Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions

Lukas Malina[1], Jan Hajny[1], Petr Dzurenda[1] and Sara Ricci[2]
[1]*Dept. of Telecommunications, Brno University of Technology, Technicka 12, Brno, Czech Republic*
[2]*Dept. of Computer Science and Mathematics, Universitat Rovira i Virgili, Av. Pasos Catalans 26, Tarragona, Spain*

Keywords: Anonymity, Cryptography, e-Voting, Privacy, Rabin Cryptosystem, Ring Signatures, Transactions.

Abstract: Current digital transactions such as e-payments and e-voting services, should be secure and also offer privacy protection to their users in order to be widely used. This work focuses on advanced cryptographic solutions based on ring signatures that provide anonymity to payment senders or to voters during e-voting. Since more and more constrained mobile devices are used in current networks, the proposed technologies and solutions should be also efficient and provide reasonable computational complexity. In this paper, we present a lightweight privacy-preserving ring signature scheme that is suitable for anonymous transactions and e-voting services run in an environment with constrained devices such as handheld devices and IoT nodes. Our solution provides the fast verification of signatures without using heavy operations such as pairings and exponentiation. Further, we add signature linkability and uniqueness in order to provide double-spending protection.

1 INTRODUCTION

Modern digital services such as e-voting or electronic payment transactions including various cryptocurrencies, smart contracts and e-coins try to employ privacy protection and security properties for their users. These properties can be achieved by using many technologies such as privacy-enhancing cryptographic constructions as zero knowledge protocols, ring signatures, blind signatures or by various mixing network protocols. In current e-voting solutions, voter's anonymity is the main requirement as in classic votes. E-voting systems should not be used without this property. Similarly the users of e-transactions also require privacy protection. The privacy-preserving transactions can attract more users who concern about their privacy. Nevertheless, these privacy-preserving services must handle security risks that could be caused by anonymity. Hence, the solutions should be resistant to potential misusing, e.g. double-spending, double-voting, tracing of voters/transaction senders and more. For example, the most spread cryptocurrency Bitcoin is based on the public blockchain that is a distributed public ledger. This decentralized approach could be highly privacy-invasive. On the one hand, Bitcoin transactions try to keep privacy by using pseudonymous public keys. On the other hand, the bitcoin users are not really anonymous. Transactions and participants can be linked and traced by the advanced analysis of the public blockchain and by observing the Bitcoins unencrypted network. Recently, Conti *et al.* (Conti et al., 2017) have presented a study of current privacy considerations in Bitcoin, the analysis of existing privacy-preserving solutions, and discuss privacy related threats to Bitcoin users.

There are several advanced cryptographic constructions that can be deployed in order to provide anonymous and secure transactions or votes. Group signatures (GS) allow any group member to anonymously sign a message on behalf of the group. Only group managers/issuers are able to add users and trace or revoke users. Nevertheless, GS schemes are often centralized and the group manager has to be a trusted party. The environment of transactions is mostly decentralized. Therefore, ring signatures (RS) that are similar to group signatures could be interesting constructions for these decentralized digital services. In RS firstly defined in (Rivest et al., 2001), a signer signs a message with a private key and then publishes a set of public keys together with own public key. On the one hand, RS remove the centralization point of a group manager. On the other hand, RS provide a perfect privacy (untracebility) and signer is not able to prove his/her signature (non-repudation). In order to employ these constructions in transactions, double-

Malina, L., Hajny, J., Dzurenda, P. and Ricci, S.
Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions.
DOI: 10.5220/0006890505260531
In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT*, pages 526-531
ISBN: 978-989-758-319-3

spending protection must be solved and provided.

In this paper, we focus on cryptographic solutions based on ring signatures that could be suitable for anonymous payment transactions and e-voting. We propose a efficient privacy-preserving signature solution based on fast ring signatures. Our proposal offers signer anonymity, signature uniqueness and signature unforgeability that are desired properties in digital voting and digital transactions scenarios. Our solution provides a linkable mechanism by using key images in order to ensure double-spending (double-voting) protection.

