The Advance of Ring Confidential Transactions

Ruiqi Jin *

School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an, China

* Corresponding author email: ruiqi.jin@disroot.org

Abstract. Ring Confidential Transactions (RingCT) is a protocol associated with the privacy-focused cryptocurrency Monero and is used to hide the transaction amount from the third party while still providing the confidentiality of the hide transaction. With the Pederson commitment scheme, ring signature, and other cryptographic constructions, RingCT plays a major role in making the transactions of Monero private. As a privacy coin, Monero has the unique property of fungibility in the cryptocurrency market from the protocols implemented. These protocols provided opportunities and challenges for its future. In this paper, the version of the protocol implemented in Monero is first inspected, including the commitment to zero and the range proof. Then, two critical cryptographic constructions used by RingCT 2.0, the accumulator and the signature of knowledge, are introduced. Finally, the influence of RingCT and other privacy features and the current situation of privacy coin is discussed.

Keywords: Monero; RingCT; Ring Signature; Privacy Coin.

1. Introduction

The idea of confidential transactions was first addressed by Adam Back in 2013, and is later elucidated and investigated by Greg Maxwell as a cryptographic tool for Bitcoin to hide transaction amounts. The protocol used the Pedersen commitment scheme, which allows commitment of transaction amounts and verification without revealing the commitment. Therefore, the protocol allows two kinds of proof: 1) Commitment to zero, i.e., the amounts in the inputs and outputs in a transaction adds to zero, and 2) Range proof, i.e., the amounts in each output are in a given range (positive). Due to requiring a soft fork, the protocol is not added to the Bitcoin mainchain and is implemented only on the lightning side-chain.

In 2015, Nicolas van Saberhagen proposed Ring Confidential Transactions for the cryptocurrency Monero [1]. Although Monero, based on the original CryptoNote protocol submitted by Nicolas van Saberhagen in 2013, uses a ring signature as a method combined with one-time stealth addresses to conceal the sender's identity, the number of transactions was public on the chain at that time [2]. The original RingCT is a modification of Bitcoin's CT, allowing the use of ring signatures. A Multilayered Linkable Spontaneous Anonymous Group Signature is used to prevent double-spending and preserve the anonymity provided by ring signatures. To provide the commitment to zero and range proof similar to the original CT, RingCT uses two kinds of ring signatures: the whole transaction is signed with a ring signature to prove the amounts added to zero, and bits of the transaction amounts are signed with separate ring signatures to ensure amounts are in a given range. The major drawback of this protocol is the size of the ring signatures. The protocol was implemented in Monero in January 2017 and became mandatory after the hard fork in September 2017.

Optimization is the RingCT 2.0 protocol proposed by Shi-Feng Sun et al. in August 2017 [3]. In the paper, Sun et al. defined the security criteria of the RingCT protocol, which is not available in the original RingCT paper. RingCT 2.0 uses the one-way accumulator, a one-way function which is able to confirm membership of a group, i.e., whether an element belong to the group, without revealing individual members of the group. It also uses the accumulator's relating signature of knowledge as a replacement for the linkable group ring signature in the 1.0 protocol. In RingCT 2.0's construction, the signature size is independent of the number of groups, while in RingCT 1.0, the size grew linearly with the size of groups. However, RingCT 2.0 requires a trusted setup: the nodes must trust each other initially, which could cause a potential identity leak. Therefore, the protocol is not implemented in Monero.

Tim Ruffing et al. also proposed a setup, later called RTRS RingCT, to optimize the ring signature's space. In RTRS RingCT, the signature is logarithmical, enabling a huge ring without significant growth of signature size. While the spatial complexity is greatly reduced, the verification process of RTRS RingCT has a greater time complexity, requiring a longer verification time than the original MLS. Therefore, it's considered not worth to be implemented.

Bulletproof was presented in 2017 by Benedikt Bünz et al. as an efficient range-proof method requiring no trusted setup [4]. A single small proof could be used to prove all output amounts are in range at the same time, and the proof size grows logarithmically with the data size. Bulletproof was implemented in Monero in October 2018 as an optimization of the original RingCT, and this is also the current version used in Monero.

