIAM J. Comput.* **1991**, *20*, 1084–1118. [CrossRef]
88. Brickell, E. An Efficient Protocol for Anonymously Providing Assurance of the Container of the Private Key. *Trusted Comp. Group (April 2003)* **2003**, submitted.
89. Libert, B.; Vergnaud, D. Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model. In Proceedings of the 8th International Conference on Cryptology and Network Security, Kanazawa, Japan, 12–14 December 2009; Volume 5888, pp. 498–517.
90. Kiayias, A.; Tsiounis, Y.; Yung, M. Traceable signatures. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; Volume 3027, pp. 571–589.
91. Libert, B.; Mouhartem, F.; Nguyen, K. A Lattice-Based Group Signature Scheme with Message-Dependent Opening. In Proceedings of the 2016 Annual Meeting and Courses, Orlando, FL, USA, 10–14 February 2016; Volume 9696, pp. 137–155.
92. Manulis, M. Democratic group signatures: On an example of joint ventures. In Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2006, Taipei, Taiwan, 21–24 March 2006; p. 365.
93. Manulis, M.; Sadeghi, A.R.; Schwenk, J. Linkable democratic group signatures. In Proceedings of the Information Security Practice and Experience: Second International Conference, Ispec 2006, Hangzhou, China, 11–14 April 2006; Volume 3903, pp. 187–201.
94. Ibrahim, M.H. Resisting Traitors in Linkable Democratic Group Signatures. *Int. J. Netw. Secur.* **2009**, *9*, 51–60.
95. Zheng, D.; Li, X.; Ma, C.; Chen, K.; Li, J. Democratic Group Signatures with Threshold Traceability. *IACR Cryptol. EPrint Arch.* **2008**, *2008*, 112.
96. Ghadafi, E. Efficient distributed tag-based encryption and its application to group signatures with efficient distributed traceability. In Proceedings of the Third International Conference on Cryptology and Information Security in Latin America, Florianópolis, Brazil, 17–19 September 2014; Volume 8895, pp. 327–347.
97. Blömer, J.; Juhnke, J.; Löken, N. Short group signatures with distributed traceability. In Proceedings of the Mathematical Aspects of Computer and Information Sciences: 6th International Conference, MACIS 2015, Berlin, Germany, 11–13 November 2015; Volume 9582, pp. 166–180.
98. Gennaro, R.; Goldfeder, S.; Ithurburn, B. Fully Distributed Group Signatures. 2019. Available online: https://www.orbs.com/wp-content/uploads/2019/04/Crypto_Group_signatures-2.pdf (accessed on 3 March 2021).
99. Kohlweiss, M.; Miers, I. Accountable metadata-hiding escrow: A group signature case study. *Proc. Priv. Enhancing Technol.* **2015**, *2015*, 206–221. [CrossRef]
100. Ling, S.; Nguyen, K.; Wang, H.; Xu, Y. Accountable tracing signatures from lattices. In Proceedings of the Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, 4–8 March 2019; Volume 11405, pp. 556–576.
101. Ishida, A.; Emura, K.; Hanaoka, G.; Sakai, Y.; Tanaka, K. Group signature with deniability: How to disavow a signature. *IEICE TRANSACTIONS Fundam. Electron. Commun. Comput. Sci.* **2017**, *100*, 1825–1837. [CrossRef]
102. Benjumea, V.; Choi, S.G.; Lopez, J.; Yung, M. Fair traceable multi-group signatures. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Francisco, CA, USA, 4–8 March 2008; Volume 5143, pp. 231–246.
103. Lu, T.; Li, J.; Zhang, L.; Lam, K.Y. Group Signatures with Decentralized Tracing. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 4–6 December 2019; pp. 435–442.
104. Xu, S.; Yung, M. Accountable ring signatures: A smart card approach. In *Smart Card Research and Advanced Applications VI*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 153, pp. 271–286.
105. Jeong, I.R.; Kwon, J.O.; Lee, D.H. Ring signature with weak linkability and its applications. *IEEE Trans. Knowl. Data Eng.* **2008**, *20*, 1145–1148. [CrossRef]
106. Torres, W.A.A.; Steinfeld, R.; Sakzad, A.; Liu, J.K.; Kuchta, V.; Bhattacharjee, N.; Au, M.H.; Cheng, J. Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1. 0). In Proceedings of the 23rd Australasian Conference on Information Security and Privacy (ACISP 2018), Wollongong, Australia, 11–13 July 2018; Volume 10946, pp. 558–576.
107. Lu, X.; Au, M.H.; Zhang, Z. Raptor: A practical lattice-based (linkable) ring signature. In Proceedings of the 17th International Conference on Applied Cryptography and Network Security (ACNS 2019), Bogotá, Colombia, 5–7 June 2019; Volume 11464, pp. 110–130.
108. Boyen, X.; Haines, T. Forward-secure linkable ring signatures. In Proceedings of the 23rd Australasian Conference on Information Security and Privacy (ACISP 2018), Wollongong, Australia, 11–13 July 2018; Volume 10946, pp. 245–264.

109. Baum, C.; Lin, H.; Oechsner, S. Towards practical lattice-based one-time linkable ring signatures. In Proceedings of the Iformation and Communications Security–20th International Conference, ICICS 2018, Lille, France, 29–31 October 2018; Volume 11149, pp. 303–322.
110. Chaum, D. Blind signatures for untraceable payments. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1983; pp. 199–203.
111. Chaum, D.; Fiat, A.; Naor, M. Untraceable electronic cash. In Proceedings of the 8th Annual International Cryptology Conference, Santa Barbara, CA, USA, 21–25 August 1990; Volume 403, pp. 319–327.
112. Okamoto, T.; Ohta, K. Universal electronic cash. In Proceedings of the 11th Annual International Cryptology Conference, Santa Barbara, CA, USA, 11–15 August 1991; Volume 576, pp. 324–337.
113. Camenisch, J.; Hohenberger, S.; Lysyanskaya, A. Compact e-cash. In Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Volume 3494, pp. 302–321.
114. Branco, P.; Mateus, P. A traceable ring signature scheme based on coding theory. In Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, 8–10 May 2019; Volume 11505, pp. 387–403.
115. Han, L.; Cao, S.; Yang, X.; Zhang, Z. Privacy Protection of VANET Based on Traceable Ring Signature on Ideal Lattice. *IEEE Access* **2020**, *8*, 206581–206591. [CrossRef]
116. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
117. Grontas, P.; Pagourtzis, A.; Zacharakis, A. Security models for everlasting privacy. *IACR Cryptol EPrint Arch.* **2019**, *2019*, 1193.
118. Huang, J.; Huang, Q.; Susilo, W. Leakage-resilient group signature: Definitions and constructions. *Inf. Sci.* **2020**, *509*, 119–132. [CrossRef]