1.1 State of the Art

Since the paper (Rivest et al., 2001) published in 2001, ring signatures and their implementation in e-voting, anonymous data sharing, e-cash services and other privacy-preserving services have been studied in many works, e.g. (Liu et al., 2004), (Tsang and Wei, 2005), (Wu et al., 2006), (Chandran et al., 2007), (Shacham and Waters, 2007), (Fujisaki and Suzuki, 2007), (Liu et al., 2009), (Liu et al., 2014), (Yang et al., 2015), (Noether et al., 2016), (Sun et al., 2017). Ring signatures provide various properties (e.g. linkability, deniability, exculpability, disavowal) and security assumptions. For example, Wu *et al.* (Wu et al., 2006) present ad hoc group signatures that combine some properties of group signatures and ring signatures. These schemes provide the privacy protection for self-organized groups. The ad hoc group signature scheme removes the trusted third party such as a group manager from a system and adds the self-traceability property to ring signatures. In a decentralized system, signers can produce constant-sized anonymous signatures on behalf of the group (a variable set of members). Furthermore, the non-interactive deniable ring signature scheme (Zeng et al., 2016) provides the confirmation of signing (e.g. a lottery game winner) and signature disavowal for non-signers in the ring in order to a signer detection. Nevertheless, both advanced ring signature schemes do not offer double-spending protection.

Liu *et al.* (Liu et al., 2004) propose a linkable, spontaneous and anonymous group (LSAG) signature scheme. The scheme provides the culpability property that allows an investigator to conduct that the authorship of the signature belongs to the user. This scheme also provides the linkability of two signatures. Tsang and Wei (Tsang and Wei, 2005) extend the short ring signature scheme construction of Dodis *et al.* (Dodis et al., 2004) and discuss the application of their scheme to E-voting, offline anonymous electronic cash and direct anonymous attestation. Dodis *et al.* offer a constant-sized ring signature scheme secured in Random Oracle model. Both constructions are based on a three-move zero-knowledge proof-of-knowledge system using the Fiat-Shamir transformation. Fujisaku and Suzuki (Fujisaki and Suzuki, 2007) propose traceable ring signatures that use tags. The tag consists of a list of ring members and the issue of the event. The signer can sign only once per the event in order to stay anonymous in the system. Van Saberhagen (Van Saberhagen, 2013) proposes CryptoNote transactions that are based on a ring signature. Each user of CryptoNote uses a set of public keys and private keys. CryptoNote combines a Diffie-Hellman exchange, one-time signatures and the modification of ring signatures (Fujisaki and Suzuki, 2007). These ring signatures have size n+1, where n is the size of the sender anonymity. A verifier also checks if transactions have been already spent or not by a Link procedure. Noether *et al.* (Noether et al., 2016) propose Ring Confidential Transactions (Ring CT) that enhance the original CryptoNote protocol. They propose a Multilayered Linkable Spontaneous Anonymous Group signature (MLSAG) scheme that provides a signature on a set of n key vectors. Nevertheless, many ring signature schemes have several heavy computations (e..g. pairings, exponentiation, point multiplication) and sizable signatures that depends on the number of ring members.

The most related paper Yang *et al.* (Yang et al., 2015) present the ring signatures based on the Rabin cryptosystem. In their paper, the comparison with existing ring signatures shows that the ring signature scheme is very efficient in sign and verify phases and does not need any pairings. Nevertheless, the Rabin signature in the signing phase usually take similar time like exponentiation in the RSA decryption. Moreover, the scheme defines only two properties: unconditionally signer ambiguity and existentially unforgeability and does not solve double-spending by linkability and signature uniqueness. In our paper, we aim to provide efficient and privacy-preserving ring signature solution that supports signature uniqueness and protect against double-spending which is important in e-voting or anonymous transactions.

1.2 Our Contribution

We design a lightweight privacy-preserving signature solution that can be suitable for anonymous transactions or e-voting services in a constrained environment such as IoT.

We modify the efficient Yang's ring signature scheme (Yang et al., 2015) by the employing key im-

age tags. Thus, our solution adds a signature uniqueness property that provides double-spending protection of each transaction or vote. Furthermore, we add a public key shuffling property in order to increase user anonymity during signing messages (e.g. transactions or votes). In the origin description of the Yang's ring signature scheme (Yang et al., 2015), the signer's public key is the last key in the list of public keys. Therefore, the actual signer can be tracked by his/her public key. In our solution, the verifiers or observers are not able to recognize the actual signer public key that could be any from the list. Moreover, we precise several steps how to employ our solution in anonymous transactions and e-voting scenarios.

2 BACKGROUND

In this section, the cryptography background and security properties are outlined.