Tsz Hong Yuen and RingCT 2.0 team released work on RingCT 3.0 in 2019 [5]. RingCT 3.0 removed the trusted setup and greatly improved the size of signature without increasing the verification time. This version has a logarithmic proof size and linear verification time.

Rui Morais et al. presented a modification of RingCT to make it compatible with Delegated Proof of Stake based consensus mechanisms [6]. The construction is the first to combine RingCT and PoS, as Monero is a Proof of Work cryptocurrency. The Pedersen commitment used in other versions of RingCT is replaced with a ciphertext of a public encryption scheme while still holding the properties of the original construction that enabled the verification of the amount. This modification allows the owner to encrypt the amount with a long-time public key, thus redelegating the stake corresponding to the amount by proving they know the secret key of such encryption.

Several post-quantum lattice cryptography-based versions of RingCT are also proposed, including Lattice RingCT by Wilson Abel Alberto Torres et al. and MatRiCT by Muhammed F. Esgin et al. [7, 8]. MatRiCT is the most efficient of all post-quantum schemes, and can scale to large anonymity sets. A potential hard fork against quantum computing is discussed, and lattice-based RingCT will likely be implemented on Monero.

In this paper, the version of protocol implemented in Monero is first inspected, including the commitment to zero and the range proof. Then, two important cryptographic constructions used by RingCT 2.0, the accumulator and the signature of knowledge, are introduced. Finally, influence of RingCT and other privacy features, and the current situation of privacy coin is discussed.

2. RingCT in Monero

2.1 RingCT 1.0

2.1.1 Discrete Logarithm Problem on Elliptic Curve

Each point P on a finite Elliptic Curve (EC) can generate a cyclic group of points, and it is able to compute point addition and scalar multiplication on it. Scalar product between an integer n and a point P is presented in the form nP. Given n and P where P is a point on EC, it is not difficult to compute nP. However, given P and nP, calculating n is computationally hard. This is called the discrete logarithm problem on EC, making scalar multiplication on EC a one-way function. Therefore, it is able to construct a public key cryptographic scheme on EC, while the random number k is used as a private key. The public key is a point K, calculated with the generator G of a group $(G,\cdot)$ on EC such that $K = kG$.

2.1.2 Ring Signature

Ring signature or specifically Multilayered Linkable Spontaneous Anonymous Group signatures (MLSAG) are used to hide the sender’s identity. These kinds of signatures are based on the Schnorr signatures on EC, which is a zero-knowledge proof to prove someone knows the private key of a given public key. A Schnorr signature is constructed as follows:

- Select a random number a and compute aG.
- Let challenge $c = Hash(aG)$, where $Hash()$ is a cryptographic hash function which outputs a number.

- compute $r = a + ck$.
- Publish r and aG as proof.

The verifier knowing K, r, G and aG can verify that $rG = aG + ckG = aG + cK$ without knowing k, and the only way for the prover to construct the proof without reversing $Hash()$ is the knowledge of k. Ring signature is similar, except it's constructed with multiple public keys, while the prover only knows the corresponding private key k_π to one of the public keys K_π, and it's a signature to a message. Unlike the single signature, challenge c_i in ring signature for key K_i is generated by hashing the fake proof relating to K_{i-1} and the message. The only real proof is the one relating to K_π, constructed with the private key, making the full ring of proof being valid. Thus, it is possible to use ring signature to prove the sender knows one of secret keys corresponding to the public keys forming the ring.

2.1.3 Pederson Commitment Scheme

Pederson Commitment Scheme is constructed on a large group on which the discrete logarithm problem (DLP) is hard. With a secret integer message m and a group $(G,\cdot)$ the committer constructs the commitment as follows:

- Select two random generators g and h.
- Decide a random integer r.
- Commit $C(r,m) = g^r \cdot H^m$.

With the group of points on EC, a Pederson Commitment Scheme could be constructed:

- Select two random generator points G and H on curve.
- Decide a random integer r.
- Commit $C(r,m) = rG + mH$.

If an adversary could solve the discrete logarithm problem on EC, they can reveal the envelope $C(r,m)$ in more than one way. Therefore, Pederson Commitment is computationally binding.

