Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Linked or unlinked: A systematic review of linkable ring signature schemes ☆

Justice Odoom [a,*], Xiaofang Huang [a], Zuhong Zhou [b], Samuel Danso [c], Jinan Zheng [a], Yanjie Xiang [a]

[a] Southwest University of Science and Technology, School of Computer Science and Technology, Mianyang, 621010, Sichuan, China
[b] Mianyang Central Hospital, Information Center, Mianyang, Sichuan, China
[c] Ghana Communication Technology University, Faculty of Engineering, Accra, PMB 100, Ghana

ARTICLE INFO

Keywords:
Anonymity
Cryptocurrency
Key image
Linkability
Ring signature

ABSTRACT

As a prominent cryptographic primitive underlying anonymous communication, privacy-preserving cryptocurrencies, and other blockchain-based applications, ring signatures have garnered much attention in both research and industry over a decade with diverse guarantees of which linkability is an integral constituent. The linkability property enables any verifier to ascertain the fact that two ring signatures were generated by the same signer under a specified condition at the same time preserving signer anonymity. In this paper, we present a systematic investigation into linkable ring signature (LRS) schemes by reviewing 31 articles from 2006 to the first quarter of the year 2022 thereby providing readers with a broad synthesis of state-of-the-art information on LRS, current approaches to their constructions, security model, security guarantees, instantiation and applications. Our findings reveal non-uniformity in link tag constructions, diversity in underlying computational hard problems, and signature sizes as well as application areas. We point out the ramifications of construction paradigms as well as future research prospects aimed at providing guidance and reference for future research along this promising and vital cryptographic primitive.

1. Introduction

Ring signature as a cryptographic primitive was advanced by Rivest et al. [1] in 2001 primarily as a departure from the trusted setup associated with group signatures [2] consequently allowing for spontaneous instantiation of any ad-hoc group of users (in other words the user group is spontaneously conscripted by the signer) while still guaranteeing signer anonymity.

Ring signatures have found massive relevance and adoption in diverse facets of life where security and privacy are highly cherished from the initial application setting of whistle-blowing or leaking secrets [1]. Worth mentioning is such application areas as anonymous authentication [3–6], remote attestation mechanisms [7–9], and anonymous communication within typical domains such as Blockchain [10–15] and e-cash [16–18], e-voting [19,20], location-based services [21], cloud computing platforms [22,23] as well as outsourced computation [24]. Moreover, they act as building blocks for other cryptographic constructs like designated-verifier signature [25], anonymous verifiably encrypted signature [26], ad-hoc anonymous key agreement protocol [27], and concurrent signature [28].

However, whereas classical ring signatures provide signer anonymity, in some scenarios or application settings, an extra guarantee of the capability to determine whether two ring signatures were generated by the same signer under a specified condition is desired. This was an open problem until 2004 when Liu et al. [29] advanced the first linkable ring signature (LRS) where given two signatures by the same signer under a known condition (for example, an event id, name, or label), it is feasible to ascertain the fact that both signatures were generated by the same signer although the signer's identity remains anonymous. Extending the application scenario of leaking secrets, LRS thus provides a very powerful guarantee for the credibility or trustworthiness of a whistle-blower given past signatures on some reliable messages without compromising his/her identity.

It is however worth pointing out that extant research works have made limited attempts to encapsulate holistically existing knowledge by utilizing systematic literature reviews (SLRs) (example: [31–38]). For instance, [31,32,35] expatiated on the main privacy-related challenges in blockchain and performed an analysis of the prevailing privacy-preserving protocols like ring signatures, zero-knowledge proofs [39],

☆ This work was supported by National Natural Science Foundation of China (Youth), Image Source Forensics Security Research (Grant No. 61702429) and Sichuan Provincial Department of Science and Technology, China, A trusted basic service platform for universities based on independent and controllable blockchain technology (Grant No. 2021YFG0311).

* Corresponding author.
E-mail address: odoom.justice@ieee.org (J. Odoom).

https://doi.org/10.1016/j.sysarc.2022.102786
Received 5 July 2022; Received in revised form 11 November 2022; Accepted 13 November 2022
Available online 18 November 2022

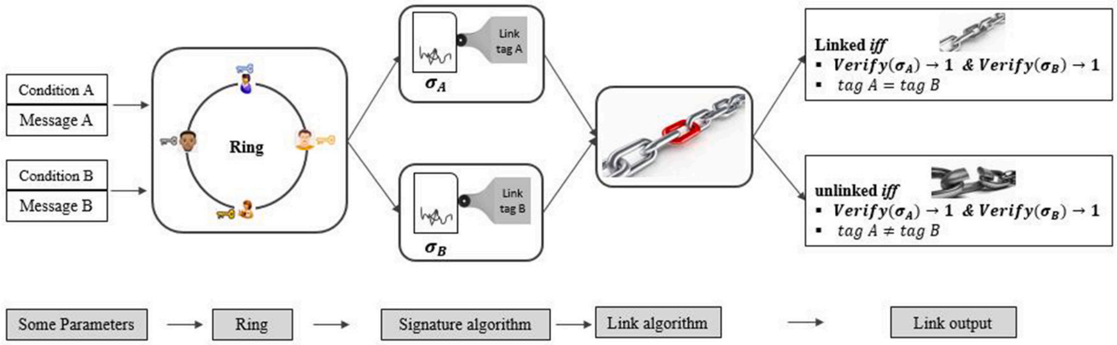

Fig. 1. A high-level model of linkable ring signatures.
Source: (Inspired by [30]).

and homomorphic hiding [40] among others along with identified challenges and future research directions. Similarly, [34] performed a systematic study regarding the cryptographic primitives utilized in blockchains based on the premise that blockchain is a crypto-intensive creature with a focus on its usages, functionalities, and evolution, with a similar approach adopted in [33]. [36] on the other hand, performs a comprehensive study of the threats and attacks that aim to deanonymize e-cash protocols by first presenting a detailed survey on anonymity-provisioning of blockchain-based e-cash transactions along with their features and limitations. [37] surveyed ring signatures over a decade ago and more recently [38] reviewed group and ring signatures which are the two prominent group-oriented signature schemes with a specific focus on the dynamics involved in traceability by exploring existing approaches that address the identification of malicious user activities.

While the aforementioned studies have in no doubt made advancements to the existing body of knowledge, it is obvious that their focus has primarily been on synthesizing or delineating prevailing privacy-preserving trends in the blockchain [31,32,35,36], expositions on cryptographic primitives [33,34] inherent in blockchain and the disparities in group-oriented signature schemes [38]. However, given the fact that LRS has an extra guarantee and plays an indispensable role in anonymous authentication and communication, researchers would significantly benefit from a tailored discussion on them. A systematic literature review is, therefore, cardinal to highlight such areas as cryptographic construction, security model, usage, challenges, and future research directions. We resolve such deficiencies by conducting an SLR on the construction and use of LRS as well as highlighting the ramifications of improper constructions.

1.1. Our contributions

The contributions of this SLR can be summarized as follows:

- We present a state-of-the-art research profile of prior studies relating to LRS. As far as we know, this is the first SLR in this domain.
- Based on the findings in the SLR, we posit a synthesizing framework highlighting potential aspects that require scholarly attention in furtherance of the extant body of knowledge primarily by addressing the four (4) research questions **RQs** that follow:
    1. **RQ1**: What is the state-of-the-art research profile regarding LRS?
    2. **RQ2**: What are the principal areas or domains wherein LRS has been utilized?
    3. **RQ3**: What are the variants of LRS that the literature posits, their security guarantees, underlying cryptosystem, and ramifications?
    4. **RQ4**: What are the future avenues, use cases, or domains that might benefit from LRS?

1.2. Organization of this work

The remainder of this paper is organized as follows. In Section 2, we introduce LRS, their algorithmic definition, and related security model whereas the methodology adopted in this SLR is presented in Section 3. We advance our findings in Section 4 and explicate on implications as well as future research directions in Section 5. Section 6 presents concluding remarks.

2. Linkable Ring Signatures (LRS)

A Linkable Ring Signature (LRS), unlike classical ring signatures allows any verifier to ascertain the fact that two signatures were generated by the same signer under a specified event (an identifier, transaction number, etc.) while preserving signer anonymity. This specified event is a publicly declared value/string uniquely describing the circumstances surrounding the signature hence not a secret. It is part of the parameters sent together with the signature for verification. For instance, in the issuance of digitally signed COVID-19 testing and vaccination certificates in the year 2022 by a group of medical professionals, the event identifier could be *COVID-19cert2022*. Linkability guarantees also exist in group signatures [41,42] and attribute-based signatures with controllable linkability [43–45]. There also exists subtle linkability in some blind signatures which unresolved, arms the signer to link a valid message-signature pair obtained from some user [46].

Note also that LRS differs from a variant of ring signatures known as Traceable Ring Signatures (TRS) [38,47,48]. Even though there exist linkability subtleties, the dichotomy lies primarily in the intent. Given two LRS under two different messages m_1 and m_2, the objective is to ascertain whether the same signer generated both signatures under the same event while preserving the anonymity of the signer whereas the purpose under the case of two TRS under m_1 and m_2 is to identify the specific signer often divulging the public key or identity of the signer thereby preventing the abuse of anonymity [49]. Moreover, whereas linkability in LRS is performed by any verifier (publicly verifiable), traceability is often the reserve of a trusted authority [49,50] although few exceptions on public traceability exist [51]. TRS is therefore akin to double authentication preventing signatures [52] in a ring setting. For brevity and due to disparities in constructions, we focus on LRS.

In LRS, the linking property is realized via a special feature integrated into the signing phase known as link tag [53] also known as link flag [54], signature image [55,56], key image [57], and tracking mark [58] often computed from the signer's secret/private key and the specified event. We expatiate upon some interesting findings regarding how the computation is done in Section 4.1. Based on inspiration from [30], we show a typical high-level model of LRS in Fig. 1.

2.1. Algorithmic definitions

A Linkable Ring Signature (LRS) scheme is a tuple comprising two Probabilistic Polynomial Time (PPT) algorithms, a randomized algorithm, and two deterministic algorithms. These five algorithms are **Setup**, **KeyGen**, **Sign**, **Verify**, and **Link**. Note that **Verify** and **Link** are also known as boolean algorithms. Following, we expatiate upon these five algorithms.

1. $param \leftarrow \textbf{Setup}(\lambda)$: This is a PPT algorithm. On input the security parameter (λ), it outputs a set of security parameters ($param$) where λ is inclusive.
2. $(sk, pk) \leftarrow \textbf{KeyGen}(param)$: This is also a PPT algorithm. On input $param$, it outputs a private key or secret key (sk) and a verification or public key (pk). We only explicitly include this algorithm for clarity on sk and pk.
3. $\sigma \leftarrow \textbf{Sign}(n, ev, \mathcal{L}, m, sk)$: This is a randomized algorithm that takes as inputs the cardinality or size of the ring (n), the specified condition or event identifier (ev), the public key list ($\mathcal{L}$) comprising all public keys of ring members including the signer, the message (m) to be signed, and the secret key (sk) of the signer. The algorithm outputs a ring signature (σ).
4. $0|1 \leftarrow \textbf{Verify}(n, ev, \mathcal{L}, m, \sigma)$: This is a boolean algorithm that takes as inputs the cardinality of the ring (n), an event identifier (ev), the public key list ($\mathcal{L}$) comprising all public keys of ring members including the signer and the message-signature pair (m, σ). The algorithm returns either 0 or 1 denoting $reject$ and $accept$ respectively. Note that $accept$ guarantees that the message-signature pair is valid.
5. $linked|unlinked \leftarrow \textbf{Link}(ev, n_1, n_2, \mathcal{L}_1, \mathcal{L}_2, m_1, m_2, \sigma_1, \sigma_2)$: This is a deterministic algorithm in which on input an event identifier ev, a list of public keys $\mathcal{L}_1$ and $\mathcal{L}_2$ of n_1, n_2 ring members, message-signature pairs (m_1, σ_1) and (m_2, σ_2) $s.t.$:

   $$\textbf{Verify}(n_1, ev, \mathcal{L}_1, m_1, \sigma_1) \rightarrow 1$$

   and

   $$\textbf{Verify}(n_2, ev, \mathcal{L}_2, m_2, \sigma_2) \rightarrow 1$$

   returns *linked* **iff** both signatures have the same link tags otherwise *unlinked*. Mathematically, this can be represented as:

   $$\textbf{Link}(params) = \begin{cases} linked & \text{if } Tag_1 = Tag_2 \\ unlinked & \text{if otherwise} \end{cases}$$

   where $parmas = ev, n_1, n_2, \mathcal{L}_1, \mathcal{L}_2, m_1, m_2, \sigma_1, \sigma_2$ and Tag_1, Tag_2 are link tags.
   Notice that both signatures must be generated under the same event identifier (ev).

It must be noted that LRS must guarantee correctness on two levels:

- Verification correctness: A valid signature guarantees acceptance at the verification phase.
- Linking correctness: Any two valid signatures generated under the same event identifier become *linked* **iff** both were generated by the same signer.

2.2. Security model

An LRS scheme must adhere to the security guarantee of anonymity, unforgeability, linkability, and non-slanderability. Before presenting the definitions, we provide below Oracles modeling the capabilities of the adversary hereafter $\mathcal{A}$ in breaking the security of an LRS scheme.

- $pk \leftarrow \mathcal{JO}(\perp)$: This is Joining Oracle ($\mathcal{JO}$) which upon request adds a user to the system and returns the public key $(pk) \in \mathcal{L}$ of the newly added user.
- $sk \leftarrow \mathcal{CO}(pk)$: This is Corruption Oracle ($\mathcal{CO}$) which upon input of the user public key $pk \in \mathcal{L}$, outputs the secret key sk corresponding to pk.
- $\sigma' \leftarrow \mathcal{SO}(n, ev, \mathcal{L}, pk_s, m)$: This is the Signing Oracle ($\mathcal{SO}$) and on input the cardinality of the ring n, an event identifier ev, a public key list $\mathcal{L} = (pk_1, pk_2, \dots, pk_n)$ where n denotes the ring's cardinality, the public key of the signer $pk_s \in \mathcal{L}$, and a message m returns a valid signature σ'.

Following, we present the definition of the security notions using a game-based approach where applicable between the simulator hereafter $\mathcal{S}$ and $\mathcal{A}$.

1. **Anonymity**: It should be infeasible for $\mathcal{A}$ to deduce pk (ID in the case of Identity-based Cryptography) or the true signer given a valid signature. This is modeled as a game played between $\mathcal{S}$ and $\mathcal{A}$ with access to $\mathcal{JO}$.

   (a) $\mathcal{S}$ generates the $param$ and gives to $\mathcal{A}$.
   (b) Adaptive strategy may be adopted by $\mathcal{A}$ in querying $\mathcal{JO}$.
   (c) $\mathcal{A}$ gives $\mathcal{S}$ the following: an event identifier ev, a ring size of $n \in \mathbb{N}$, a set $\mathcal{L}$ of n public keys $s.t.$ every $pk_i \in \mathcal{L}$ is a query output of $\mathcal{JO}$ and a message m. $\mathcal{S}$ randomly selects $\tau \overset{R}{\leftarrow} \{1, \dots, n\}$ and computes $\sigma_\tau \leftarrow \textbf{Sign}(n, ev, \mathcal{L}, sk_\tau, m)$ where sk_τ denotes the secret key corresponding to pk_τ. σ_τ is subsequently given to $\mathcal{A}$.
   (d) $\mathcal{A}$ outputs a guess $\tau' \in \{1, \dots, n'\}$.

   The advantage of $\mathcal{A}$ in this game is computed as:

   $$\textbf{Adv}_{\mathcal{A}}^{ANON-LRS}(\lambda) =| Pr[\tau' = \tau] - \frac{1}{n'} |$$

   where λ denotes the security parameter.
   Note, however, that anonymity concerning ring signatures can be unconditional (anonymity is guaranteed even amid unlimited computational capabilities or resources at the disposal of $\mathcal{A}$) or computational (where anonymity is guaranteed under the assumption of some mathematical/computational hard problems like Discrete logarithm, factorization, computational Diffie–Hellman, bilinear decision Diffie–Hellman, etc.). Consequently, we give the two definitions as follows.