2.1 Cryptography Used

In this work, we modify the ring signature scheme (Yang et al., 2015) based on the Rabin cryptosystem (Rabin, 1979).

The Rabin cryptosystem is essentially a special version of RSA with an encryption key $e = 2$, and it is secure under the factorization problem. The Rabin cryptosystem is based on factoring $N = pq$, where N is a public key and p and q are private keys. A message M is encrypted as $C = M^2 \bmod N$. The decryption process produces four possible roots of C computed by using the Chinese Remainder Theorem (CRT) and $\sqrt{C} \bmod p$ and $\sqrt{C} \bmod q$. The integer C is called a quadratic residue. The main benefit of the Rabin cryptosystem is that encryption computes only single squaring in mod N. The decryption (signing) is more expensive because of computing the quadratic residue.

2.2 Security Properties

The proposed solution provides these security properties: Correctness, Signer Anonymity, Signature Uniqueness, Signature Unforgeability and Signature Linkability.

- **Correctness** - a valid signature is always accepted (completeness) and an invalid signature is always rejected (soundness).
- **Signer Anonymity** - a signature is produced by one member from the set of public key holders. Therefore, the identity of a signer is hidden in the group and no one can determine the actual signer from the signature.
- **Signature Uniqueness** - a valid signature on the message could be created only once by a honest signer. The second signature from the same signer during one event (transaction, e-voting) is linked by a key image and is rejected.
- **Signature Unforgeability** - a produced signature is unforgeable. An attacker with negligible probability can produce a valid signature without the corresponding private key.
- **Signature Linkability** - two valid signatures on the same message m with one private/public keypair can be linked by the key image. This property implies the double-spending/voting protection.

3 PROPOSED SOLUTION

In this section, we describe our proposed solution for secure and privacy-preserving transactions or voting based on ring signatures. We assume 3 parties: a signer (a sender, a voter), a verifier (a receiver of the transaction or polling manager/bulletin board application) and an investigator (a trusted third party which detects dishonest signers). Our solution consists of these phases: Key Generation, Signature Generation, Signature Validation and Link Procedure.

3.1 Key Generation

In this phase, key pairs are generated. For $i = 1, ..., n$, where n is the number of ring users, each i-th user selects two safe primes p_i, q_i such that $p_i = 2p'_i + 1, q_i = 2q'_i + 1$ where p'_i, q'_i are primes. The i-th user securely stores a private key that is p_i, q_i and computes a public key as $N_i = p_i q_i$. The public key is then sent to an ad hoc group of n users. The public parameters are a set of public keys $L = (N_1, ..., N_n)$, a defined hash functions $H_i : \{0,1\}^* \rightarrow Z_{N_i}$ for $i = 1, ..., n$ and a hash function $H : \{0,1\}^* \rightarrow QR(N_i)$ used for key images, where $QR(N_i) = \{x \in Z_{N_i} \text{s.t. } x = y^2 \text{ for some } y \in Z_{N_i}\}$.

3.2 Signature Generation

We assume that a signer (e.g. a transaction sender/ a voter) **S** signs the message m (e.g. transaction amount with a metadata, ballot in e-voting) by the ring signature scheme.

Our proposal modifies Yang *et al.* ring signature scheme (Yang et al., 2015) that is based on the Rabin scheme. Yang *et al.*'s ring signature scheme (Yang

et al., 2015) defines only two properties: unconditionally signer ambiguity and existentially unforgeability. We modify this scheme and enhance it by the unique tag in order to achieve a double-spending protection. Moreover, we shuffle actual user public key in the list, then, a verifier (an observer) is not able to determine which the public key has been used.

Let $L = (N_1, ..., N_n)$ is a list of n ring users' public keys, the signer j uses his/her private key (p_j, q_j) to produce a signature of the message m as (L, m, σ). The j-th signer ($\mathbf{S}_j$) also computes a key image $I = H(p_j||N_j||ID_{event})^{1/2} \bmod N_j$ by the knowledge of the factorization of N_j and by applying the Chinese remainder theorem. In order to enable the signer reuses the keypair in more events (e.g. more transactions or e-votes), the signer maps also an event identifier ID_{event} (i.e. a transaction number or an e-voting event). The key image commits signer's public and private keys and prevents the reuse the same keys during one event.