The Pederson Commitment defined on EC is also Additively Homomorphic, i.e., $C(r_1 + r_2, m_1 + m_2) = C(r_1, m_1) + C(r_2, m_2)$ if same G and H are used in the commitment. This gives the ability to verify the message m has certain property without revealing the envelope.

2.1.4 Amount Commitment

Monero uses Pederson Commitment scheme to hide the transaction amount. A commitment to amount b is defined as:

$$C(y,b) = yG + bH \tag{1}$$

Here G and H are two random generators. y is called the mask or blinding factor which should only be known by the receiver. In particular, it is constructed with the Diffie-Hellman shared secret K in the transaction [9]. In the tth output of a transaction,

$$y = Hash("commitment\_mask", Hash(K,t)) \tag{2}$$

Therefore, the receiver could calculate the factor with their view key and decrypt the output amounts in the commitment. Similarly, the encrypted amount is also stored in the transaction:

$$amount = b \oplus_8 Hash("amount", Hash(K,t)) \tag{3}$$

The receiver could decrypt this to get b of each output. With addictive homomorphism, there are two verifications could be done with the envelopes in the transaction, specifically: 1) Commitment to zero. 2) Range proof.

2.1.5 Commitment to Zero

The Commitment to Zero is making any third party be able to verify the amount of all output in envelopes $C(y,b)$ equals the amount of all input in envelopes $C(x,a)$. It seems that it could be done by letting

$$\sum y_o = \sum x_i \tag{4}$$

However, in avoiding sender identifiability, the output blinding factors could not be equal to the input blinding factors. This is solved by generating pseudo output commitments.

Pseudo output commitments are commitments of input amounts by the sender. With input envelope

$$C(x_i, a_i) = x_i G + a_i H \tag{5}$$

The sender knows a_t, and is able to construct

$$C(x_i', a_i) = x_i' G + a_i H \tag{6}$$

The new commitment is a pseudo output commitment. Here, in constructing those envelopes, the sender knows their differences as

$$C(x_i, a_i) - C(x_i', a_i) = (x_i - x_i')G \tag{7}$$

In knowing x_i and x_i', sender knows the private key of the difference as $x_i - x_i'$. The key is used together with the one-time private transaction keys in constructing the MLSAG ring signature in order to show that sender is actually the owner of the input amounts. Specifically, by using $x_i - x_i'$ as private key, and $C(x_i, a_i) - C(x_i', a_i)$ as the corresponding public key, sender could construct a ring with fake public keys, i.e., fake commitments to zero.

With pseudo-output commitments, a third party is able to verify that in all the commitments signed by rings, the amounts corresponding to the private key known by the sender add to zero. Specifically, the blinding factors are constructed in that

$$\sum y_o = \sum x_i' \tag{8}$$

This is done by selecting every x_i' random except for the last one.

2.1.6 Range Proof

Range proofs are used to show all output amounts are greater than zero, avoiding the sender spending negative amount of XMR to generate new money. The amount in a transaction is bounded between 0 and 2^{64}.

The range proof part is separated from the commitment to zero part, and is done by breaking the amount into powers of 2 (binary representation of amounts). Then, the sender generates commitments with each part. Specifically, if the nth bit in the binary representation of amounts is 1, the sender generates

$$C_n(w_n, 1 \times 2^n) = w_n G + 2^n H \tag{9}$$

While w_n are randomly selected. If the bit is 0, they generate

$$C_n(w_n, 0 \times 2^n) = w_n G \tag{10}$$

Therefore, the sum of all C_n is differ to the output commitment by a factor of G. With these committed envelopes, the sender again construct a ring signature with the secret keys w_n and the corresponding public key, which in this case, has two possibilities: The ring signature are used to prove that the sender knows either the secret key of C_n (when the nth bit is 0) or $C_n - 2^n H$ (when the nth bit is 1), therefore the sum of all these amount is presentable with a binary number in the specified range.

2.2 RingCT 2.0

2.2.1 Accumulator with One-way Domain

Accumulator with one-way domain is used as a decentralized replacements to digital signature and is used in RingCT 2.0 to reduce the size of Pederson commitment scheme. The construction of the accumulator makes it able to confirm that something belongs to a certain group, without revealing individual members of the group [10]. Specifically, it's a one-way function $f: X \times Y \rightarrow X$ such that the quasi-commutativity condition holds for $x \in X$ and $y_1, y_2 \in Y$, it holds $f(f(x, y_1), y_2) = f(f(x, y_2), y_1)$.

