Experimemt Designs for RCT+

Abstract.

Keywords:

1 Introduction

Let's consider a transaction with m inputs and n outputs. As shown the Fig. 1, for both the Ring-CT (RCT) in the original/current Monero and the Ring-CT+ (RCT+) in our work, there are a 'Generation' phase and a 'Verification' phase. The Generation phase prepares the mixin input coins, forming the Ring(s), and computes the MLSAG and range proofs. The output of the Generation phase include (1) input (mixin) matrix, (2) n output coins, (3) MLSAG(s) for the Ring(s), and (4) the rang proofs. These output data will be broadcast to the miner(s), and the miner will run the Verification phase to check whether these data form a valid transaction.

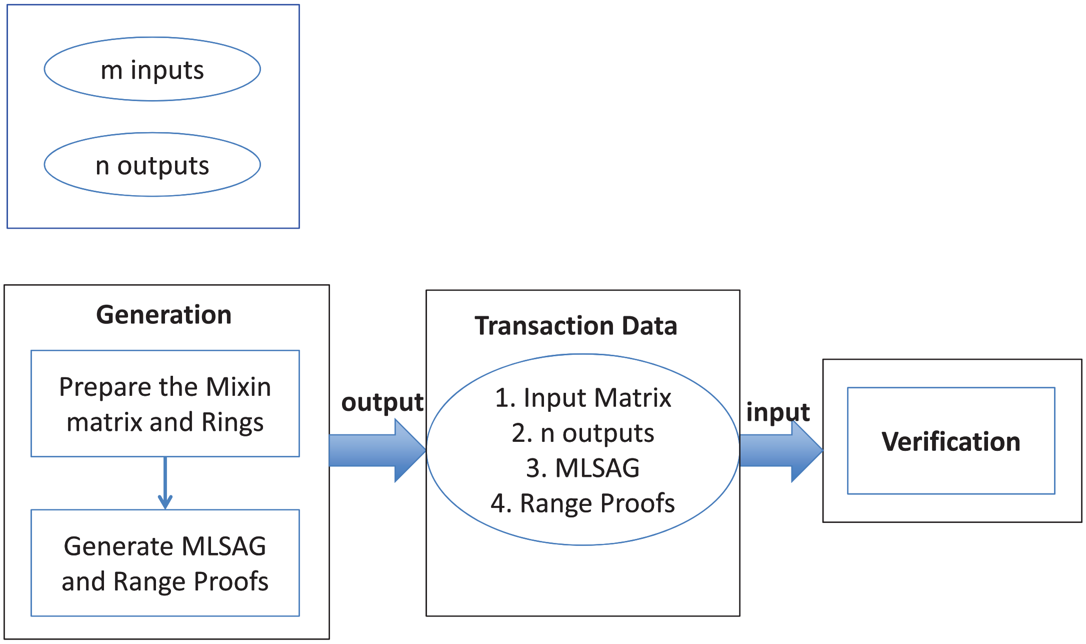

Fig. 1. Outline

To compare the performance of RCT and our RCT+ under the same m inputs and n outputs, we consider

1. The computation cost (computation time) of the Generation phase

2. The storage cost (communication cost/ size) of the output of the Generation Phase (i.e. the transaction data)
3. The computation cost (computation time) of the Verification phase
4. The network latency:
   (a) Latency 1 : The time from a wallet begins to propose a transaction to the first miner receives that transaction
   (b) Latency 2: The time from a wallet begins to propose a transaction to all the miners receive that transaction

Note that the Transaction Data size and the Verification time will decide the latency of the transaction data spreading on the network. In particular, Latency 1 includes the Transaction Generation Time and the time that the transaction data is transferred to the first miner(which is decided by the transaction data size), while the Latency 2 includes the Latency, the Verification Time of each node(miner), and the time that the transaction data spreads in the whole network.