The signer knows his/her private key (p_j, q_j) and public key N_j and executes following steps:

1. $\mathbf{S}_j$ chooses a random element $r_j \in Z_{N_j}$ and computes:
   $h = H_1(L||m||ID_{event})$,
   $c_{j+1} = H_{j+1}(h||r_j)$.
2. For i = 1,...,n and $i \neq j$, $\mathbf{S}_j$ randomly generates element $x_i \in Z_{N_i}$, i.e. for all other ring members.
3. $\mathbf{S}_j$ successively computes in j modulo n, i.e. for each i started from j+1, $j+2 \ldots 0 \ldots j-1$:
   $c_{i+1} = H_{i+1}(h||c_i I + x_i^2 \bmod N_i)$.
4. If $r_j - c_j I \bmod N_j \in QR(N_j)$ then $\mathbf{S}_j$ assigns $t_j = r_j - c_j I \bmod N_j$, otherwise $\mathbf{S}_j$ chooses another element $x_{j-1} \in Z_{N_{j-1}}$ and computes new c_j from step 3 until $r_j - c_j I$ is a quadratic residue.
5. $\mathbf{S}_j$ solves $x_j = t_j^{1/2} \bmod N_j$ by the knowledge of the factorization of N_j with using the Chinese remainder theorem. Square roots could be computed by the Tonelli - Shanks algorithm or by its modifications.

Finally, the signer produces the signature $\sigma = (I, c_1, x_1, ..., x_n)$ on the message m in the event ID_{event}.

The computational and memory complexity could be reduced if the signer chooses smaller subset of k users' public keys from n ring members. Nevertheless, the level of signer privacy is reduced as well.

3.3 Signature Validation

A verifier (a transaction receiver or a polling manager/bulletin board service) **V** checks the signature on the message by checking the ring signature σ on the message m and by checking its uniqueness in the event ID_{event}.

3.3.1 Ring Signature Verification

The verifier uses public parameters (L, H) and checks the received ring signature $\sigma = (I, c_1, x_1, ..., x_n)$ on the message m during the event ID_{event}.

1. **V** computes $h = H_1(L||m||ID_{event})$.
2. For each i = 1,...,n, **V** restores $r_i = c_i I + x_i^2 \bmod N_i$.
3. For each i = 1,...,$n-1$, **V** computes $c_{i+1} = H_{i+1}(h||r_i)$.
4. If $c_1 = H_1(h||r_n)$, the output is true and the signature is accepted and **V** continues by checking the signature uniqueness. Otherwise, **V** rejects the signature and the algorithm halts.

3.3.2 Signature Uniqueness Verification

V checks if the image key I of the signature has not been used in past signatures in the event ID_{event}. In case that the key image I is not presented in a dataset of key images, the verifier accepts the signature. Then, the key image of the signature is added to the dataset of key images in order to prevent double spending in the future. Otherwise, the signature of the message (e.g. a transaction/vote) is marked as the duplicated and it is rejected.

3.4 Link Procedure

In case that the n+1 or more ring signatures occur at the end of an event (e.g. transaction bulk, closing e-voting) with n participants, an investigator (i.e. a third trusted party) runs this procedure in order to detect among the members of the ring such a malicious signer who produces more valid signatures. The investigator precomputes all I^2. Further, each honest signer, which knows such private key p_j, securely sends to the investigator a set of $(H(r_1||N_1||ID_{event}) \bmod N_1, \ldots H(p_j||N_j||ID_{event}) \bmod N_j, \ldots H(r_n||N_n||ID_{event}) \bmod N_n)$ in randomized order. The investigator then checks that at least one received $H(p_i||N_i) \bmod N_i = I^2$ for $i = 0 \ldots n$. The mixed set of hash hides the index of the signer so the signer is still anonymous against external parties.

4 SECURITY ANALYSIS

In this section, we provide the security analysis of the proposed solution. We discuss these security proper-

ties: correctness, signer anonymity, signature uniqueness, signature unforgeability, signature linkability.

Theorem 1. *Correctness* - Completeness and soundness are provided. A honest verifier is always able to accept a valid ring signature and reject a false signature.