   Definition 1.1 ***Unconditional anonymity:*** *An* **LRS** *scheme is unconditionally anonymous if for any unbounded adversary* $\mathcal{A}$, $\textbf{Adv}_{\mathcal{A}}^{ANON-LRS}(\lambda) = 0$.

   Definition 1.2. ***Anonymity:*** *An* **LRS** *scheme is anonymous if for any Probabilistic Polynomial Time (PPT) adversary* $\mathcal{A}$, $\textbf{Adv}_{\mathcal{A}}^{ANON-LRS}(\lambda)$ *is negligible*.
2. **Unforgeability**: It should not be possible for an $\mathcal{A}$ to forge any signature just from the public keys of the ring members. This is modeled as a game between $\mathcal{S}$ and $\mathcal{A}$ with $\mathcal{A}$ given access to $\mathcal{JO}$, $\mathcal{CO}$ and $\mathcal{SO}$.

   (a) $\mathcal{S}$ generates the $param$ and gives to $\mathcal{A}$.
   (b) Adaptive strategy may be adopted by $\mathcal{A}$ in querying the oracles.
   (c) $\mathcal{A}$ gives $\mathcal{S}$ the following: an event identifier ev, a ring size of $n \in \mathbb{N}$, a set $\mathcal{L}$ of n public keys, a message m and a signature σ.

   $\mathcal{A}$ wins **iff**:

   (a) $1 \leftarrow \textbf{Verify}(n, ev, \mathcal{L}, m, \sigma)$.
   (b) $\forall pk_i \in \mathcal{L}$, pk_i is a query output from $\mathcal{JO}$.
   (c) No $pk_i \in \mathcal{L}$ has been input to $\mathcal{CO}$.
   (d) σ is not a query result from $\mathcal{SO}$.

   The advantage of $\mathcal{A}$ in winning this game is computed as:

   $$\textbf{Adv}_{\mathcal{A}}^{UNF-LRS}(\lambda) = Pr[\mathcal{A} \text{ wins the game}]$$

Definition 2. ***Unforgeability:*** *An* **LRS** *scheme is unforgeable if* $\forall$ *PPT* $\mathcal{A}$*,* $\mathbf{Adv}_{\mathcal{A}}^{UNF-LRS}$ *is negligible.*

3. **Linkability**: It should be infeasible for the same signer to generate two signatures under the same event such that they are determined to be **unlinked**. Game-wise, this is modeled as follows where $\mathcal{A}$ is granted access to $\mathcal{JO}$, $\mathcal{CO}$ and $\mathcal{SO}$.

   (a) $\mathcal{S}$ generates the *param* and gives to $\mathcal{A}$.
   (b) Adaptive strategy may be adopted by $\mathcal{A}$ in querying the oracles.
   (c) $\mathcal{A}$ gives $\mathcal{S}$ two tuples $(n_1, ev, \mathcal{L}_1, m_1, \sigma_1)$ and $(n_2, ev, \mathcal{L}_2, m_2, \sigma_2)$ with each comprising ring size $n \in \mathbb{N}$, an event identifier ev, sets $\mathcal{L}_1$ and $\mathcal{L}_2$ of n public keys, (m_1, σ_1) and (m_2, σ_2) as message-signature pair.

   In this game, $\mathcal{A}$ wins **iff**:

   (a) For $i = 1, 2$: $1 \leftarrow \mathbf{Verify}(n_i, ev, \mathcal{L}_i, m_i, \sigma_i)$ and σ_i is not an output from $\mathcal{SO}$.
   (b) $\forall pk_i \in \mathcal{L}$, pk_i is a query output from $\mathcal{JO}$.
   (c) < 2 queries was made to $\mathcal{CO}$. In other words, $\mathcal{A}$ had access to at most 1 secret key.
   (d) $unlinked \leftarrow \mathbf{Link}(ev, n_1, n_2, \mathcal{L}_1, \mathcal{L}_2, m_1, m_2, \sigma_1, \sigma_2)$.

   The advantage of $\mathcal{A}$ in winning this game is denoted as:

   $\mathbf{Adv}_{\mathcal{A}}^{LNK-LRS}(\lambda) = Pr[\mathcal{A}$ wins the game$]$

   Definition 3. ***Linkability:*** *An* **LRS** *scheme is linkable if* $\forall$ *PPT* $\mathcal{A}$*,* $\mathbf{Adv}_{\mathcal{A}}^{LNK-LRS}$ *is negligible.*

4. **Non-slanderability**: It should be impossible for any signer to generate a signature which at a later time is determined to be linked with another signature not generated by the signer. This security guarantee informally forestalls an $\mathcal{A}$ from framing an honest signer. Game-wise, this is modeled as follows where $\mathcal{A}$ is granted access to $\mathcal{JO}$, $\mathcal{CO}$ and $\mathcal{SO}$.

   (a) $\mathcal{S}$ generates the *param* and gives to $\mathcal{A}$.
   (b) Adaptive strategy may be adopted by $\mathcal{A}$ in querying the oracles.
   (c) $\mathcal{A}$ gives $\mathcal{S}$ the following: an event identifier ev, a message m, a set of $n \in \mathbb{N}$ public keys $\mathcal{L}$, the public key of an insider public key $pk_\tau \in \mathcal{L}$ *s.t.* pk_τ has neither been queried to $\mathcal{CO}$ nor included in any query to $\mathcal{SO}$. Subsequently, $\mathcal{S}$ utilizes the secret key sk_τ corresponding to pk_τ to run the sign algorithm as: $\sigma' \leftarrow \mathbf{Sign}(n, ev, \mathcal{L}, sk_\tau, m)$. σ' is given to $\mathcal{A}$.
   (d) $\mathcal{A}$ queries the oracles with arbitrary interleaving except pk_τ can neither be queried to $\mathcal{CO}$ nor included in any query to $\mathcal{SO}$ as aforementioned.
   (e) $\mathcal{A}$ outputs a ring size of n^*, a tuple of n^* public keys $\mathcal{L}^*$, a message m^*, and a signature $\sigma^* \neq \sigma'$.

   $\mathcal{A}$ wins the game **iff**:

   (a) $1 \leftarrow \mathbf{Verify}(n^*, ev, \mathcal{L}_i^*, m^*, \sigma^*)$ and σ^* is not an output from $\mathcal{SO}$.
   (b) $\forall pk_i \in \mathcal{L} \& \mathcal{L}^*$, pk_i is a query output from $\mathcal{JO}$.
   (c) pk_τ has not been queried to $\mathcal{CO}$.
   (d) $Linked \leftarrow \mathbf{Link}(ev, n, n^*, \mathcal{L}, \mathcal{L}^*, m, m^*, \sigma', \sigma^*)$.

   The advantage of $\mathcal{A}$ in winning this game is denoted as:

   $\mathbf{Adv}_{\mathcal{A}}^{NS-LRS}(\lambda) = Pr[\mathcal{A}$ wins the game$]$

   Definition 4. ***Non-slanderability:*** *An* **LRS** *scheme is non-slanderable if* $\forall$ *PPT* $\mathcal{A}$*,* $\mathbf{Adv}_{\mathcal{A}}^{NS-LRS}$ *is negligible.*

3. Methodology

In this paper, we utilize the SLR guidelines [59] and the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [60]. SLRs generally provide a synthesizing view of the whole research landscape paving way for readers to acquire comprehensive knowledge of the literature in a specified field via a holistic and organized standard protocol [61,62] aside from pointing out existing knowledge gaps and future research opportunities.

In this SLR, we employ three distinct phases encompassing design, implementation, and synthesis as our SLR protocol. Adopting the protocol illustration in [63], we depict our SLR protocol in Fig. 2.

To address **RQ1**, we present qualitative and quantitative statistics pertaining to:

- the number of articles published per year.
- average citations per year for each article.
- scholarly contributions in the research area regarding publishers, journals, and countries.

Our efforts geared towards addressing **RQ2-RQ4** involved:

- identifying prior study contexts and primary constructs.
- identifying the latest research developments by summarizing key findings and bottlenecks.
- deducing implications both from theoretical and practical contexts.
- pinpointing emergent knowledge gaps and avenues for further research.

Taking cues from [64] regarding database selection, we select four databases: Web of Science (WOS), IEEE Explore, ScienceDirect, and DBLP with article selection accomplished via specific inclusion and exclusion criteria relying on recommendations from prior research [63]. Note that in all database searches, the query used was *"ring signature" AND linkable OR linkability*. We refer the reader to Table 1 for details regarding the output of the search query on the aforementioned databases.

In other to retain quality articles in line with the scope of this SLR, we evaluated each article using an article quality assessment (QA) criteria by crafting four QA metrics as presented in Table 2 with a predetermined eligibility score set at ≥ 6 (see Table 3 for details on scores for all articles).

Based on Table 3, **seven** articles (marked *) not meeting the eligibility score were eliminated with 30 remaining. It must be noted that we also conducted citation chaining to resolve feedback loops based on which **one** article was identified and upon meeting the eligibility score, was subsequently added to the article pool. Consequently, the final article pool comprised **31** journal articles.

3.1. Research outlook

To better understand the status quo of extant works on LRS, we profile extant works by performing bibliometric analysis via bibliometrix [95], an R-tool for comprehensive science mapping analysis.

Statistics and bibliometric analysis of the research profile on LRS show a noticeable increase in yearly publications (see Fig. 3) especially from 2018 as well as average citations for works included in this SLR (see Fig. 4). We notice that Liu J.K., Susilo W., and Au M.H. collaboratively were top contributors in this domain with four publications of which Liu J.K. first authored three.

The institutional affiliation(s) of the first authors of the included articles were discovered to be located in nine countries with the number (n) of publications emanating from China ($n = 17$), India ($n = 4$), and Australia ($n = 2$) as shown in Table 4.

We also note that even though the articles were published in diverse journals (see Table 5), leading sources emanated from IEEE Access ($n =$

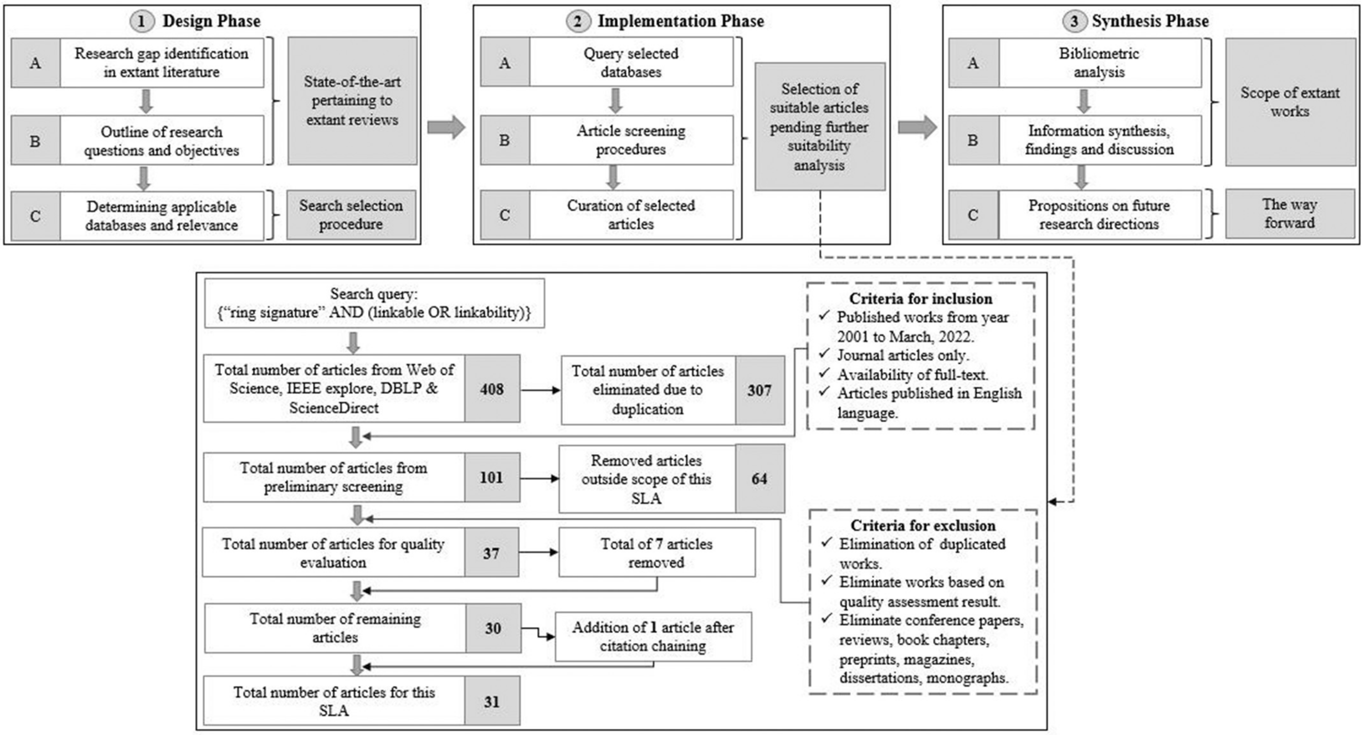
1 Design Phase
A Research gap identification in extant literature
B Outline of research questions and objectives
C Determining applicable databases and relevance
State-of-the-art pertaining to extant reviews
Search selection procedure
2 Implementation Phase
A Query selected databases
B Article screening procedures
C Curation of selected articles
Selection of suitable articles pending further suitability analysis
3 Synthesis Phase
A Bibliometric analysis
B Information synthesis, findings and discussion
C Propositions on future research directions
Scope of extant works
The way forward
Search query: {"ring signature" AND (linkable OR linkability)}
Total number of articles from Web of Science, IEEE explore, DBLP & ScienceDirect 408
Total number of articles eliminated due to duplication 307
Total number of articles from preliminary screening 101
Removed articles outside scope of this SLA 64
Total number of articles for quality evaluation 37
Total of 7 articles removed
Total number of remaining articles 30
Addition of 1 article after citation chaining
Total number of articles for this SLA 31
Criteria for inclusion
✓ Published works from year 2001 to March, 2022.
✓ Journal articles only.
✓ Availability of full-text.
✓ Articles published in English language.
Criteria for exclusion
✓ Elimination of duplicated works.
✓ Eliminate works based on quality assessment result.
✓ Eliminate conference papers, reviews, book chapters, preprints, magazines, dissertations, monographs.

Fig. 2. Schematic diagram of the systematic literature review.
Source: (Inspired by [63]).

Table 1
Statistics from the database search.

Database	Query string	Total hits	Read abstracts	Full text downloaded
Web of Science	{“ring signature” AND (linkable OR linkability)}	204	204	193
IEEE explore		151	151	57
DBLP		53	53	7
ScienceDirect		198	198	151
Total		606	606	408

Table 2
Article quality assessment criteria.

Quality Assessment (QA)	Assessment metric
QA1	The proposition of a new or modified ring signature scheme: Yes (+2.0), No (+0)
QA2	Linkability guarantee added to the signature scheme: Yes (+2.0), No (+0)
QA3	Provision of robust security analysis: Yes (+2.0), Partly (+1.0), No (+0)
QA4	Peer-recognition of the article and source reliability: (+2.0) sum of citations and H index is ≥ 40 (+1.5) sum of citations and H index is ≥ 15 and ≤ 39 (+1.0) sum of citations and H index is ≥ 1 and ≤ 14 (+0) sum of citations and H index $= 0$

8) along with other IEEE-based publications making IEEE the leading publisher in this domain followed by Security and Communication Networks ($n = 4$) by Hindawi.

A conspicuous observation from our bibliometric analysis based on keywords and author-indicated keywords revealed that extant works focus on “schemes”, “efficiency”, “linkability”, “privacy” or anonymity, and “blockchain” as a conducive environment for implementation (see Fig. 5).