Furthermore, we will compare the above four Key Performance Index (KPI)s from two perspectives: (1) the same mixin matrix size, and (2) the same privacy. In particular,

- For the same mixin matrix size, say l rows and m columns, we need to find $(l-1)\times m$ mixin input coins to form the mixing matrix, and the privacy will be $1/l^m$ for RCT+ and $1/l$ for RCT respectively.
- For the same privacy level, say $1/l^m$, for RCT, we need to find $(l^m-1)\times m$ mixin input coins, while for RCT+ we need to find $(l-1)\times m$ mixin input coins, to form the mixin matrix.

In addition, we will use a parameter K to denote the times of running a transaction process, and compute the average value of the above three items. We may adjust the value of K to get the desired results.

2 Experiment Designs

2.1 Experiment Environment

We build a simulating environment by deploying a 'private' Monero network.

- The network should be as similar as possible to the real Monero network, including the number of (miner) nodes and the connections among the nodes.
- We may use virtual machine to simulate the miner nodes.
- We only evaluate the four above items for transactions, not for blocks.

2.2 Experiment Designs

Under the same mixing matrix, say $l \times m$. First we need to design the values of (m,n) and l by investigating the real data of current Monero. We may also analysize and present the Monero data situations, then design the values of (m,n) and l. For (m,n) we may use the values that appear in Monero. For l, there may be only one value for Monero, and we may add some values to get a more comprehensive view.

For fairness, we run the simulation for RCT and RCT+ from the same start point, namely, setup a simulation environment, the run all the cases for RCT, and the setup a new/same environment and run all the cases for RCT+. NOTE that we may need to setup a new environment for each different l, while we may use the same environment for different (m,n).

1. For a $l\in[L]$ ([L] is the value set of l we designed):
   (a) For each $(m,n)\in[M,N]$($[M,N]$ is the value set of (m,n) we designed) run the following K times:
      i. A wallet proposes a transaction by choosing m coins to be the input coins and set n coins to be the output coins, running the Generation phase using these inputs;
      ii. The wallet broadcasts the Transaction Data to the network.

iii. Each miner receives the Transaction data, runs the Verification algorithm, and broadcasts the transaction data to the network.

(b) In the above step [1(a)i], the wallet records the time from choosing the input and output coins to broadcasting the transaction data, as well as the transaction data size. Each miner records the time it receives the transaction data, and the time it takes to perform the Verification. These information will enable us to compute the four KPIs.

Under the same privacy level, say $1/l^m$. First we need to design the values of (m, n) and l by investigating the real data of current Monero. We may also analysize and present the Monero data situations, then design the values of (m, n) and l. For (m, n) we may use the values that appear in Monero. For l, there may be only one value for Monero, and we may add some values to get a more comprehensive view.

For fairness, we run the simulation for RCT and RCT+ from the same start point, namely, setup a simulation environment, the run all the cases for RCT, and the setup a new/same environment and run all the cases for RCT+. NOTE that we may need to setup a new environment for each different l, while we may use the same environment for different (m, n).

1. For a $l \in [L]$ ([L] is the value set of l we designed):
   (a) For each $(m, n) \in [M, N]$($[M, N]$ is the value set of (m, n) we designed) run the following K times:
      i. A wallet proposes a transaction by choosing m coins to be the input coins and set n coins to be the output coins, running the Generation phase using these inputs; Note that for RCT, the wallet needs to choose $(l^m - 1) \times m$ coins to be the mixin coins, while for RCT+ the wallet needs to choose $(l - 1) \times m$ coins to be the mixin coins.
      ii. The wallet broadcasts the Transaction Data to the network.
      iii. Each miner receives the Transaction data, runs the Verification algorithm, and broadcasts the transaction data to the network.
   (b) In the above step [1(a)i], the wallet records the time from choosing the input and output coins to broadcasting the transaction data, as well as the transaction data size. Each miner records the time it receives the transaction data, and the time it takes to perform the Verification. These information will enable us to compute the four KPIs.