For a member in specific group, it can compute witness to prove that the member is indeed been accumulated. For example with set $\{y_1, y_2, y_3\}$ and the accumulated value $acc = f(f(f(x, y_1), y_2), y_3)$, the witness of member y_2 is computed as $w_2 = f(f(x, y_1), y_3)$, and verifier can verify that $acc = f(w_2, y_2)$ and prove that y_2 is accumulated.

The important property of accumulator is that as acc and w_2 both belong to set X, they have the same length, i.e., the length of witness and accumulated value is constant no matter the size of the set is. Thus, it can reduce the signature size with accumulator.

2.2.2 Signature of Knowledge

The signature of Knowledge is constructed as an extension of the public key signature scheme. It solves the issue of linear dependence of the public key size on the group size in group signatures. SoK allows one to issue signatures on behalf of any NP statement with a valid pair in the language of that NP-hard relation [11].

In signing a SoK on message m, a valid pair (x, y) is used, and $\pi = Sign(m, x, y)$ is the signature of knowledge on message m. To verify the signature, one need m, the SoK π and statement y. $Verify(m, \pi, y)$ outputs the validity of the SoK.

As the size of the signature and public key is not dependent on the size of the group, SoK is used to reduce the size of MLSAG in RingCT 1.0, in which the size of signature grows linearly as the size of group grow.

3. The Discussion of Privacy Coin

The privacy coin is a type of cryptocurrency that provides anonymity to the user and the confidentiality of the transaction details. Cryptocurrencies are not naturally private, as it's digital and decentralized. If no specific protocol is implemented on the chain, everyone could have access to the ledger and can track transactions. To provide privacy, the developer team must intentionally utilize the privacy features. There are other famous privacy coins like Zcash, in which shielded transactions are available; Dash, which provides a method to disassociate a coin with its transaction history through mixing; and Litecoin, which utilized MimbleWimble protocol recently to provide transaction privacy. However, Monero is still the most famous and popular privacy coin in the cryptocurrency market. Its privacy constructions are mandatory, making privacy its main feature.

Monero mainly uses two privacy constructions: Stealth Addresses and RingCT. The latter, to hide the transaction amounts, is discussed in this article. It utilizes Ring Signature as a zero-knowledge proof. Stealth Addresses, stated in the CryptoNote protocol, are used to unlink different transactions one receives, preventing a third party from monitoring the amount a certain party holds using their unique address. This is made possible by generating random one-time addresses, making the sender in a certain transaction only know about one transaction associated with the receiver. To prevent tracing coins moving between addresses by monitoring the output, Ring Signature is used to hide the output, providing untraceability.

A coin is associated with its history of cryptocurrencies that are not privacy-focused with a transparent ledger. Therefore, coins are not interchangeable, i.e., they are not fungible. This enabled the ability to deny a coin based on its problematic transaction history and devalue it, regardless of whether the current holder is innocent. For the privacy coins in which privacy features are not mandatory, transparent transactions are the default state, making those transactions intentionally enabling privacy features suspicious and potentially discouraging their use of them. For example, in the coin pool of Zcash, only around 4% of the coins are in the anonymous shielded pool. These privacy coins still have a mostly transparent ledger, which cannot provide fungibility. The mandatory privacy features of Monero enabled the fungibility of the coin.

Fungibility is an important characteristic for assets that are supposed to function like a medium of exchange, like cryptocurrency. While cryptocurrency is sometimes called digital cash, they do not have the same property that belongs to cash, which is fungible by law. Although physical cash is not indistinguishable since they have a unique identifier, its transaction history does not devalue them. The fungibility of Monero already provides a special prospect besides the privacy considerations of the participants in cryptocurrencies.