4. Findings

Carefully analyzing each article that qualified for inclusion in this SLR led to some interesting discoveries. We thoroughly discuss these in various subsections that follow.

4.1. Tag construction

Extant works employ a myriad of approaches in the construction of link tags. There is no uniformity in link tag constructions. Whereas some researchers employ randomness, others make use of the ring (group-dependency). The *event* description although widely adopted is not used by all researchers. However, a common feature among all schemes is the utilization of the private key of the signer to somewhat bind the link tag to the signer (signer-binding). The dominant cryptographic primitive used here is cryptographic hash functions. In Table 6, we present the various schemes and link tag constructions. For clarity and uniformity in Table 6, we denote the signer’s secret/public key pair as $\{sk, pk\}$, the public key list for the entire ring as $\mathcal{L}$ and the link tag as T. Also, note that we use $\mathcal{H}$ and its variants to denote a cryptographic hash function.

Table 3
Results from article quality assessment.

Reference	Total cites	H-index	*Quality Assessment*					Average yearly citation
			QA1	QA2	QA3	QA4	Total Score	
Yadav V. K. et. al. [21]	0	0	2.0	2.0	2.0	0	6.0	0.00
Guo L. et. al. [24]	0	0	2.0	2.0	2.0	0	6.0	0.00
Cai X. et. al. [51]	3	1	2.0	2.0	2.0	1.0	7.0	1.00
Ren Y. et. al. [53]	0	0	2.0	2.0	2.0	0	6.0	0.00
Yan X. et. al. [54]	8	1	2.0	2.0	2.0	1.0	7.0	2.00
Li X. et. al. [55]	19	3	2.0	2.0	2.0	1.5	7.5	6.33
Cai Y. et. al. [58]	4	1	2.0	2.0	2.0	1.0	7.0	2.00
Le H. Q. et. al. [30]	0	0	2.0	2.0	2.0	0	6.0	0.00
Jeong I. et. al. [65]	7	1	2.0	2.0	2.0	1.0	7.0	0.47
Ren Y. et. al. [66]	2	1	2.0	2.0	2.0	1.0	7.0	0.67
Liu J. K. et. al. [67]	42	1	2.0	2.0	2.0	2.0	8.0	4.67
Ferrag M. A. et. al. [68]	0	0	2.0	2.0	2.0	0	6.0	0.00
Deng L. et. al. [69]	4	4	2.0	2.0	2.0	1.0	7.0	1.00
Jeong I. R. et. al. [70]	9	1	2.0	2.0	2.0	1.0	7.0	0.64
Deng L. et. al. [71]	14	1	2.0	2.0	2.0	1.5	7.5	0.33
Yuen T. H. et. al. [72]	31	1	2.0	2.0	2.0	1.5	7.5	3.10
Mazumdar S. et. al. [73]	1	1	2.0	2.0	2.0	1.0	7.0	0.50
Au M. H. et. al. [74]	35	1	2.0	2.0	2.0	1.5	7.5	3.50
Fujisaki E. [75]	5	2	2.0	2.0	2.0	1.0	7.0	0.45
Mu. R. et. al. [76]	0	0	2.0	2.0	2.0	0	6.0	0.00
Mao X. et. al. [77]	0	0	2.0	2.0	2.0	0	6.0	0.00
Huang K. et. al. [78]	0	0	2.0	2.0	2.0	0	6.0	0.00
Huang K. et. al. [79]	5	1	2.0	2.0	2.0	1.0	7.0	2.50
Liu J. et. al. [80]*	0	0	2.0	0	2.0	0	4.0	0.00
Galdi C. et. al. [81]*	0	0	2.0	0	2.0	0	4.0	0.00
Wu T. et. al. [82]	0	0	2.0	2.0	2.0	0	6.0	0.00
Lin. H. et. al. [83]*	1	1	2.0	0	2.0	1	5.0	1.00
Yadav V. K. et. al. [84]	2	2	2.0	2.0	2.0	1.0	7.0	1.00
Boyen X. et. al. [85]	4	1	2.0	2.0	2.0	1.0	7.0	0.27
Liu J. et. al. [86]	19	1	2.0	2.0	2.0	1.5	7.5	1.20
Bouakkaz S. et. al. [87]	1	1	2.0	2.0	2.0	1.0	7.0	0.33
Wang L. et. al. [88]	3	1	2.0	2.0	2.0	1.0	7.0	0.50
Hara K. et. al. [89]*	0	0	2.0	0	2.0	0	4.0	0.00
Au M. H. et. al. [90]*	13	1	2.0	0	2.0	1.0	5.0	1.30
Chen S. et. al. [91]*	3	1	2.0	0	2.0	1.0	5.0	0.60
Ren. J. et. al. [92]*	11	14	2.0	0	2.0	1.5	5.5	0.73
Li W. et. al. [93]	0	0	2.0	2.0	2.0	0	6.0	0.00
Dharani J. et. al. [94]	0	0	2.0	2.0	2.0	0	6.0	0.00

Table 4
Article count from countries.

Country	Total published articles
China	17
India	4
Australia	2
Korea	2
Singapore	2
Algeria	1
Germany	1
Japan	1
Vietnam	1

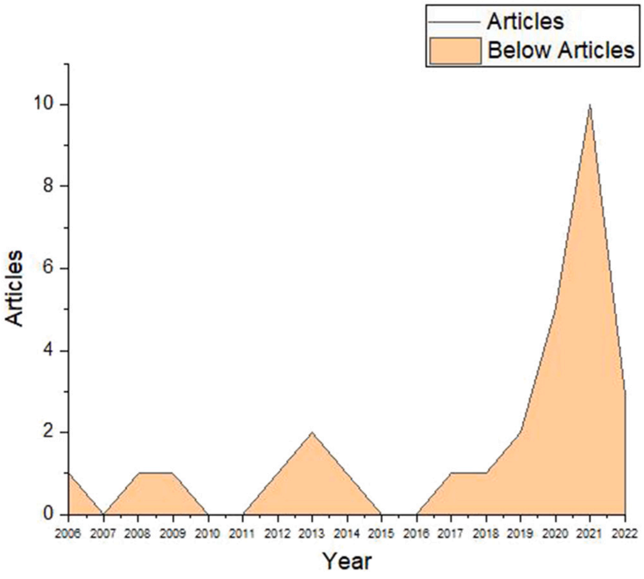

Fig. 3. Yearly distribution of published articles.

4.2. *Cryptosystems*

As fundamental building blocks for designing security protocols, cryptosystems invariably are at the core of the security guarantees and efficiency of LRS schemes.

Performing content analysis of the reviewed articles included in this SLR comprising schemes constructed in the Public-key Infrastructure (PKI), Identity-based Cryptography (IBC), and Certificateless Public Key Cryptography (CL-PKC) settings, we in this section advance the diverse cryptosystems employed by researchers in the construction of LRS schemes and present detailed findings in Table 7. In Fig. 6, we graphically show the quantum of LRS constructions in the various cryptosystems.

4.2.1. *Rabin and RSA cryptosystem-based constructions*

The Rabin cryptosystem (a special type of RSA with an encryption key denoted as $e = 2$) is an asymmetric cryptographic technique whose security as with RSA is secure under the hardness of factorization [96]. We find one LRS [73] based on this cryptosystem making it among the least utilized cryptosystem underlying LRS schemes.

Table 5
Number of articles from journals.

Name of journal	Number of articles
IEEE ACCESS	8
SECURITY AND COMMUNICATION NETWORKS	4
IEEE TRANSACTIONS ON CLOUD COMPUTING	2
IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING	2
IEICE TRANS. ON FUNDA. OF ELECT. COMM. AND COMP. SCI.	2
INFORMATION SCIENCES	2
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS	2
COMPUTER JOURNAL	1
COMPUTERS & SECURITY	1
CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE	1
IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING	1
IEEE TRANS. ON INTELLIGENT TRANSPORTATION SYSTEMS	1
INT. JOUR. OF FOUNDATIONS OF COMPUTER SCIENCE	1
J. OF AMBIENT INTELL. & HUMANIZED COMPUTING	1
MDPI CRYPTOGRAPHY	1
THEORETICAL COMPUTER SCIENCE	1

Table 6
Approaches to link tag construction.

Scheme	Link tag construction	Meaning of notations	Approach
Yadav V. K. et. al. [21] Li X. et. al. [55] Mao X. et. al. [77]	$T = sk\mathcal{H}(pk)$	-	Signer-binding
Guo L. et. al. [24] Yan X. et. al. [54] Huang K. et. al. [78] Huang K. et. al. [79] Yadav V. K. et. al. [84] Liu J. et. al. [86]	$T = h^{sk}$	$h = \mathcal{H}(\mathcal{L})$	Group-dependent
Cai X. et. al. [51]	$T = l_i pk$	$l_i = \mathcal{H}(pk, ID_i)$	Signer-binding
Ren Y. et. al. [53,66]	$T = Bsk$	$B \leftarrow R_q^{h\times v}$,[a]	Signer-binding
Cai Y. et. al. [58]	$T = x_i Q_{ID_i}$	$x_i \overset{R}{\leftarrow} Z_q^*, Q_{ID_i} = \mathcal{H}(ID_i)$	Randomness
Jeong I. et. al. [65]	$T = D_0^r$	$D_0 \overset{R}{\leftarrow} \mathcal{G}$ and $r \overset{R}{\leftarrow} \mathbb{Z}$	Randomness
Liu J. K. et. al. [67] Jeong I. R. et. al. [70] Au M. H. et. al. [74] Wu T. et. al. [82]	$T = e^{sk}$	$e = \mathcal{H}(ev)$	Signer & event-binding
Le H. Q. et. al. [30]	$T = Ksk$	$K = \mathcal{H}(ev)$	Signer & event-binding
Ferrag M. A. et. al. [68]	$T = t_{k,1} + t_{k,2}$	$t_{k,i} : sk_i * master\ pk$	Signer-binding
Deng L. et. al. [69]	$T = e(E, D_s)$	$E = \mathcal{H}(ev),\ D_s = \mathcal{H}(ID_i)$	Signer & event-binding
Deng L. et. al. [71]	$T = (sk + ht_s)E$	$E = \mathcal{H}_2(ev),\ h = \mathcal{H}_3(ev),\ t_s \overset{R}{\leftarrow} Z_q^*$	Randomness
Yuen T. H. et. al. [72]	$T = \frac{1}{g^{sk+\tau}}$	g : Group generator, $\tau = \mathcal{H}(ev)$	Signer & event-binding
Mazumdar S. et. al. [73]	$T = g_{tid}^{sk}$	$g_{tid} = g^{\mathcal{H}(trans.-id)},\ g \in QR(N)$	Signer & transaction-binding
Fujisaki E.[75]	$T = \mathcal{H}(tag)$	$tag = (ev, \mathcal{L})$	Group-dependent
Mu. R. et. al. [76]	$T = \mathcal{H}(\mathcal{L})$	–	Group-dependent
Boyen X. et. al. [85]	$T = \mathcal{E}([d]_{l-v}, [\sum_{i=1}^{k} g^{i-k} h^{k-i} \mathcal{L}]_v)$	$\mathcal{E}$: Multilinear map[b]	Group-dependent
Bouakkaz S. et. al. [87]	$T = \mathcal{H}_2(m \Vert ev \Vert t \Vert Q'_k \Vert sk \Vert pk \Vert r_k)$	$Q'_k = w_i \mathcal{H}_1(ID)\mathcal{G}, t$: timestamp[c]	Randomness
Wang L. et. al. [88]	$T = \mathcal{H}(\mathcal{L} \Vert \mathcal{H}(N) \Vert K)$	N : A key node in MHT[d]	Group-dependent
Li W. et. al. [93]	$T = H_i sk$	$H_i = H_m t,\ H_m : R_q^k \rightarrow R_q^{m\times l}$[e]	Signer-binding
Dharani J. et. al. [94]	$T = VRF(sk, tid)$	VRF[f]	Signer & transaction-binding

[a] $h\&v$: rows/columns in the matrix, q : odd number.

[b] $[d]_{l-v} = \mathcal{H}_{l-v}(t \Vert ev), g, h$: group generators, l : l-multilinear map, k : cardinality of a set, $v = k + (\mathcal{T}\ mod\ b) - 1$, $\mathcal{T}$: The number of time periods, b : key level.

[c] $w_i, r_k :\overset{R}{\leftarrow} Z_q^*$.

[d] MHT : Merkle Hash Tree, $K = g^{r_x} h^{r_y} \prod_{j=1, j\neq i}^{n} z_j^{c_j}, g, h$: group generators, $z_j, r_x, r_y, c_j :\overset{R}{\leftarrow} Z_p$.

[e] k, l, m, q : Setup params, $t = \mathcal{H}(r)s,\ s \overset{R}{\leftarrow} set$.

[f] VRF: Verifiable Random Function, tid : Transaction identifier.

4.2.2. Elliptic curve-based constructions

Most extant works are dependent on this cryptosystem (see Table 7) with the Discrete Logarithm Problem (DLP) as the dominant hardness assumption utilized (specifically, 54.8% of all schemes analyzed in this SLR). Note however that DLP is among the most basic yet hard problem in cryptography although it is not resistant to post-quantum attacks.

4.2.3. Pairing-based constructions

Although LRS based on this employs Elliptic Curve Cryptography (ECC), such constructions typically involve the pairing of algebraic curves where pairing is done between elements of two cryptographic groups to a third group (often called the target group) traditionally via a mapping often denoted as e as follows: $\mathcal{G}_1 \times \mathcal{G}_2 \rightarrow \mathcal{G}_T$. Noteworthy

Table 7
Underlying cryptosystems of linkable ring signature schemes.

Cryptosystem	Schemes	Hardness assumption	Post-quantum secure
Lattices	Ren Y. et. al. [53]	Modulo short integer solution (MSIS)	✓
	Le H. Q. et. al. [30]	Short Integer Solution (SIS)	
	Ren Y. et. al. [66]	Syndrome Decoding (SD), GSD, CF[a]	
	Ferrag M. A. et. al. [68]	NTRU-SIS	
	Li W. et. al. [93]	BDH, MSIS, Module-LWE assumption.	
ECC (No pairing)	Yadav V. K. et. al. [21]	Discrete Logarithm Problem (DLP)	×
	Cai X. et. al. [51]	DLP	
	Yan X. et. al. [54]	Subgroup Decision Problem, l-SDH assumption	
	Li X. et. al. [55]	DLP	
	Jeong I. et. al. [65]	DLP	
	Liu J. K. et. al. [67]	DLP	
	Deng L. et. al. [71]	DLP	
	Yuen T. H. et. al. [72]	SDH, Sub-group decision in $\mathcal{G}_q$, DDHI[b]	
	Mu. R. et. al. [76]	DLP	
	Huang K. et. al. [79]	DLP, CDH, DDHP, GDH[c]	
	Wu T. et. al. [82]	DLP, DDH	
	Yadav V. K. et. al. [84]	DLP, DDH	
	Liu J. et. al. [86]	DLP, DDH	
	Wang L. et. al. [88]	DLP	
ECC (Pairing-based)	Guo L. et. al. [24]	DBDH, Decisional q-BDHI	×
	Cai Y. et. al. [58]	DLP	
	Deng L. et. al. [69]	CDH, DBDH[d]	
	Jeong I. R. et. al. [70]	DLP, DDH, SDH	
	Au M. H. et. al. [74]	DLP, DDH, SDH	
	Fujisaki E. [75]	Sub-group Decision Assumption, SDH, DDHI	
	Huang K. et. al. [78]	DLP, CDH, SDH	
	Boyen X. et. al. [85]	GMDP[e]	
	Bouakkaz S. et. al. [87]	CDH, Inverse CDH (invCDH), modified invCDH	
	Dharani J. et. al. [94]	Generic construction	
Rabin/RSA	Mazumdar S. et. al. [73]	SRSA, LD-RSA[f]	×
Biometric and pairing	Mao X. et. al. [77]	DLP, DDH	×

[a] GSD:General Syndrome Decoding, CF: Codeword Finding.
[b] SDH:Q-Strong Diffie–Hellman, Q'-Decisional Diffie–Hellman Inversion.
[c] CDH: Computational Diffie–Hellman, GDH: Gap Diffie–Hellman.
[d] DBDH: Decisional Bilinear Diffie–Hellman.
[e] GMDP: Generalized Multilinear Decoding Problem (see [85] for specifications).
[f] SRSA: Strong RSA, LD-RSA: Link Decisional RSA.