Proof. Suppose that a verifier has correct public parameters such as set of public keys $L = (N_1, ..., N_n)$ and a set of defined hash functions. He/she can check a signature $\sigma = (I, c_1, x_1, ..., x_n)$ on a message m by restoring parameters r_i and c_i for each i from 1 to n and finally by checking $c_1 = H_1(h||r_n)$. Assume that $r_n = c_n I + x_n^2 \text{mod} N_n$ and somewhere in the ring $c_{j+1} = H_{j+1}(h||r_j) = H_{j+1}(h||c_j I + x_j^2 \text{mod}\ N_j)$ where $x_j^2 = t_j \text{ mod } N_j = r_j - c_j I \text{ mod } N_j$ so that $c_{j+1} = H_{j+1}(h||c_j I + r_j - c_j I \text{mod } N_j = H_{j+1}(h||r_j)$.

Theorem 2. *Signer Anonymity* - It is infeasible to identify which private key creates the ring signature.

Proof. A verifier uses a set L of n public keys and is not able to identify which public key belongs to a signer. The chance of guessing correctly which public key is used to generate a given signature is negligibly greater than $1/n$. We assume that the private key is chosen at random and an adversary only knows the public keys and not the other private keys. If the adversary knows k private keys then the guessing of signer key is negligibly greater than $1/(n-k)$.

Further, the key image I does not leak the signer identity if the private keys are chosen at random. The user anonymity holds also in the link procedure for external observers due the signers who prove their honesty by sending only basic hash of values in randomized order.

Theorem 3. *Signature Uniqueness* - a signer is able to produce only one valid signature on the message by the one public/private keypair.

Proof. The key image $I = H(p_j||N_j||ID_{event})^{1/2} \text{mod}$ N_j of j-th user maps public and private keys and is integrated in the produced signature. A verifier restores $r_i = c_i I + x_i^2 \text{mod} N_i$ for each i from 1 to n where I is a part in all r_i. In fact, if a malicious user tries to re-use more times the same signature, the verifier can detect the re-use by checking the dataset of key images.

Theorem 4. *Signature Unforgeability* - it is hard to produce a valid signature without a private key.

Proof. A signer without a private key p_j, q_j is not able to solve $x_j = t_j^{1/2} \text{mod} N_j$ by using the knowledge of the factorization of N_j with factors p_j, q_j. If an adversary is successful in forgery, he/she must output x_j that satisfies such $c_{j+1} = H_{j+1}(h||c_j I + x_j^2 \text{mod}$ $N_j)$ which causes that $c_1 = H_1(h||r_n) = H_1(h||c_n I +$ $x_n^2 \text{mod} N_n)$ and encloses the ring. More formal analysis for the property can be found in (Yang et al., 2015).

Theorem 5. *Signature Linkability* - it is hard to produce n+1 valid signatures on the message by the n public/private keypair.

Proof. The key image $I = H(p_j||N_j||ID_{event})^{1/2}$ mod N_j maps public and private keys of a honest signer, ID_{event} and is integrated in the produced signature. ID_{event} is also used in the ring signature. Any observer (a verifier) can link two signatures on the same message during one event by I from one honest signer. Hence, a honest signer cannot re-use more times the valid signatures of one private/public keypair and a correct H function. In case that a malicious signer will try to produce a new signature with a different key image but with same keypair, then the Link procedure detects this signature and rejects it. All signatures with incorrect key images can be detected.

5 PERFORMANCE EVALUATION

This section discusses the computational complexity of the proposed solution and compares signature sizes and the complexity of most significant phases such as signing and verification with other related works that are based on ring signatures and provide linkability. Table 1 provides the comparison of performance and memory costs of the proposed ring signature scheme and related schemes. We denote a pairing operation as P, exponentiation as E, multiplication as M, squaring as S. The relatively fast operations such as addition and a hash function are omitted. N denotes the number of users in a ring/ad hoc group. In order to evaluate the length of signatures, we use the following notation, e.g. $O(1)$ - constant size, $O(\sqrt{N})$ - semi-linear size, $O(N)$ - linear size.

In our solution and Yang *et al.* scheme (Yang et al., 2015), the signing procedure employs the Rabin signing that computes the square root of the parameter in modular arithmetic. We consider this operation as expensive as 1 exponentiation, therefore it is noted as E also in our comparison. Yang *et al.* (Yang et al., 2015) is the most efficient scheme from the compared schemes but does not support linkability. Then, our solution, which provides signature uniqueness and linkability by adding a key image, is very efficient during signing and verification in comparing with other related schemes.

6 CONCLUSIONS

We presented a lightweight privacy-preserving solution based on ring signatures. The solution provides

Table 1: Performance comparison of related schemes.