This mandatory anonymity may also limit the prospects of Monero and other privacy coins that adopt similar constructions. As almost all cryptocurrencies have transparent and traceable blockchains, government and cryptocurrency exchanges need more experiences to deal with the new problems with privacy coins, making Monero delisted from major exchanges. Although this makes Monero harder to get or exchange with others, the issues related to untraceability and its relation to crime have been introduced previously. According to Gurvais Grigg, CTO of Chainalysis, although Monero is less traceable than Bitcoin, physical cash is still the most difficult to trace. Criminology researcher David Décary-Hétu suggests that it is not a privacy coin with the limited prospect, but the exchanges and regulators must adapt to it.

The real concern of privacy coins is vulnerabilities related to their design. They tend to be more complex than cryptocurrencies with transparent blockchains, as they utilize more cryptographic constructions. Thus, they may be more vulnerable to potential attacks. In 2017 Amrit Kumar et al. found three weaknesses of Monero: 1) the ability to see the output amount using a ring signature of size zero, 2) the ability to associate different transactions made by the same user, and 3) the possibilities of guessing the correct input by analyzing temporal information [12]. Although the first vulnerability is fixed according to the development team, other issues are harder to tackle. The third one, also mentioned by Malte Möser et al. in 2017, is especially hard to handle, as it utilized user's behavior in cryptocurrency: coins are likely to be spent instead of stay [13]. Thus, the real output cited as a transaction input is likely the newest one. This might be fixed with a better sampling method, while those methods tend to have greater time and space complexity. There may still be other vulnerabilities undiscovered and potentially break all anonymity in the past, as transaction histories are on a public chain.

4. Summary

In this paper, RingCT used on privacy coin is investigated. RingCT and other cryptographic constructions are designed and implemented to protect cryptocurrency users' privacy. At the same time, they could also become the design's attack vectors or decrease the cryptocurrency's usability. Monero and other privacy coins must constantly improve, review their protocol, and adapt to changing conditions to ensure all privacy promises and related characteristics. In order to ensure this, the implementation of these protocols and their attack surface need to be examined. The protocols designed as a replacement of the current implementation of RingCT also need further investigation to ensure safety.

References

[1] Noether, S., & Mackenzie, A. (2016). Ring confidential transactions. Ledger, 1, 1-18.

[2] Van Saberhagen, N. (2013). CryptoNote v 2.0.

[3] Sun, S. F., Au, M. H., et al. (2017, September). Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In European Symposium on Research in Computer Security (pp. 456-474). Springer.

[4] Bünz, B., Bootle, J., Boneh, D., et al. (2018, May). Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE symposium on security and privacy (SP) (pp. 315-334). IEEE.

[5] Yuen, T. H., Sun, S. F., Liu, J. K., et al. (2020, February). RingCT 3.0 for blockchain confidential transaction: shorter size and stronger security. In International Conference on Financial Cryptography and Data Security (pp. 464-483). Springer, Cham.

[6] Morais, R., Crocker, P., & de Sousa, S. M. (2020). Delegated RingCT: faster anonymous transactions. arXiv preprint arXiv:2011.14159.

[7] Alberto Torres, W., Kuchta, V., Steinfeld, R., et al. (2019, July). Lattice RingCT V2. 0 with multiple input and multiple output wallets. In Australasian Conference on Information Security and Privacy (pp. 156-175). Springer, Cham.

[8] Esgin, M. F., Zhao, R. K., Steinfeld, R., et al. (2019, November). MatRiCT: efficient, scalable and post-quantum blockchain confidential transactions protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 567-584).

[9] Alonso, K. M. (2020). Zero to monero.

[10] Benaloh, J., & Mare, M. D. (1993, May). One-way accumulators: A decentralized alternative to digital signatures. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 274-285). Springer, Berlin, Heidelberg.

[11] Chase, M., & Lysyanskaya, A. (2006, August). On signatures of knowledge. In Annual International Cryptology Conference (pp. 78-96). Springer, Berlin, Heidelberg.

[12] Kumar, A., Fischer, C., Tople, S., et al. (2017, September). A traceability analysis of monero's blockchain. In European Symposium on Research in Computer Security (pp. 153-173). Springer, Cham.

[13] Möser, M., Soska, K., Heilman, E., et al. (2017). An empirical analysis of traceability in the monero blockchain. arXiv preprint arXiv:1704.04299.