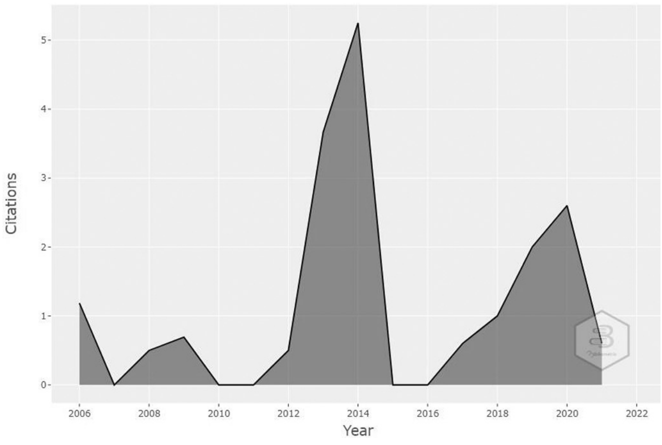

Fig. 4. Average citations per year (See 3 for details.).

is supersingular bilinear groups also referred to as symmetric pairing following the structure $\mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_T$.

Pairing-based cryptography has garnered attention and has successfully been used to design ingenious protocols with optimizations for different platforms including emerging embedded systems already implemented [97]. It is therefore not surprising several LRS schemes [58, 69,74,75,85] are based on them (see Fig. 6 for analysis).

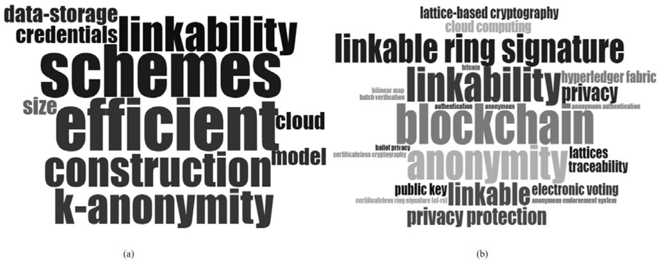

Fig. 5. WordCloud of keywords (a) Keyword-Plus (b) Author-indexed.

4.2.4. Lattice-based constructions

Directly after ECC pairing-based constructions is Lattices (comprising 16.1% of the article pool).

Lattices denote sets of points in n-dimensional spaces composed of a periodic structure and come ingrained with hard problems including Shortest Vector Problem (SVP): an NP-hard problem where the objective is to determine the shortest non-zero vector within a lattice [98].

Unlike the other computational hard problems aforementioned that are vulnerable in the post-quantum era, LRS based on Lattices are resistant to post-quantum adversarial attacks or security against quantum computers. Given that ECC and pairing-based computational hard problems upon which most extant LRS are constructed are not post-quantum secure, it would be refreshing to have more lattice-based constructions. It is however worth mentioning that Lattice-based constructions typically involve the storage and utilization of large keys.

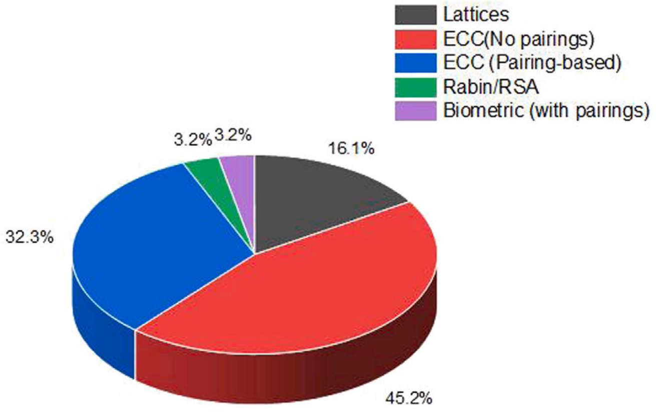

Fig. 6. Cryptosystems underlying LRS schemes.

4.2.5. Biometrics-based constructions

In biometric cryptosystems, cryptographic keys are generated from biometric features or used to secure biometric templates [99].

Our findings show only one article [77] employing a biometric cryptosystem in conjunction with non-interactive zero-knowledge (NIZK) proof and pairings in constructing LRS.

4.3. Extended security guarantees and ring variants

Extant LRS just like classical RS schemes provides *culpability* (the notion that it is impossible for the actual signer to deny that he/she made a ring signature if his/her private key is known). This follows that the actual signer can prove to others that he/she is the actual signer by revealing his/her signing key which is the same in intuition as the notion of *claimability*.

Carefully examining extant LRS works reveal some dynamics about other security guarantees. For instance, the notion of selective linkability [65] has been proposed which affords the signer to prove the linkability of already generated signatures even though at the time of generation the linkability property was not desirable. Concisely, this permits proof of signature linkability post-factum.

We also notice LRS in use in other RS settings including threshold paradigm [72,94] consequently paving way for LRS that enables several signers to sign the same message on behalf of a group. LRS in a redactable RS setting has also been achieved [79]. The work on revocable-iff-linked [74] is equally worth mentioning where the linkability property is leveraged to perform revocation.

4.4. Anonymity guarantee

Anonymity is an inherent security guarantee in RS schemes. Given that vanilla RS schemes provide anonymity in two paradigms: unconditional or computational, extant LRS schemes also follow such paradigms. In Table 8, we provide details in this regard. Notice from Table 8 that computational anonymity is the prevailing anonymity guarantee provided by extant LRS schemes.

4.5. Signature size

Signature-size is a cardinal metric in the evaluation of signature schemes especially ring signatures (RS). Constant-size RS (where signature size is independent of the cardinality of the ring) is often desirable due to usability in both resource-constrained environments (power-limited devices, slower communication network, etc.) and fully-fledged systems. This is so, in that in the case of RS with linear size, the signature size is dependent on the cardinality of the ring hence as the cardinality of the ring increases, so does the signature size consequently posing computational and practical challenges.

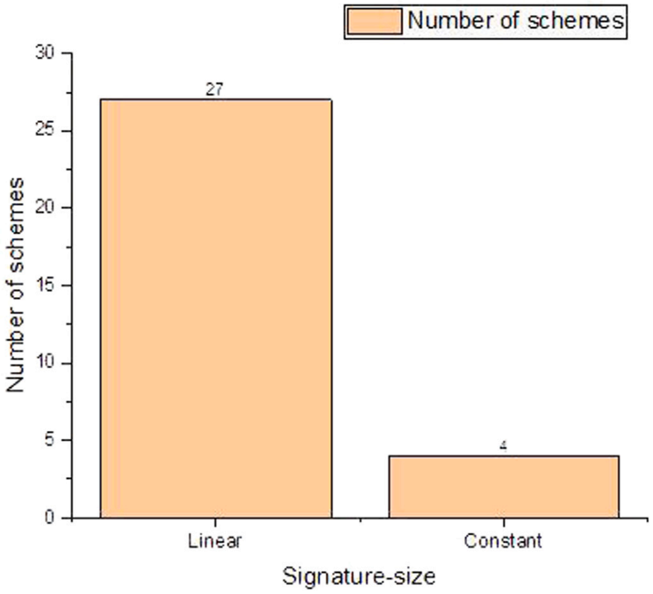

Fig. 7. Signature-size distribution.

Leveraging constant-size RS, signers can increase ring membership for a signature generation without incurring further computational costs thereby strengthening the anonymity guarantee inherent in RS since by design principles, amid a large domain or ring cardinality, anonymity is heightened [100]. Simply put, anonymity is best achieved in numbers hence constant-size RS is best suited to realizing this desire of signers.

We discover that only about 12.9% of extant LRS schemes yield constant signature size (see Fig. 7). In Table 9, we show the signature size of each article reviewed as part of this SLR.

4.6. Instantiations and scheme implementations

LRS schemes reviewed fall into two distinct categories: Schemes fully instantiated using a myriad of programming languages from low-level languages to high-level languages and those that were not. In the case of the latter, researchers primarily employ theoretical analysis based on computational costs and storage overhead after scheme construction for performance analysis against other schemes. In the former, however, diverse programming environments are utilized by researchers with no clear consensus on the implementation environment (see Fig. 8) for instantiation. Implemented schemes constitute 48% (approximately 15 of the articles reviewed). We present our scheme-specific findings based on instantiated schemes in Table 10.

4.7. Use-cases

In this section, we advance findings pertaining to the diverse applicable areas in which LRS have been identified in extant works. For conciseness, we depict a generalized use-case in Fig. 9 and elucidate on specific use cases in subsequent sections.

4.7.1. Blockchain and Cryptocurrency

Unlike fiat currency issued by a central authority (e.g central bank of a country), cryptocurrencies are decentralized requiring no trusted authority. This in part is accomplished by leveraging the decentralized consensus mechanism of the underlying blockchain infrastructure.

Table 8
Level of anonymity guaranteed.

LRS Scheme	*Anonymity guarantee*	
	Unconditional	Computational
Yadav V. K. et. al. [21],Guo L. et. al. [24], Cai X. et. al. [51], Ren Y. et. al. [53]		✓
Yan X. et. al. [54],Ren Y. et. al.[66],Deng L. et. al. [69],Jeong I. R. et. al.[70]		✓
Yuen T. H. et. al. [72],Mazumdar S. et. al. [73], Au M. H. et. al.[74],Fujisaki E.[75]		✓
Mu. R. et. al.[76],Mao X. et. al.[77],Huang K. et. al. [78,79],Yadav V. K. et. al.[84]		✓
Liu J. et. al. [86],Wang L. et. al.[88],Li W. et. al.[93],Dharani J. et. al.[94]		✓
Li X. et. al. [55],Cai Y. et. al.[58],Le H. Q. et. al.[30],Jeong I. et. al.[65],Liu J. K. et. al.[67]	✓	
Ferrag M. A. et. al.[68],Deng L. et. al. [71],Wu T. et. al.[82],Boyen X. et. al. [85]	✓	
Bouakkaz S. et. al. [87]	✓	

Table 9
Signature-size of linkable ring signatures (LRS).

LRS Scheme	*Signature size*	
	$\mathcal{O}(1)$	$\mathcal{O}(n)$
Yadav V. K. et. al.[21],Guo L. et. al.[24],Cai X. et. al.[51],Ren Y. et. al.[53,66],Yan X. et. al.[54]		✓
Le H. Q. et. al.[30],Jeong I. et. al.[65],Liu J. K. et. al.[67],Ferrag M. A. et. al.[68],Deng L. et. al.[69]		✓
Jeong I. R. et. al.[70],Deng L. et. al.[71],Yuen T. H. et. al. [72],Mu. R. et. al.[76],Mao X. et. al.[77]		✓
Huang K. et. al. [78,79],Wu T. et. al.[82],Yadav V. K. et. al.[84],Boyen X. et. al. [85],Liu J. et. al.[86]		✓
Li X. et. al.[55],Cai Y. et. al.[58],Wang L. et. al.[88], Li W. et. al.[93],Dharani J. et. al.[94]		✓
Mazumdar S. et. al. [73],Au M. H. et. al.[74],Fujisaki E.[75],Bouakkaz S. et. al. [87]	✓	

Table 10
Programming environment for scheme instantiation.

LRS Scheme	*Programming environment*						
	PBC[a]	SageMath	Go	Python	C	C++	Java & JPBC[b]
Yadav V. K. et. al. [21]				✓			
Guo L. et. al. [24]							✓
Cai X. et. al. [51]						✓	
Yan X. et. al. [54]							✓
Cai Y. et. al. [58]	✓						
Le H. Q. et. al. [30]		✓					
Ferrag M. A. et. al. [68][c]							
Mazumdar S. et. al. [73]			✓				
Mao X. et. al. [77]				✓			
Huang K. et. al. [78]					✓		
Huang K. et. al. [79]	✓						
Wu T. et. al. [82]							✓
Yadav V. K. et. al. [84]				✓			
Wang L. et. al. [88]						✓	
Dharani J. et. al. [94]			✓				

[a] PBC:Pairing Based Cryptography (PBC) library, a C library.

[b] JPBC: Java pairing-based cryptography (JPBC) library.

[c] Instantiated yet programming environment unspecified by authors.

LRS including [77,93] have been used to carefully balance anonymity enjoyed by users of cryptocurrencies and the need to prevent double-spending (where the same coin is spent more than once by the same owner) under the guise of the inherent anonymity such that the same transaction by the same signer under the same signing key and the event would be detected and discarded by mining nodes owing to the linkability guarantee [36]. LRS has been adopted in designing diverse cryptocurrencies including CryptoNote [101], Monero [102], AEON [103], and Bytecoin [104]. Other LRS like [21,24,51,55,73,76,78,79,82] have been applied in diverse blockchain-driven applications. We notice that this usage comprises the largest application setting of existing LRS schemes.

4.7.2. Electronic voting

Electronic voting (e-voting) [105,106] is another notable use case in which LRS have proved to be a robust and highly efficient cryptographic primitive [67,107]. Given that e-voting must be anonymous yet double-voting-resistant, LRS satisfies such traits courtesy of its anonymity, linkability, and public verifiability guarantees. Successful implementation of e-voting using LRS [19,82,108] have been implemented atop blockchain platforms [20].

4.7.3. Authentication in ad-hoc networks

A characteristic feature of ad-hoc networks is spontaneousity thereby providing a suitable application of ring signatures. However, often as in the case of charging systems [3], it becomes imperative to ascertain whether or not a communication message emanates from the same device as an authentication mechanism. LRS, therefore, support such feature while shielding the device from any deanonymization whatsoever as evident in works like [3–5,29,58,76].

4.7.4. Cloud computing

Clouds provide virtual platforms allowing consumers to store and share data, perform high-performance computing tasks including outsourced computation, subscription services via built-in hosted services, and much more. Unfortunately, as technology advances at light speed, so too have cloud-based security-related threats [109]. Access control mechanisms, therefore, play a cardinal role in the cloud computing paradigm. LRS provides an elevated security control while guaranteeing anonymous access to such platforms consequently allowing Cloud Service Providers (CSPs) to link a user every time a resource is accessed while guaranteeing anonymity. For instance, CSPs may set the access threshold to say n times. The use of LRS like [22,24,88] makes it possible to realize such constraint on consumers as well as other cloud-based requirements.

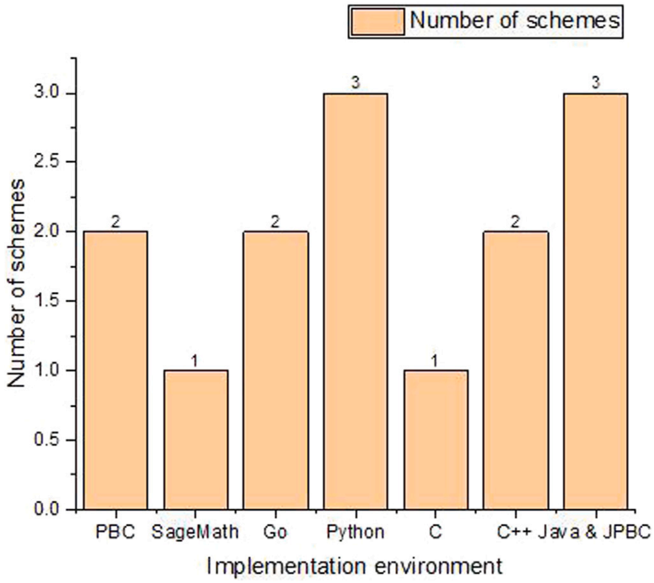

Fig. 8. Programming languages for LRS implementations.