Scheme	Sign	Verify	Signature size
Liu *et al.* (Liu et al., 2004)	(3+4($N-1$))E + (1+2N)M	(4N)E + 2NM	$O(N)$, $N+2$
Fujisaki and Suzuki *et al.* (Fujisaki and Suzuki, 2007)	(3+2N)E + (2+3N)M	(4N)E + (3N)M	$O(N)$, $2N+1$
Chandran *et al.* (Chandran et al., 2007)	(5+6$\sqrt{N}$+(N+1)/3)E+ (6$\sqrt{N}$+8)M	(6+6$\sqrt{N}$)P + (3$\sqrt{N}$+1)E + (4$\sqrt{N}$ +1)M	$O(\sqrt{N})$, $6\sqrt{N}+6$
Liu *et al.* (Liu et al., 2009)	NE	N E	$O(N)$, $2N+1$
Liu *et al.* (Liu et al., 2014)	(5+N)E+(4+N)M	(4+N)E+(3+N)M	$O(N)$, $N+3$
Yang *et al.* (Yang et al., 2015)	E+NS	NS	$O(N)$, $N+1$
This solution	2E+2M+NS	M+NS	$O(N)$, $N+2$

anonymity, uniqueness, linkability and unforgeability, and can be applied in applications with double-spending and double-voting protection. The solution does not use heavy operations. The ring signature verification takes only 1 multiplication and N squaring which depends on the size of ring (N). Therefore, the solution could be implemented in services running in heterogeneous networks with small and medium groups of constrained devices.

As future work, we would like to make the link procedure more efficient and integrate the proposed ring signature scheme into a transaction model based on blockchain.

ACKNOWLEDGEMENTS

Research described in this paper was financed by the National Sustainability Program under grant LO1401 and Ministry of Interior under grant VI20162018003.

REFERENCES

Chandran, N., Groth, J., and Sahai, A. (2007). Ring signatures of sub-linear size without random oracles. In *International Colloquium on Automata, Languages, and Programming*, pages 423–434. Springer.

Conti, M., Lal, C., Ruj, S., et al. (2017). A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*.

Dodis, Y., Kiayias, A., Nicolosi, A., and Shoup, V. (2004). Anonymous identification in ad hoc groups. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 609–626. Springer.

Fujisaki, E. and Suzuki, K. (2007). Traceable ring signature. In *International Workshop on Public Key Cryptography*, pages 181–200. Springer.

Liu, J. K., Au, M. H., Susilo, W., and Zhou, J. (2009). Online/offline ring signature scheme. In *International Conference on Information and Communications Security*, pages 80–90. Springer.

Liu, J. K., Au, M. H., Susilo, W., and Zhou, J. (2014). Linkable ring signature with unconditional anonymity. *IEEE Transactions on Knowledge and Data Engineering*, 26(1):157–165.

Liu, J. K., Wei, V. K., and Wong, D. S. (2004). Linkable spontaneous anonymous group signature for ad hoc groups. In *Australasian Conference on Information Security and Privacy*, pages 325–335. Springer.

Noether, S., Mackenzie, A., et al. (2016). Ring confidential transactions. *Ledger*, 1:1–18.

Rabin, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization. Technical report, Massachusetts ints. of tech. Cambridge lab for computer science.

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–565. Springer.

Shacham, H. and Waters, B. (2007). Efficient ring signatures without random oracles. In *International Workshop on Public Key Cryptography*, pages 166–180. Springer.

Sun, S.-F., Au, M. H., Liu, J. K., and Yuen, T. H. (2017). Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In *European Symposium on Research in Computer Security*, pages 456–474. Springer.

Tsang, P. P. and Wei, V. K. (2005). Short linkable ring signatures for e-voting, e-cash and attestation. In *International Conference on Information Security Practice and Experience*, pages 48–60. Springer.

Van Saberhagen, N. (2013). Cryptonote v 2. 0.

Wu, Q., Susilo, W., Mu, Y., and Zhang, F. (2006). Ad hoc group signatures. In *International Workshop on Security*, pages 120–135. Springer.

Yang, X., Wu, W., Liu, J. K., and Chen, X. (2015). Lightweight anonymous authentication for ad hoc group: A ring signature approach. In *International Conference on Provable Security*, pages 215–226. Springer.

Zeng, S., Li, Q., Qin, Z., and Lu, Q. (2016). Non-interactive deniable ring signature without random oracles. *Security and Communication Networks*, 9(12):1810–1819.