4.7.5. *Smart cities*

Smart city encompasses such areas as smart environments, smart technology including smart grids and vehicles, smart mobility, and smart economy among others geared towards enhancing the liveability of cities [110]. LRS [58,76] have equally found adoption in smart cities and applicable scenarios like location-based Services via linkable location-based services [84] and their related scheme dubbed double authentication prevention [52,80] in smart cities where smart vehicles are integral components. Note, however, that although linkability is desirable in some cases, other researchers [111,112] have a contrary opinion hence eliminate linkability given the fact that it weakens anonymity.

4.7.6. *E-commerce*

E-commerce [113,114] enables internet-based commercial services or transactions at both country and global levels. Unlike classical ring signatures that preclude the possibility of the service-based linkage which is vital for administering discounts or rewards to a loyal customer, LRS makes this a reality while still providing customer anonymity. So far, LRS has been employed in anonymous auctions [78].

5. Discussion and implications

We present in this section a concise discussion and implications of this SLR, posit future works worth exploring as well as some limiting factors of this work.

5.1. *Discussion*

This work performed a systematic review of extant literature on Linkable Ring Signatures (LRS) to understand the status quo and future prospects. To accomplish these, four specific research questions (RQ) were posed. **RQ1** was geared towards better appreciating the current profile of research on LRS and was realized by carefully summarizing works from the top contributors, diverse publication sources, publishers, and trends in publications. **RQ2** sought to find out the applicable settings or domains of LRS and was answered by a discourse on applicable areas as evident in Section 4.7. **RQ3** was aimed at carefully examining extant works to highlight differences in cryptographic constructions, underlying hardness problems, and possible ramifications. To this end, we presented two linkability paradigms (see Tables 11 and 12), intuitions, and ramifications along with their cryptosystems (see Table 7 and Fig. 7). Finally, **RQ4** pertained to the prospects of LRS. We addressed this by analyzing emergent gaps, security guarantees, implementation environments, and signature size of LRS schemes (see Table 9) which is a key metric for evaluating signature schemes as well as post-quantum security (see Table 7) all of which in no doubt provide great insights to guide future research efforts in this domain.

5.1.1. *Linkability computations*

As already mentioned, there exist disparities in the construction of link tags (see Section 4.1). Carefully analyzing the approaches adopted by researchers reveal two paradigms in link tag constructions: Weak and Strong linkability. We concede that our choice of *weak* and *strong* linkability seemingly conveys similar notions introduced in [65]. However, it is worth pointing out the dichotomy between our linkability paradigm and the notions of strong and weak linkability [65] where weak linkability is characterized by the flexibility in generating ring signatures that are either linkable or unlinkable and the inability of the signer to generate a ring signature that is linkable to ring signatures generated by other signers in the ring. Conversely, strong linkability enforces mandatory linkability [65,67]. Contrary to such notions, our linkability paradigms anchored on findings from extant works are based on the signer-binding and deterministic/static trait or "reconstructibility" of the link tag. We present in Tables 11 and 12 a classification of the papers under the two linkability paradigms. For consistency, we maintain the notations used in Table 6. Following, we expatiate upon the two linkability paradigms, suitable applications in which they find relevance, and possible ramifications.

1. Weak linkability: Extant works under this category construct link tags based on non-static or dynamic parameters at the signature generation phase. We note that such constructions are primarily dependent on a public key list (in some cases ordered list), a specified event as ev and a random number generated by the signer. A prevailing style adopted in extant works in this category is group-dependent constructions (constituting 71% of all articles in this category). Note that such linkability only suffices as long as the signer maintains the same ring members in the generation of multiple signatures. In some cases, the construction of the link tag is signer unbinding [75,76].
   Weak linkability although not suitable for cryptocurrencies since they do not provide a full guarantee for double spending prevention (see Section 4.7.1) is applicable in other areas. A candidate instance is group membership tracking where the focus is to determine membership within a specified group [24,54,76].
2. Strong linkability: Seventeen (17) extant works fall under this category as evident in Table 12 comprising the dominant linkability paradigm.
   Strong linkability tags are constructed such that they are both signer binding and decoupled from the ring setting or group. Works characterized by this paradigm all utilize the signing key of the signer together with other publicly verifiable attributes like event identifier (e.g [67,70,74,82]), signer's public key [21,51,55,77], transaction number [73,94], etc. Noteworthy is that event identifier is the prevailing attribute used in the construction of the key image. Its usage constitutes a little over 41% of all articles used in this paradigm.

5.1.2. *Efficiency and security*

We now briefly discuss the computational cost and security properties of extant LRS schemes. We refer the reader to Table 13 for a summary. Under proof model, we show whether the security of the scheme is proved in Random Oracle Model (ROM) or the Standard Model (SM). Under signature and verification phases, we use n, M, E, P and $\mathcal{H}_p$

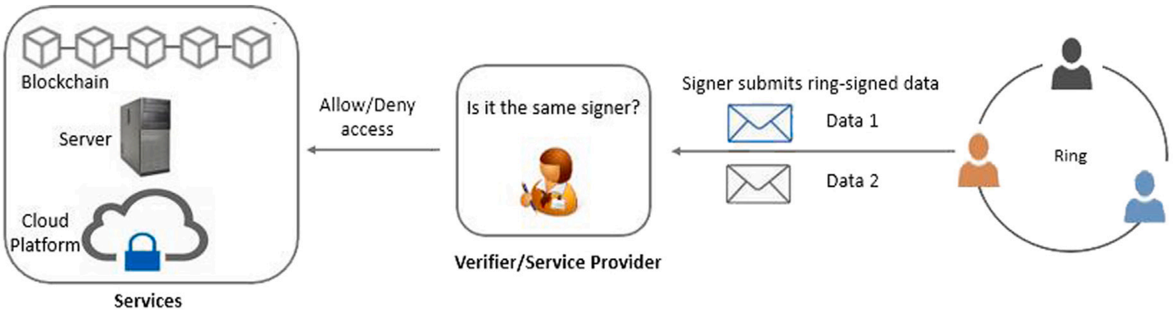

Fig. 9. A generalized high-level use-case of Linkable Ring Signatures.

Table 11
Schemes with weak linkability.

Scheme	Link tag	Meaning of notations	Remark(s)	Reason
Guo L. et. al.[24] Yan X. et. al.[54] Huang K. et. al. [78,79] Yadav V. K. et. al.[84] Liu J. et. al.[86]	$T = h^{sk}$	$h = \mathcal{H}(\mathcal{L})$	Group-dependent	Ad hoc group
Cai Y. et. al.[58]	$T = x_i Q_{ID_i}$	$x_i \overset{R}{\leftarrow} Z_q^*, Q_{ID_i} = \mathcal{H}(ID_i)$	Randomness	Not reconstructible
Jeong I. et. al.[65]	$T = D_0^r$	$D_0 \overset{R}{\leftarrow} \mathcal{G}$ and $r \overset{R}{\leftarrow} \mathbb{Z}$	Randomness	Not reconstructible
Deng L. et. al.[71]	$T = (sk + ht_s)E$	$E = \mathcal{H}_2(ev),\ h = \mathcal{H}_3(ev)$[d]	Randomness	Not reconstructible
Fujisaki E.[75]	$T = \mathcal{H}(tag)$	$tag = (ev, \mathcal{L})$	Group-dependent	Ad hoc group
Mu. R. et. al.[76]	$T = \mathcal{H}(\mathcal{L})$	–	Group-dependent	Ad hoc group
Boyen X. et. al. [85]	$T = \mathcal{E}([d]_{l-v}, [\sum_{i=1}^{k} g^{i-k} h^{k-i} \mathcal{L}]_v)$	$\mathcal{E}$: Multilinear map[a]	Group-dependent	Ad hoc group
Bouakkaz S. et. al.[87]	$T = \mathcal{H}_2(m\|\|ev\|\|t\|\|Q'_k\|\|sk\|\|pk\|\|r_k)$	$Q'_k = w_i \mathcal{H}_1(ID)\mathcal{G}$[b]	Randomness	Not reconstructible
Wang L. et. al.[88]	$T = \mathcal{H}(\mathcal{L}\|\|\mathcal{H}(N)\|\|K)$	N : A key node in MHT[c]	Group-dependent	Ad hoc group

[a] $[d]_{l-v} = \mathcal{H}_{l-v}(t||ev), g, h$: group generators, l : l-multilinear map, k : cardinality of a set, $v = k + (\mathcal{T}\, mod\ b) - 1$, $\mathcal{T}$: Number of time periods, b : key level.

[b] t : timestamp, $w_i, r_k \ :\overset{R}{\leftarrow} Z_q^*$.

[c] MHT : Merkle Hash Tree, $K = g^{r_x} h^{r_y} \prod_{j=1, j\neq i}^{n} z_j^{c_j}$, g, h : group generators, $z_j, r_x, r_y, c_j \ :\overset{R}{\leftarrow} Z_p$.

[d] $t_s \overset{R}{\leftarrow} Z_q^*$.

Table 12
Schemes with strong linkability.

Scheme	Link tag	Meaning of notations	Remark(s)	Reasons
Yadav V.K.et. al.[21] Li X. et. al.[55] Mao X. et. al.[77]	$T = sk\mathcal{H}(pk)$	-	Signer-binding	sk dependent Ring-independent Reconstructible
Cai X. et. al.[51]	$T = l_i pk$	$l_i = \mathcal{H}(pk, ID_i)$	Signer-binding	
Ren Y. et. al.[53,66]	$T = Bsk$	$B \leftarrow R_q^{h\times v}$,[a]	Signer-binding	
Liu J. K. et. al.[67] Jeong I. R. et. al.[70] Au M. H. et. al.[74] Wu T. et. al.[82]	$T = e^{sk}$	$e = \mathcal{H}(ev)$	Signer & event-binding	
Le H. Q. et. al.[30]	$T = Ksk$	$K = \mathcal{H}(ev)$	Signer & event-binding	
Ferrag M. A. et. al.[68]	$T = t_{k,1} + t_{k,2}$	$t_{k,i}$: $sk_i * master\ pk$	Signer-binding	
Deng L. et. al.[69]	$T = e(E, D_s)$	$E = \mathcal{H}(ev),\ D_s = \mathcal{H}(ID_i)$	Signer & event-binding	
Yuen T. H. et. al.[72]	$T = \frac{1}{g^{sk+\tau}}$	g : Group generator, $\tau = \mathcal{H}(ev)$	Signer & event-binding	
Mazumdar S. et. al.[73]	$T = g_{tid}^{sk}$	$g_{tid} = g^{\mathcal{H}(Tnx.-id)},\ g \in QR(N)$	Signer & Tnx-binding[d]	
Li W. et. al.[93]	$T = H_i sk$	$H_i = H_m t,\ H_m : R_q^k \rightarrow R_q^{m\times l}$[b]	Signer-binding	
Dharani J. et. al.[94]	$T = VRF(sk, tid)$	VRF[c]	Signer & Tnx-binding	

[a] $h\&v$: rows/columns in the matrix, q : odd number.

[b] k, l, m, q : Setup params, $t = \mathcal{H}(r)s$, $s \overset{R}{\leftarrow} set$.

[c] VRF: Verifiable Random Function, tid : Transaction identifier.

[d] Tnx : Transaction.

to denote the cardinality of the ring, Scaler Multiplication, Exponentiation, Bilinear Pairing, and Hash-to-Point cryptographic operations respectively. We also use k and l to denote small integers.

Security-wise, ROM is the dominant proof model (see Table 13). ROM schemes are generally more efficient with the proofs anchored on well-studied computational assumptions. Compared to the security of ad-hoc cryptographic schemes, modeling security in ROM is a better alternative and hence viewed as a “bridge” between theory and practical instantiation [115]. It is however noteworthy that unlike security proofs in ROM, SM accurately offers assumptions or suppositions that are sufficient to guarantee security properties given that proof in ROM is just an indication that an attack that does not break the proof assumptions must exploit a property not satisfied by the underlying random-oracle simulation of the security proof. Consequently, schemes might be secure in ROM yet insecure in SM [116].

Table 13
Comparison of efficiency and security.

PKI	Scheme	Security	Model	Signature phase	Verification phase
PKC	Yadav V. K. et. al.[21]	✓	ROM	$(2n+3)M+2\mathcal{H}_p$	$4nM+\mathcal{H}_p$
	Guo L. et. al.[24]	✓	ROM	$2nM+(4n+3)E+\mathcal{H}_p$	$2nM+4nE+\mathcal{H}_p$
	Cai X. et. al.[51]	✓	ROM	$(5n+3)M+\mathcal{H}_p$	$4M+\mathcal{H}_p$
	Ren Y. et. al.[53][f]	✓	ROM	$1.5n+2.375KB$	$1.5n+2.375KB$
	Yan X. et. al.[54]	✓	ROM	$2nM+(4n+3)E+\mathcal{H}_p$	$2nM+4nE+\mathcal{H}_p$
	Li X. et. al.[55]	✓	ROM	$(6n-4)M+\mathcal{H}_p$	$4nM+\mathcal{H}_p$
	Jeong I. et. al.[65]	✓	ROM	$nM+(2n+1)E$	$(n+1)M+(2n+2)E$
	Ren Y. et. al.[66][f]	✓	ROM	$(1+(n+1)w-k)s\ bits$	$(1+(n+1)w-k)s\ bits$
	Liu J. K. et. al.[67]	✓	ROM	$(n+4)M+\mathcal{H}_p$	$(n+4)M+\mathcal{H}_p$
	Yuen T. H. et. al.[72]	✓	SM	$(n+10\sqrt{n}+10)M$	$(8\sqrt{n}+10)P+2M$
	Mazumdar S. et. al.[73]	✓	ROM	$5M+13E+\mathcal{H}_p$	$10M+6E$
	Fujisaki E.[75]	✓	SM	$(n+2)M+(n+7)E+NZ+OtS$	$6P+M+(n+1)E+NZ+OtSV$[a]
	Mao X. et. al.[77]	✓	ROM	$25unE+un\mathcal{H}_p$	$2.7unE+un\mathcal{H}_p$[b]
	Huang K. et. al.[78]	✓	ROM	$2nM+(2n+3)E+\mathcal{H}_p$	$2nM+3nE+\mathcal{H}_p$
	Huang K. et. al.[79]	✓	ROM	$(4n-1)M+(5n-1)E+\mathcal{H}_p$	$(3n+1)M+(2n+2)E+\mathcal{H}_p$
	Wu T. et. al.[82]	✓	ROM	$(n+2)M+(n+6)E$	$3nM+4nE$
	Yadav V. K. et. al.[84]	✓	ROM	$2nM+(4n+3)E+\mathcal{H}_p$	$2nM+4nE+\mathcal{H}_p$
	Boyen X. et. al.[85]	✓	ROM	$nP+nM$	$nP+nM$
	Liu J. et. al.[86]	✓	ROM	$2nM+(4n+3)E+\mathcal{H}_p$	$2nM+4nE+\mathcal{H}_p$
	Wang L. et. al.[88]	✓	ROM	$(n+1)E$	$(n+2)E$
	Li W. et. al.[93][f]	✓	ROM	$B_\theta\times(SS^l_{y-2\theta n})^r\times R^m_q$	$B_\theta\times(SS^l_{y-2\theta n})^r\times R^m_q$
	Dharani J. et. al.[94]	✓	ROM	$3E+zkS+3Enc+6VRF+OTS$	$2E+zkS+OtSV$[c]
IBC	Cai Y. et. al.[58]	✓	ROM	$P+(2n+6)M$	$3P+M$
	Le H. Q. et. al.[30][f]	✓	ROM	$n(a+bk+b).D_\sigma+1.S^a_w+b^2.\mathbb{Z}_q$	$n(a+bk+b).D_\sigma+1.S^a_w+b^2.\mathbb{Z}_q$
	Ferrag M. A. et. al.[68]	✓	ROM	$2wnT_{SD}+w(n+1)T_1+2wT_{RS}$	wT_1[d]
	Deng L. et. al.[69]	✓	ROM	$4P+(n+1)M+\mathcal{H}_p$	$3P+nM+E+\mathcal{H}_p$
	Jeong I. R. et. al.[70]	✓	ROM	$2M+5E$	$3E$[e]
	Au M. H. et. al.[74]	✓	ROM	$(2n+4)M+E+\mathcal{H}_p$	$12P+8M+9E+\mathcal{H}_p$
	Mu. R. et. al.[76]	✓	ROM	$(6n-3)M+\mathcal{H}_p$	$(4n-4)M+\mathcal{H}_p$
CLPKC	Deng L. et. al. [71]	✓	ROM	$(4n-1)M+\mathcal{H}_p$	$(4n+2)M+\mathcal{H}_p$
	Bouakkaz S. et. al.[87]	✓	ROM	$4M$	$2P+M$

[a] NZ: Non-interactive Zero-Knowledge proof, OTS: One-time Signature, OtSV: OTS verification.

[b] u denotes length of each public key.

[c] zkS:zk-SNARK, Enc: Encryption, VRF: Verifiable Random Function, OTS: One-time Signature, OtSV: OTS verification.

[d] w, T_{SD}, T_{RS} and T_1 denote a positive integer, time spent for discrete Gaussian sampling algorithm, time spent for algorithm rejection sampling run once, time cost running polynomial–polynomial multiplication respectively.

[e] Excludes zero-knowledge SPK verification.

[f] Shows signature size. w, s denote a positive integer and security bits respectively, $k = w/2$, a, b: Size of matrix, B_θ, SS :Sets, R : Matrix.

Also, ROM is characterized by two fundamental problems: (1) Does not consider adversaries with quantum capabilities. (2) Falls short of capturing non-uniform adversaries capable of performing preprocessing. It would therefore be interesting to have LRS proven in a generalized notion of ROM known as quantum ROM (QROM) and QROM equipped with auxiliary input (QROM-AI) [117] to comprehensively address the aforementioned problems. This is imperative given that even extant lattice-based LRS schemes are proven secure in ROM. Note however that although proofs in QROM are stronger as compared to ROM, such security does not imply SM security and that both ROM and QROM are closer to each other than either is to SM security [118].

5.1.3. *Privacy analysis*

Given that LRS guarantees a notion of privacy dubbed anonymity, it becomes imperative to measure the level of such privacy. Taking cues from [119,120], we note that anonymity entails *unidentification* or better still *indistinguishability* amid entities with potentially the same characteristics. Given that by its nature LRS like classical RS enables the signer to conscript diversion group members (non-signers) who are oblivious to such inclusion thereby not disclosing the actual signer, ring members possess the same characteristic and are plausible signers. This shares striking characteristics with a recent notion where privacy metrics comprised anonymity, untraceability, unlinkability, unforgeability, and confidentiality [121]. Percentage-wise, we model this as Privacy Level (PL) in Eq. (1).

$$Privacy\ Level(PL) = \frac{Guaranteed\ privacy}{Privacy\ metrics} \times 100\% \tag{1}$$

Secure LRS fulfills three (anonymity, untraceability, and unforgeability) thus achieving a PL of 60%. Note that confidentiality is not provided unlike ring confidential transactions (RingCT). It is therefore not surprising [111,112,122] point out that the linkability feature in itself weakens privacy as compared to the unlinkability inherent in vanilla RS. This even excludes the fact that diversion group members can repudiate the ring signature. Considering repudiability further reduces the PL of LRS to exactly 50% whereas vanilla RS attain 66.7%.

The weakened privacy becomes more obvious when the security model of LRS and vannila RS are juxtaposed. Concretely, in LRS (modeled as *L-anonymity*), the adversary $\mathcal{A}$ cannot query signatures (σ_τ) of a user (ID_τ) who appears in the challenge phase. The principle is thus straightforward. Once $\mathcal{A}$ obtains σ_τ, it can determine if the challenge signature is generated by ID_τ given the inherent linkability.

In furtherance of the aforementioned, [123] advances seven levels of anonymity (in decreasing levels of anonymity): Full Anonymity, Linkable anonymity, Revocable-iff-linked anonymity, Revocable anonymity, Linkable and revocable anonymity, Revocable-iff-Linked and revocable anonymity, and the seventh one being no anonymity. We refer the curious reader to [123] for the explanation of the various classifications. In no doubt, LRS is captured in category two consequently falling short of full anonymity in terms of privacy. In light of the above, it is also worth noting that compared with LRS that have strong linkability guarantees, their counterparts with weak linkability provide stronger anonymity hence a heightened level of privacy owing to limited exposure. Note, however, that in both cases, the user is never deanonymized.

5.1.4. *Future application scenarios*

Although LRS schemes have found relevance in a myriad of use cases, we envision them playing other equally pivotal roles in future application settings. Below, we briefly elucidate some areas.

- *Public bulletin boards*: Public Bulletin Boards (PBB) act as broadcast media allowing parties involved in a protocol (in the cryptographic sense) to publish messages under the guarantee that none of the messages can be modified or deleted. Conceptually, PBB can be likened to an online forum or more generally, social media platform. With the gradual proliferation of decentralized, P2P anonymous social media platforms as alternatives to mainstream social media platforms like Facebook and Twitter owing to privacy concerns, LRS can play an immense role where users post ring-signed comments/posts/information. This way, leveraging the linkability guarantee, posts from specific users can be trusted based on the credibility of prior posts while guaranteeing user anonymity.
- *Bike/Scooter sharing services*: In some parts of the world (e.g. China, Denmark, Japan, etc.), bike sharing is a common phenomenon. Often, a common challenge has to do with anonymously monitoring (some sort of tracking feature with guaranteed anonymity) misbehaving commuters/users (e.g users who park haphazardly, destroy bikes, etc.) thereby preventing reoccurrence. The intuition here is to for instance deny subsequent access to services in the setting of a smart city where users may desire to use such services anonymously while encouraging responsible use. By seamlessly integrating LRS into the current workflow, this can be realized so although users use services anonymously, misbehavior can be detected. This way, users enjoy anonymity interlaced with subtle accountability. This can easily be extended to car-hailing services.
- *Anonymous auctions*: In online auctions, parties would often prefer to be anonymous. For instance, in a competitive market setting, parties would wish not to reveal their interests or preferences to competitors [124]. Besides, in some existing deployed auction platforms (for instance, eBay), a user can play dual roles: not only a bidder but also an auctioneer. Guaranteeing the credibility of anonymous users in such a setting can be a challenging task. LRS can easily resolve this complexity in current and future anonymous auctions where users (bidders and auctioneer) sign transactions which can be aggregated and later inferred to determine user legitimacy or credibility across diverse auctions. The notion of anonymity with linkability can even be extended to other e-commerce platforms.
- *Mobile crowdsourcing and crowdsensing*: In recent years, two burgeoning computing paradigms have been mobile crowdsourcing and crowdsensing. In the former, large groups of smart devices perform diverse tasks remotely either cooperatively or non-cooperatively [125]. The latter gravitates towards urban sensing for data sensing and collection leveraging built-in features of mobile or handheld devices. An obvious barrier to both technologies is user privacy-preservation with some studies employing randomizable techniques to protect user identities [126,127]. Closely tied to the quest for user privacy is a reward mechanism to users for resources expended. We envision LRS resolving these seemingly conflicting requirements by guaranteeing anonymity to users while making it possible to identity specific anonymous users to be compensated or rewarded anonymously. Such guarantees would further motivate users to opt-in for such computing paradigms consequently strengthening the industry 4.0 agenda.
- *Remote attestation*: User and platform configuration privacy are often cardinal requirements in anonymous remote attestation (RA) solutions. Techniques used to realize these include anonymous signature schemes like Direct Anonymous Attestation (DAA) [128] and more recently group signature [129]. Given spontaneity and ease in the use of ring signatures (RS) allowing diversion group members (non-signers) who may be unaware of being conscripted, RS and particularly LRS could be explored to further augment the inherent credibility or trustworthy mechanisms of RA while preserving security and privacy.
- *High-Performance Computing (HPC) platforms*: HPC systems offer large-scale computing infrastructures usable by registered users from diverse research institutions, university faculties, and companies among others. HPC systems are multi-tenant platforms owned by a specific organization, entity, or consortium with vested interests. With such systems come user privacy issues and other security threats including insider threats by legitimate users [130]. Balancing privacy and security can be a daunting task in such an environment. We envision access control merged with LRS in the future mitigating such threats while guaranteeing privacy.

5.2. Implications for research and practice

Given the current surge and popularity in cryptocurrencies, digital assets [131–133], and future use cases, it is vital for industry experts and developers to adopt LRS with the linkability paradigm that best suits their use-case. For instance, practitioners interested in developing anonymous cryptocurrencies cannot opt for LRS with weak linkability as it cannot withstand double-spending tendencies.

In light of the above and based on our findings on the two linkability paradigms aforementioned and elucidated in Section 4.1, we formulate a five-point questionnaire as a checklist where each response should be in the affirmative to guide prospective researchers and developers to realize strong linkability.

- Is the key image computed from publicly verifiable values?
- Is the key image binding to the signer in totality?
- Under the same, publicly verifiable values and signer attributes, is the key image reconstructible?
- Does the key image remain static from ring to ring? In other words, is the key image independent of ring membership?
- Can the signer sign only once with the key image without the signature being rejected?

We envision this checklist serving as a blueprint to provide guidance, especially in use-cases where strong linkability is desirable.

Also, the instantiation/implementation of cryptographic schemes is essential for robust performance analysis. Given the diversity in underlying cryptosystems and non-uniformity in programming environments for LRS instantiations, researchers and system developers often resort to theoretical analysis or limited-scope performance analysis. For instance, in their work, [54] could only be instantiated and compared to an existing scheme because both schemes were constructed in composite order groups whereas several schemes were constructed in prime order groups. The authors noted that the time cost of a Tate pairing on a 1024-bit composite order elliptic curve (EC) is around 50 times larger than that of the same pairing on a prime order EC with the same security level hence based on the principle of fairness singled out a scheme for evaluation resulting in limited-scope performance analysis. Such narrow performance analysis is further exacerbated by the non-uniformity in implementation environments as explicated in this work. This insight should be of guidance for both researchers and developers to work towards a wider performance-based analytical approach.

5.3. Challenges and future research directions

We now highlight some research areas of LRS requiring more investigations from the researcher community.

Given the limited construction of LRS that are post-quantum-secure, future works could consider more constructions that can resist quantum adversarial attacks. This is imperative given rapid advances in the field of quantum computing thereby gradually posing threat to traditional cryptosystems. Future research could therefore explore other post-quantum secure cryptosystems like Multivariate public key cryptosystems (MPKCs), Supersingular Elliptic Curve Isogeny Cryptosystems, and

Hybrid Cryptosystems [98,134] as well as those based on other lattice-based hardness assumptions which are resource-constrained friendly 1u [135]. This need for more post-quantum secure LRS schemes is justifiable given the aforementioned finding that DLP is presently the dominant hardness assumption underlying LRS constructions although it is not post-quantum secure.

Again, the extant works show diversity in the construction of link tags. To this end, future works could focus on link tags constructed based on other signer-binding and publicly verifiable parameters aside *event*. To this end, other options like biometric cryptosystem [99,136] could be considered to further contribute to signer-binding link tags.

Also, considering the limited number of constant-size LRS schemes and the need for such constructions, future works could redirect enthusiasm in this direction. Towards this end, a lacuna worth filling would be an LRS scheme that is unconditionally anonymous, constant signature-size, and quantum-resistant at the same time with security modeled in the standard model.

Another future work worth exploring is further expanding security guarantees of extant LRS schemes. Given that not quite long ago, definitions for *unrepudiability* and *unclaimability* among others were formalized [137] for RS and supported by constructions, it would be interesting to have the tentacles of LRS extended to embody such security guarantees to withstand scenarios of users under duress and where an employer, institution or authoritarian government may coercively compel users to repudiate or prove authorship for a known signature. Note that the provable inability of individuals to convincingly do so would certainly be pivotal to the existence of the individual in such a hostile environment. Such an LRS scheme would in no doubt further provide privacy protection for the signer.

5.4. Limitations of the study

The findings of the SLR should be considered in tandem with its limitations. We focused primarily on peer-reviewed journals available in specified scholarly databases. As a consequence, other publications on conference papers, books, preprints, book chapters, etc. were excluded. Again, notwithstanding the use of citation chaining, it is possible certain articles that appear solely in the ACM and Scopus were not included. We envision these limiting factors may find resolution in future studies through the inclusion of other scholarly databases thereby expanding the scope of the assimilated information.

6. Concluding remarks

The construction of ring signature schemes has garnered massive support from the researcher community right from its inception in 2001 leading to diverse security guarantees, one being linkability. This study, therefore, conducts a systematic literature review (SLR) based on publications from four well-known scholarly databases to understand the state-of-the-art of linkable ring signatures (LRS), intricacies in the constructions, link tag or signature image, inherent security and privacy guarantees, specific use-cases, signature sizes, cryptosystems that underpin the constructions and security ramifications. Findings from the SLR are used to summarize extant knowledge in LRS while providing avenues for further research in this domain.

CRediT authorship contribution statement

Justice Odoom: Conceptualization, Methodology, Writing – original draft. **Xiaofang Huang:** Formal analysis, Supervision, Funding acquisition. **Zuhong Zhou:** Review & editing, Funding acquisition. **Samuel Danso:** Methodology, Writing – review & editing. **Jinan Zheng:** Methodology, Data curation. **Yanjie Xiang:** Methodology, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001, pp. 552–565.

[2] D. Chaum, E. van Heyst, Group signatures, in: D.W. Davies (Ed.), Advances in Cryptology — EUROCRYPT '91, Springer, Berlin Heidelberg, 1991, pp. 257–265.

[3] L.F. Roman, P.R. Gondim, Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment, Ad Hoc Netw. (ISSN: 1570-8705) 97 (2020) 102004, http://dx.doi.org/10.1016/j.adhoc.2019.102004.

[4] C. Lai, Z. Ren, X. Li, Q. Jiang, Q. Cheng, J. Ma, Fast and universal inter-slice handover authentication with privacy protection in 5G network, Secur. Commun. Netw. (ISSN: 1939-0114) (2021) http://dx.doi.org/10.1155/2021/6694058.

[5] P. Mundhe, S. Verma, S. Venkatesan, A comprehensive survey on authentication and privacy-preserving schemes in VANETs, Comp. Sci. Rev. (ISSN: 1574-0137) 41 (2021) 100411, http://dx.doi.org/10.1016/j.cosrev.2021.100411.

[6] Y. Lu, Q. Tang, G. Wang, ZebraLancer: Private and anonymous crowdsourcing system atop open blockchain, in: 2018 IEEE 38th International Conference on Distributed Computing Systems, ICDCS, 2018, pp. 853–865, http://dx.doi.org/10.1109/ICDCS.2018.00087.

[7] J. Camenisch, M. Drijvers, A. Lehmann, Universally composable direct anonymous attestation, in: Public-Key Cryptography – PKC 2016, vol. 9615, Springer, Berlin Heidelberg, ISBN: 978-3-662-49386-1, 2016, pp. 234–264, http://dx.doi.org/10.1007/978-3-662-49387-8_10.

[8] Y. Fajiang, C. Jing, X. Yang, Z. Jiacheng, Z. Yangdi, An efficient anonymous remote attestation scheme for trusted computing based on improved CPK, Electronic Commerce Research 19 (2019) 1572–9362, http://dx.doi.org/10.1007/s10660-019-09366-3.

[9] B. Petros, J. Huang, J. Chen, H.-J. Zhang, Z.-Y. Sun, S. He, A remote attestation mechanism using a threshold ring signature for a perception layer of distributed networking, Wirel. Commun. Mob. Comput. 2022 (2022) 1530–8669, http://dx.doi.org/10.1155/2022/6603754.

[10] H. Wang, D. He, Z. Liu, R. Guo, Blockchain-based anonymous reporting scheme with anonymous rewarding, IEEE Trans. Eng. Manage. 67 (4) (2020) 1514–1524, http://dx.doi.org/10.1109/TEM.2019.2909529.

[11] X. Li, Y. Mei, J. Gong, F. Xiang, Z. Sun, A blockchain privacy protection scheme based on ring signature, IEEE Access 8 (2020) 76765–76772, http://dx.doi.org/10.1109/ACCESS.2020.2987831.

[12] F. Li, Z. Liu, T. Li, H. Ju, H. Wang, H. Zhou, Privacy-aware PKI model with strong forward security, Int. J. Intell. Syst. (2020) http://dx.doi.org/10.1002/int.22283.

[13] C. Duan, Y. Wu, L. Song, L. Liu, The new method of sensor data privacy protection for IoT, Shock Vib. 2021 (2021) http://dx.doi.org/10.1155/2021/3920579.

[14] G. Mwitende, Y. Ye, I. Ali, F. Li, Certificateless authenticated key agreement for blockchain-based WBANs, J. Syst. Archit. (ISSN: 1383-7621) 110 (2020) 101777, http://dx.doi.org/10.1016/j.sysarc.2020.101777.

[15] Z. Chen, C. Fiandrino, B. Kantarci, On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey, J. Syst. Archit. (ISSN: 1383-7621) 115 (2021) 102011, http://dx.doi.org/10.1016/j.sysarc.2021.102011.

[16] B. Adam, Bitcoins with homomorphic value (validatable but encrypted), 2015, URL https://bitsharestalk.org/index.php/topic,16797.msg214814.html#msg214814. (Accessed on 8 February 2022).

[17] A.K. Kwansah Ansah, D. Adu-Gyamfi, S. Anokye, Privacy preservation of users in P2P E-payment system*, in: 2019 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT, 2019, pp. 1–8, http://dx.doi.org/10.1109/ICECCT.2019.8869354.

[18] X. Liu, M. Zhang, Y. Zheng, Y. Yang, A linkable ring signature electronic cash scheme based on blockchain, in: 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 1–4, http://dx.doi.org/10.1109/SmartBlock52591.2020.00037.

[19] P. Li, J. Lai, Y. Wu, Event-oriented linkable and traceable anonymous authentication and its application to voting, J. Information Security and Applications (ISSN: 2214-2126) 60 (2021) 102865, http://dx.doi.org/10.1016/j.jisa.2021.102865.

[20] M. Pawlak, A. Poniszewska-Marańda, Trends in blockchain-based electronic voting systems, Inf. Process. Manage. (ISSN: 0306-4573) 58 (4) (2021) 102595, http://dx.doi.org/10.1016/j.ipm.2021.102595.

[21] V.K. Yadav, N. Andola, S. Verma, S. Venkatesan, P2LBS: Privacy provisioning in location-based services, IEEE Trans. Serv. Comput. (2021) 1, http://dx.doi.org/10.1109/TSC.2021.3123428.

[22] X. Huang, J.K. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, J. Zhou, Cost-effective authentic and anonymous data sharing with forward security, IEEE Trans. Comput. 64 (4) (2015) 971–983, http://dx.doi.org/10.1109/TC.2014.2315619.

[23] Z. Wang, J. Fan, Flexible threshold ring signature in chronological order for privacy protection in edge computing, IEEE Trans. Cloud Comput. (2020) 1, http://dx.doi.org/10.1109/TCC.2020.2974954.

[24] L. Guo, Q. Wang, W.-C. Yau, Online/offline rewritable blockchain with auditable outsourced computation, IEEE Trans. Cloud Comput. (2021) 1, http://dx.doi.org/10.1109/TCC.2021.3102031.

[25] S.S.M. Chow, Identity-based strong multi-designated verifiers signatures, in: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure, Springer, Berlin Heidelberg, 2006, pp. 257–259, http://dx.doi.org/10.1007/11774716_23.

[26] S.S.M. Chow, W. Susilo, T.H. Yuen, Escrowed linkability of ring signatures and its applications, in: P.Q. Nguyen (Ed.), Progress in Cryptology - VIETCRYPT 2006, Springer, Berlin Heidelberg, 2006, pp. 175–192, http://dx.doi.org/10.1007/11958239_12.

[27] S. Chow, K.-K.R. Choo, Strongly-secure identity-based key agreement and anonymous extension, in: Information Security, vol. 2007, ISBN: 978-3-540-75495-4, 2007, p. 18, http://dx.doi.org/10.1007/978-3-540-75496-1_14,

[28] S. Chow, W. Susilo, Generic construction of (identity-based) perfect concurrent signatures, in: Information and Communications Security, vol. 2006, ISBN: 978-3-540-30934-5, 2006, p. 361, http://dx.doi.org/10.1007/11602897_17,

[29] J.K. Liu, V.K. Wei, D.S. Wong, Linkable spontaneous anonymous group signature for ad hoc groups, in: Australasian Conference on Information Security and Privacy, Springer, 2004, pp. 325–335.

[30] H.Q. Le, B. Vo, D.H. Duong, W. Susilo, N.T. Le, K. Fukushima, S. Kiyomoto, Identity-based linkable ring signatures from lattices, IEEE Access 9 (2021) 84739–84755, http://dx.doi.org/10.1109/ACCESS.2021.3087808.

[31] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. (ISSN: 1084-8045) 126 (2019) 45–58, http://dx.doi.org/10.1016/j.jnca.2018.10.020, URL https://www.sciencedirect.com/science/article/pii/S1084804518303485.

[32] J. Bernal Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R. Torres Moreno, A. Skarmeta, Privacy-preserving solutions for blockchain: Review and challenges, IEEE Access 7 (2019) 164908–164940, http://dx.doi.org/10.1109/ACCESS.2019.2950872.

[33] H. Xiong, Z. Qin, F. Li, A taxonomy of ring signature schemes: Theory and applications, IETE J. Res. 59 (4) (2013) 376–382, http://dx.doi.org/10.4103/03772063.2013.10876518.

[34] L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains, J. Netw. Comput. Appl. 127 (2019) 43–58.

[35] D. Wang, J. Zhao, Y. Wang, A survey on privacy protection of blockchain: The technology and application, IEEE Access 8 (2020) 108766–108781, http://dx.doi.org/10.1109/ACCESS.2020.2994294.

[36] N. Andola, Raghav, V.K. Yadav, S. Venkatesan, S. Verma, Anonymity on blockchain based e-cash protocols—A survey, Comp. Sci. Rev. (ISSN: 1574-0137) 40 (2021) 100394, http://dx.doi.org/10.1016/j.cosrev.2021.100394, URL https://www.sciencedirect.com/science/article/pii/S1574013721000344.

[37] L. Wang, G. Zhang, C. Ma, A survey of ring signature, Front. Electr. Electron. Eng. China (ISSN: 1673-3584) 3 (2008) http://dx.doi.org/10.1007/s11460-008-0012-8.

[38] M.N.S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, K. Sakurai, A survey on group signatures and ring signatures: Traceability vs. anonymity, Cryptography (ISSN: 2410-387X) 6 (1) (2022) http://dx.doi.org/10.3390/cryptography6010003, URL https://www.mdpi.com/2410-387X/6/1/3.

[39] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof systems, SIAM J. Comput. 18 (1) (1989) 186–208, http://dx.doi.org/10.1137/0218012.

[40] C. Gentry, Fully homomorphic encryption using ideal lattices, in: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, 2009, pp. 169–178.

[41] T. Nakanishi, T. Fujiwara, H. Watanabe, A linkable group signature and its application to secret voting, Trans. Inf. Process. Soc. Japan 40 (7) (1999) 3085–3096.

[42] H. Zheng, Q. Wu, b. Qin, L. Zhong, S. He, J. Liu, Linkable group signature for auditing anonymous communication, Springer International Publishing, ISBN: 978-3-319-93637-6, 2018, pp. 304–321, http://dx.doi.org/10.1007/978-3-319-93638-3_18.

[43] A. El Kaafarani, L. Chen, E. Ghadafi, J. Davenport, Attribute-based signatures with user-controlled linkability, in: D. Gritzalis, A. Kiayias, I. Askoxylakis (Eds.), Cryptology and Network Security, Springer International Publishing, Cham, 2014, pp. 256–269.

[44] M. Urquidi, D. Khader, J. Lancrenon, L. Chen, Attribute-based signatures with controllable linkability, in: M. Yung, J. Zhang, Z. Yang (Eds.), Trusted Systems, Springer International Publishing, 2016, pp. 114–129, http://dx.doi.org/10.1007/978-3-319-31550-8_8.

[45] A. El Kaafarani, E. Ghadafi, Attribute-based signatures with user-controlled linkability without random oracles, in: M. O'Neill (Ed.), Cryptography and Coding, Springer International Publishing, Cham, 2017, pp. 161–184, http://dx.doi.org/10.1007/978-3-319-71045-7_9.

[46] J. Mao, Linkability analysis of some blind signature schemes, in: Y. Wang, Y.-m. Cheung, H. Liu (Eds.), Computational Intelligence and Security, Springer, Berlin, Heidelberg, 2007, pp. 556–566, http://dx.doi.org/10.1007/978-3-540-74377-4_58.

[47] E. Fujisaki, K. Suzuki, Traceable ring signature, in: Public Key Cryptography – PKC 2007, vol. E91.A, ISBN: 978-3-540-71676-1, 2007, pp. 181–200, http://dx.doi.org/10.1007/978-3-540-71677-8_13,

[48] H. Feng, J. Liu, D. Li, Y.-N. Li, Q. Wu, Traceable ring signatures: general framework and post-quantum security, Des. Codes Cryptogr. 89 (2021) http://dx.doi.org/10.1007/s10623-021-00863-x.

[49] K. Gu, X. Dong, L. Wang, Efficient traceable ring signature scheme without pairings, Adv. Math. Commun. 14 (2) (2020) 207–232.

[50] L. Han, S. Cao, X. Yang, Z. Zhang, Privacy protection of VANET based on traceable ring signature on ideal lattice, IEEE Access 8 (2020) 206581–206591, http://dx.doi.org/10.1109/ACCESS.2020.3038042.

[51] X. Cai, Y. Ren, X. Zhang, Privacy-protected deletable blockchain, IEEE Access 8 (2020) 6060–6070, http://dx.doi.org/10.1109/ACCESS.2019.2962816.

[52] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, H. Zhang, Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks, Tsinghua Sci. Technol. 24 (5) (2019) 575–584, http://dx.doi.org/10.26599/TST.2018.9010131.

[53] Y. Ren, H. Guan, Q. Zhao, An efficient lattice-based linkable ring signature scheme with scalability to multiple layer, J. Ambient Intell. Humaniz. Comput. (2021) http://dx.doi.org/10.1007/s12652-021-03092-1.

[54] X. Yan, X. He, J. Yu, Y. Tang, White-box traceable ciphertext-policy attribute-based encryption in multi-domain environment, IEEE Access 7 (2019) 128298–128312, http://dx.doi.org/10.1109/ACCESS.2019.2939413.

[55] X. Li, Y. Mei, J. Gong, F. Xiang, Z. Sun, A blockchain privacy protection scheme based on ring signature, IEEE Access 8 (2020) 76765–76772, http://dx.doi.org/10.1109/ACCESS.2020.2987831.

[56] J. Odoom, X. Huang, L. Wang, Stateless forward-secure key-insulated linkable ring signature scheme in ID-based setting, J. Syst. Archit. (ISSN: 1383-7621) 129 (2022) 102600, http://dx.doi.org/10.1016/j.sysarc.2022.102600.

[57] L. Malina, J. Hajny, P. Dzurenda, S. Ricci, Lightweight ring signatures for decentralized privacy-preserving transactions, in: 15th International Joint Conference on E-Business and Telecommunications, 2018, pp. 692–697, http://dx.doi.org/10.5220/0006890506920697.

[58] Y. Cai, H. Zhang, Y. Fang, A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks, IEEE Internet Things J. 8 (1) (2021) 647–656, http://dx.doi.org/10.1109/JIOT.2020.3037252.

[59] B.A. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering, Tech. Rep., Keele University and Durham University Joint Report, 2007, URL https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf.

[60] D. Moher, A. Liberati, J. Tetzlaff, D. Altman, Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement, PLoS Med. 6 (2009) http://dx.doi.org/10.1371/journal.pmed.1000097.

[61] S. Afrooz, N.J. Navimipour, Memory designing using quantum-dot cellular automata: systematic literature review, classification and current trends, J. Circuits Syst. Comput. 26 (12) (2017) 1730004.

[62] F. Aznoli, N.J. Navimipour, Cloud services recommendation: Reviewing the recent advances and suggesting the future research directions, J. Netw. Comput. Appl. 77 (2017) 73–86.

[63] A. Tandon, A. Dhir, A.N. Islam, M. Mäntymäki, Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda, Comput. Ind. (ISSN: 0166-3615) 122 (2020) 103290, http://dx.doi.org/10.1016/j.compind.2020.103290.

[64] S. Misra, A step by step guide for choosing project topics and writing research papers in ICT related disciplines, in: S. Misra, B. Muhammad-Bello (Eds.), Information and Communication Technology and Applications, Springer International Publishing, 2021, pp. 727–744.

[65] I.R. Jeong, J.O. Kwon, D.H. Lee, Ring signature with weak linkability and its applications, IEEE Trans. Knowl. Data Eng. 20 (8) (2008) 1145–1148, http://dx.doi.org/10.1109/TKDE.2008.19.

[66] Y. Ren, Q. Zhao, H. Guan, Z. Lin, On design of single-layer and multilayer code-based linkable ring signatures, IEEE Access 8 (2020) 17854–17862, http://dx.doi.org/10.1109/ACCESS.2020.2967789.

[67] J.K. Liu, M.H. Au, W. Susilo, J. Zhou, Linkable ring signature with unconditional anonymity, IEEE Trans. Knowl. Data Eng. 26 (1) (2013) 157–165.

[68] M.A. Ferrag, Y. Tang, F. Xia, Q. Ye, M. Wang, R. Mu, X. Zhang, Identity-based linkable ring signature on NTRU lattice, Secur. Commun. Netw. (ISSN: 1939-0114) (2021) http://dx.doi.org/10.1155/2021/9992414.

[69] L. Deng, Y. Jiang, B. Ning, Identity-based linkable ring signature scheme, IEEE Access 7 (2019) 153969–153976.

[70] I.R. Jeong, J.O. Kwon, D.H. Lee, Analysis of revocable-iff-linked ring signature scheme, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 92 (1) (2009) 322–325.

[71] L. Deng, H. Shi, Y. Gao, Certificateless linkable ring signature scheme, IEEE Access 8 (2020) 54641–54651, http://dx.doi.org/10.1109/ACCESS.2020.2981360.

[72] T.H. Yuen, J.K. Liu, M.H. Au, W. Susilo, J. Zhou, Efficient linkable and/or threshold ring signature without random oracles, Comput. J. 56 (4) (2013) 407–421.

[73] S. Mazumdar, S. Ruj, Design of anonymous endorsement system in hyperledger fabric, IEEE Trans. Emerg. Top. Comput. 9 (4) (2021) 1780–1791, http://dx.doi.org/10.1109/TETC.2019.2920719.

[74] M.H. Au, J.K. Liu, W. Susilo, T.H. Yuen, Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction, Theoret. Comput. Sci. 469 (2013) 1–14.

[75] E. Fujisaki, Sub-linear size traceable ring signatures without random oracles, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 95 (2012) 151–166.

[76] R. Mu, B. Gong, Z. Ning, J. Zhang, Y. Cao, Z. Li, W. Wang, X. Wang, An identity privacy scheme for blockchain-based on edge computing, Concurr. Comput.: Pract. Exper. 34 (1) (2022) e6545, http://dx.doi.org/10.1002/cpe.6545.

[77] X. Mao, L. You, C. Cao, G. Hu, L. Hu, Linkable ring signature scheme using biometric cryptosystem and nizk and its application, Secur. Commun. Netw. 2021 (2021) 1–14, http://dx.doi.org/10.1155/2021/7266564.

[78] K. Huang, Y. Mu, F. Rezaeibagha, Z. He, X. Zhang, BA2p : Bidirectional and anonymous auction protocol with dispute-freeness, Secur. Commun. Netw. 2021 (2021) 1–12, http://dx.doi.org/10.1155/2021/6690766.

[79] K. Huang, X. Zhang, Y. Mu, F. Rezaeibagha, X. Du, Scalable and redactable blockchain with update and anonymity, Inform. Sci. 546 (2020) http://dx.doi.org/10.1016/j.ins.2020.07.016.

[80] J. Liu, Y. Yu, K. Li, L. Gao, Post-quantum secure ring signatures for security and privacy in the cybertwin-driven 6G, IEEE Internet Things J. 8 (22) (2021) 16290–16300, http://dx.doi.org/10.1109/JIOT.2021.3102385.

[81] C. Galdi, C. Cao, L. You, G. Hu, Fuzzy identity-based ring signature from lattices, Secur. Commun. Netw. (2021) http://dx.doi.org/10.1155/2021/6692608.

[82] T. Wu, G. Yang, L. Zhu, Y. Wu, Privacy-preserving voluntary-tallying leader election for internet of things, Inform. Sci. (ISSN: 0020-0255) 574 (2021) 461–472, http://dx.doi.org/10.1016/j.ins.2021.06.028.

[83] H. Lin, M. Wang, Repudiable ring signature: Stronger security and logarithmic-size, Comput. Stand. Interfaces (ISSN: 0920-5489) 80 (2022) 103562, http://dx.doi.org/10.1016/j.csi.2021.103562.

[84] V.K. Yadav, S. Verma, S. Venkatesan, Linkable privacy-preserving scheme for location-based services, IEEE Trans. Intell. Transp. Syst. (2021) 1–15, http://dx.doi.org/10.1109/TITS.2021.3074974.

[85] X. Boyen, T. Haines, Forward-secure linkable ring signatures from bilinear maps, Cryptography 2 (4) (2018) 35.

[86] J. Liu, D. Wong, Enhanced security models and a generic construction approach for linkable ring signature, Internat. J. Found Comput. Sci. 17 (2006) 1403–1422, http://dx.doi.org/10.1142/S0129054106004480.

[87] S. Bouakkaz, F. Semchedine, A certificateless ring signature scheme with batch verification for applications in VANET, J. Inf. Secur. Appl. (ISSN: 2214-2126) 55 (2020) 102669, http://dx.doi.org/10.1016/j.jisa.2020.102669.

[88] L. Wang, Q. Xie, H. Zhong, Cooperative query answer authentication scheme over anonymous sensing data, IEEE Access 5 (2017) 3216–3227, http://dx.doi.org/10.1109/ACCESS.2017.2676008.

[89] K. Hara, K. Tanaka, Ring signature with unconditional anonymity in the plain model, IEEE Access 9 (2021) 7762–7774, http://dx.doi.org/10.1109/ACCESS.2021.3049240.

[90] M.H. Au, J.K. Liu, W. Susilo, J. Zhou, Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE, IEEE Trans. Inf. Forensics Secur. 8 (12) (2013) 1909–1922, http://dx.doi.org/10.1109/TIFS.2013.2282908.

[91] S. Chen, P. Zeng, K.-K.R. Choo, X. Dong, Efficient ring signature and group signature schemes based on q-ary identification protocols, Comput. J. 61 (4) (2018) 545–560, http://dx.doi.org/10.1093/comjnl/bxx112.

[92] J. Ren, L. Harn, Generalized ring signatures, IEEE Trans. Dependable Secure Comput. 5 (3) (2008) 155–163, http://dx.doi.org/10.1109/TDSC.2008.22.

[93] W. Li, Z. Lin, C. Qi, A hybrid design of linkable ring signature scheme with stealth addresses, Secur. Commun. Netw. 2022 (2022) 1–9, http://dx.doi.org/10.1155/2022/1417607.

[94] D. J., K. Sundarakantham, K. Singh, S. Mercy Shalinie, A privacy-preserving framework for endorsement process in hyperledger fabric, Comput. Secur. (ISSN: 0167-4048) 116 (2022) 102637, http://dx.doi.org/10.1016/j.cose.2022.102637.

[95] M. Aria, C. Cuccurullo, bibliometrix: An R-tool for comprehensive science mapping analysis, J. Informetr. (ISSN: 1751-1577) 11 (4) (2017) 959–975, http://dx.doi.org/10.1016/j.joi.2017.08.007.

[96] D. Singh, B. Kumar, S. Singh, S. Chand, P.K. Singh, RCBE-AS: Rabin cryptosystem–based efficient authentication scheme for wireless sensor networks, Pers. Ubiquitous Comput. (2021) http://dx.doi.org/10.1007/s00779-021-01592-7.

[97] R. Azarderakhsh, D. Fishbein, G. Grewal, S. Hu, D. Jao, P. Longa, R. Verma, Fast software implementations of bilinear pairings, IEEE Trans. Dependable Secure Comput. 14 (6) (2017) 605–619, http://dx.doi.org/10.1109/TDSC.2015.2507120.

[98] T.M. Fernández-Caramès, P. Fraga-Lamas, Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, IEEE Access 8 (2020) 21091–21116, http://dx.doi.org/10.1109/ACCESS.2020.2968985.

[99] S. Mohamed, L. Messikh, A. Zaoui, A review regarding the biometrics cryptography challenging design and strategies, in: BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 8, (ISSN: 2067-395) 2017, pp. 41–64.

[100] M. Möser, R. Böhme, Anonymous alone? Measuring bitcoin's second-generation anonymization techniques, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2017, pp. 32–41, http://dx.doi.org/10.1109/EuroSPW.2017.48.

[101] S. van, Cryptonote v 2.0, 2013, URL https://cryptonote.org/whitepaper.pdf. (Accessed on 9 February 2022).

[102] S. Noether, Ring signature confidential transactions for monero, IACR Cryptol. ePrint Arch. 2015 (2015) 1098.

[103] Aeon, AEON, 2017, URL https://www.aeon.cash/en/home/. (Accessed on 17 January 2022).

[104] Bytecoin, The first private untraceable cryptocurrency, 2011, URL https://bytecoin.org/about/what-is-bytecoin. (Accessed on 21 January 2022).

[105] L. Chen, N. Tokuda, Stability analysis of regional and national voting schemes by a continuous model, IEEE Trans. Knowl. Data Eng. 15 (2003) 1037–1042, http://dx.doi.org/10.1109/TKDE.2003.1209019.

[106] Q. Feng, Y. Sun, L. Liu, Y. Yang, Y. Dai, Voting systems with trust mechanisms in cyberspace: Vulnerabilities and defenses, IEEE Trans. Knowl. Data Eng. 22 (2011) 1766–1780, http://dx.doi.org/10.1109/TKDE.2009.214.

[107] S. Chow, J. Liu, D. Wong, Robust receipt-free election system with ballot secrecy and verifiability, in: Proceedings of the Network and Distributed System Security Symposium, 2008.

[108] P.P. Tsang, V.K. Wei, Short linkable ring signatures for e-voting, e-cash and attestation, in: International Conference on Information Security Practice and Experience, Springer, 2005, pp. 48–60.

[109] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, M. Ayaz, A systematic literature review on cloud computing security: Threats and mitigation strategies, IEEE Access 9 (2021) 57792–57807, http://dx.doi.org/10.1109/ACCESS.2021.3073203.

[110] V. Javidroozi, H. Shah, G. Feldman, Urban computing and smart cities: Towards changing city processes by applying enterprise systems integration practices, IEEE Access 7 (2019) 108023–108034, http://dx.doi.org/10.1109/ACCESS.2019.2933045.

[111] J.S. Shin, S. Lee, S. Choi, M. Jo, S.-H. Lee, A new distributed, decentralized privacy-preserving ID registration system, IEEE Commun. Mag. 59 (6) (2021) 138–144, http://dx.doi.org/10.1109/MCOM.011.2000699.

[112] L. Benarous, B. Kadri, Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles, Electron. Netw., Res. Appl. Policy 15 (2022) http://dx.doi.org/10.1007/s12083-021-01233-z.

[113] J. Ge, Y. Tian, L. Liu, R. Lan, X. Zhang, Understanding E-commerce systems under massive flash crowd: Measurement, analysis, and implications, IEEE Trans. Serv. Comput. 13 (6) (2020) 1180–1193, http://dx.doi.org/10.1109/TSC.2017.2767600.

[114] Y. Huang, Y. Chai, Y. Liu, J. Shen, Architecture of next-generation e-commerce platform, Tsinghua Sci. Technol. 24 (1) (2019) 18–29, http://dx.doi.org/10.26599/TST.2018.9010067.

[115] M. Bellare, P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in: Proceedings of the 1st ACM Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, ISBN: 0897916298, 1993, pp. 62–73, http://dx.doi.org/10.1145/168588.168596.

[116] G. Leurent, P.Q. Nguyen, How risky is the random-oracle model? in: S. Halevi (Ed.), Advances in Cryptology - CRYPTO 2009, Springer, Berlin, Heidelberg, 2009, pp. 445–464, http://dx.doi.org/10.1007/978-3-642-03356-8_26.

[117] M. Hhan, K. Xagawa, T. Yamakawa, Quantum random oracle model with auxiliary input, in: S.D. Galbraith, S. Moriai (Eds.), Advances in Cryptology – ASIACRYPT 2019, Springer International Publishing, Cham, 2019, pp. 584–614, http://dx.doi.org/10.1007/978-3-030-34578-5_21.

[118] E. Eaton, F. Song, A note on the instantiability of the quantum random oracle, in: J. Ding, J.-P. Tillich (Eds.), Post-Quantum Cryptography, Springer International Publishing, Cham, 2020, pp. 503–523, http://dx.doi.org/10.1007/978-3-030-44223-1_27.

[119] A. Pfitzmann, M. Hansen, Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management–a consolidated proposal for terminology, 31, 2007, pp. 1–54, Version V0.

[120] C. Adams, Introduction To Privacy Enhancing Technologies: A Classification-Based Approach To Understanding PETs, Springer Cham, ISBN: 978-3-030-81042-9, 2021, pp. XIII–324, http://dx.doi.org/10.1007/978-3-030-81043-6.

[121] R. Attarian, S. Hashemi, An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions, Comput. Netw. (ISSN: 1389-1286) 190 (2021) 107976, http://dx.doi.org/10.1016/j.comnet.2021.107976.

[122] T. Sato, K. Emura, T. Fujitani, K. Omote, An anonymous trust-marking scheme on blockchain systems, IEEE Access 9 (2021) 108772–108781, http://dx.doi.org/10.1109/ACCESS.2021.3097710.

[123] M.H. Au, W. Susilo, S.-M. Yiu, Event-oriented k-times revocable-iff-linked group signatures, in: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy, Springer, Berlin Heidelberg, 2006, pp. 223–234, http://dx.doi.org/10.1007/11780656_19.

[124] G. Sharma, D. Verstraeten, V. Saraswat, J.-M. Dricot, O. Markowitch, Anonymous fair auction on blockchain, in: 2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS, 2021, pp. 1–5, http://dx.doi.org/10.1109/NTMS49979.2021.9432664.

[125] A. Hamrouni, T. Alelyani, H. Ghazzai, Y. Massoud, Toward collaborative mobile crowdsourcing, IEEE Int. Things Mag. 4 (2) (2021) 88–94, http://dx.doi.org/10.1109/IOTM.0001.2000185.

[126] J. Ni, X. Lin, Q. Xia, X.S. Shen, Dual-anonymous reward distribution for mobile crowdsensing, in: 2017 IEEE International Conference on Communications, ICC, 2017, pp. 1–6, http://dx.doi.org/10.1109/ICC.2017.7996808.

[127] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, P. Bouvry, A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2419–2465, http://dx.doi.org/10.1109/COMST.2019.2914030.

[128] K. Yang, L. Chen, Z. Zhang, C.J.P. Newton, B. Yang, L. Xi, Direct anonymous attestation with optimal TPM signing efficiency, IEEE Trans. Inf. Forensics Secur. 16 (2021) 2260–2275, http://dx.doi.org/10.1109/TIFS.2021.3051801.

[129] J. Huang, H.-J. Zhang, S. He, Z.-Y. Chen, A remote attestation mechanism using group signature for the perception layer in centralized networking, EURASIP J. Wireless Commun. Networking 2022 (2022) 11, http://dx.doi.org/10.1186/s13638-022-02092-9.

[130] T. Hou, T. Wang, D. Shen, Z. Lu, Y. Liu, Autonomous security mechanisms for high-performance computing systems: Review and analysis, in: Adaptive Autonomous Secure Cyber Systems, Springer International Publishing, Cham, ISBN: 978-3-030-33431-4, 2020, pp. 109–129, http://dx.doi.org/10.1007/978-3-030-33432-1_6.

[131] G. Giudici, A. Milne, D. Vinogradov, Cryptocurrencies: market analysis and perspectives, J. Ind. Bus. Econ. (2020) http://dx.doi.org/10.1007/s40812-019-00138-6.

[132] Y. Yuan, F.-Y. Wang, Blockchain and cryptocurrencies: Model, techniques, and applications, IEEE Trans. Syst. Man Cybern. A 48 (9) (2018) 1421–1428, http://dx.doi.org/10.1109/TSMC.2018.2854904.

[133] R. Yousuf, Z. Jeelani, D.A. Khan, O. Bhat, T.A. Teli, Consensus algorithms in blockchain-based cryptocurrencies, in: 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT, 2021, pp. 1–6, http://dx.doi.org/10.1109/ICAECT49130.2021.9392489.

[134] D.J. Bernstein, T. Lange, Post-quantum cryptography, Nature 549 (2017) http://dx.doi.org/10.1038/nature23461.

[135] K. Seyhan, T.N. Nguyen, S. Akleylek, K. Cengiz, Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey, Cluster Comput. (2021) http://dx.doi.org/10.1007/s10586-021-03380-7.

[136] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, M. Gnjatović, A novel fingerprint biometric cryptosystem based on convolutional neural networks, Mathematics (ISSN: 2227-7390) 9 (7) (2021) http://dx.doi.org/10.3390/math9070730.

[137] S. Park, A. Sealfon, It wasn't me!, in: Annual International Cryptology Conference, Springer, 2019, pp. 159–190.

Justice Odoom received his B.Sc. and MSE degrees in Computer Science from Data Link University, Tema, Ghana and Southwest University of Science and Technology, Mianyang, China, in 2015 and 2020 respectively. He is a Doctoral candidate with the School of Computer Science and Technology, Southwest University of Science and Technology, China and is a certified Elsevier and Publons academy peer reviewer. His research interests include information security, blockchain technology, ring signatures and privacy-preservation in the sharing of Electronic Health Records (EHRs). He is a member of IEEE and IEEE Computer Society.

Xiaofang Huang received the Ph.D. degree from the Beijing University of Posts and Telecommunications in 2010. She is currently a Professor with the school of computer science and technology, Southwest University of Science and Technology, Mianyang, China. Her main research interests include information security, cloud computing, and blockchain technology. She got the information security leading talent award of the district level in 2015.

Zuhong Zhou born in 1966, Chief Information Officer in the Mianyang Central Hospital. His main research interests include computer software system development, information construction of hospital and in charge of hospital's comprehensive work. He participated in the editing of 2 monographs and he has published 5 theses as the first author, and he also published more than 20 conferences exchange theses about the conferences above the provincial level, of which 3 of them won the National Society Outstanding Paper Award, 1 out of them won the provincial first prize.

Samuel Danso obtained his first degree in Computer Science in Ghana and Masters degree in Telecom Technology at SMU-India in the year 2012. He is a full-time lecturer, Ghana Communication Technology University-Ghana and obtained the Ph.D. degree from Southwest University of Science and Technology Mianyang-China in the year 2022. His area of research interests include terahertz active imaging and security on-line, data communications, system and network security.

Zheng Jinan is currently pursuing the masters degree with the school of Computer Science and Technology, Southwest University of Science and Technology Mianyang-China. His current research interests include blockchain technology, Cryptography and ring signatures.

Yanjie Xiang is currently pursuing the masters degree with the school of Computer Science and Technology, Southwest University of Science and Technology Mianyang-China. Her current research interests include blockchain technology, Cryptography and encryption techniques.