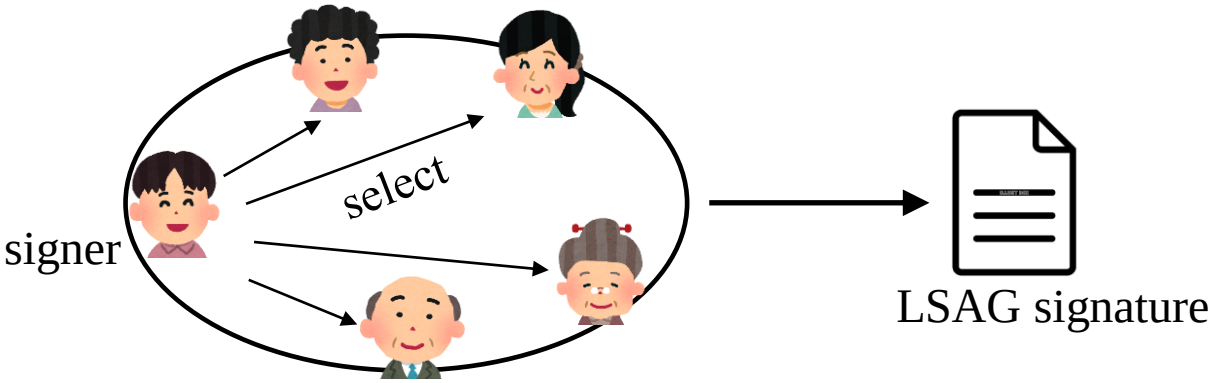
Partial Linkable Spontaneous Anonymous Group (PLSAG) signatures for Monero

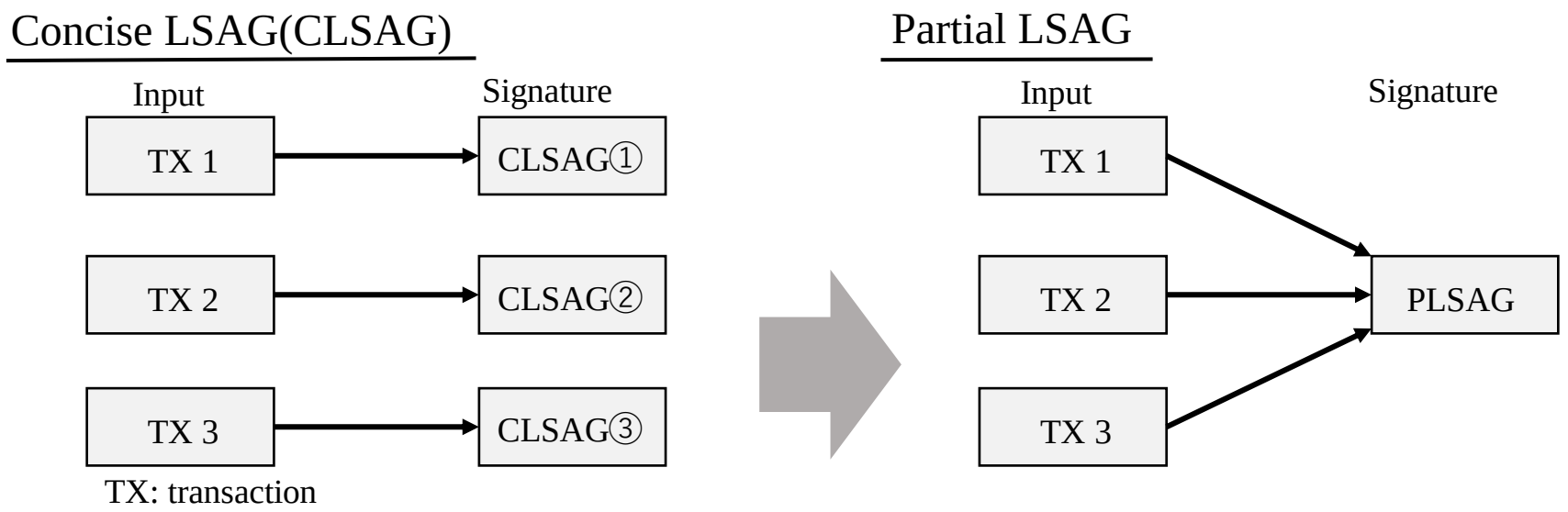
LSAG(Linkable Spontaneous Anonymous Group) Signatures

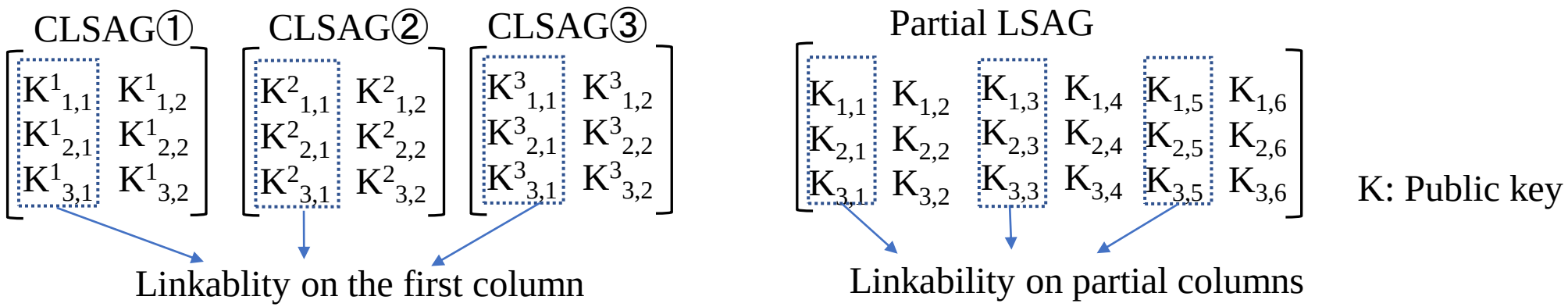
- It is necessary to prove sender's ownership of transaction inputs.
- A signer can select the group members. (Spontaneous)
- It is difficult for a third party to identify the actual signer in the group. (Anonymous)
- Avoiding double-spending attacks. (Linkable)
- Monero currently uses Concise LSAG (CLSAG) signatures.



Concept of Partial LSAG

- The number of signatures is reduced to one regardless of the transaction inputs.





Evaluation of PLSAG

- The anonymity set (5<N)
  → The total size of PLSAG is the smallest.

- N is usually much larger than M
  → PLSAG is more efficient than Concise LSAG and Multilayered LSAG.

Table1. size and signatures

Ring Signatures	The total signatures size
MLSAG	(2N+3)M
CLSAG	(N+3)M
PLSAG(Proposed)	$N+1+2M^2$

N: the number of anonymity sets
M: the number of inputs

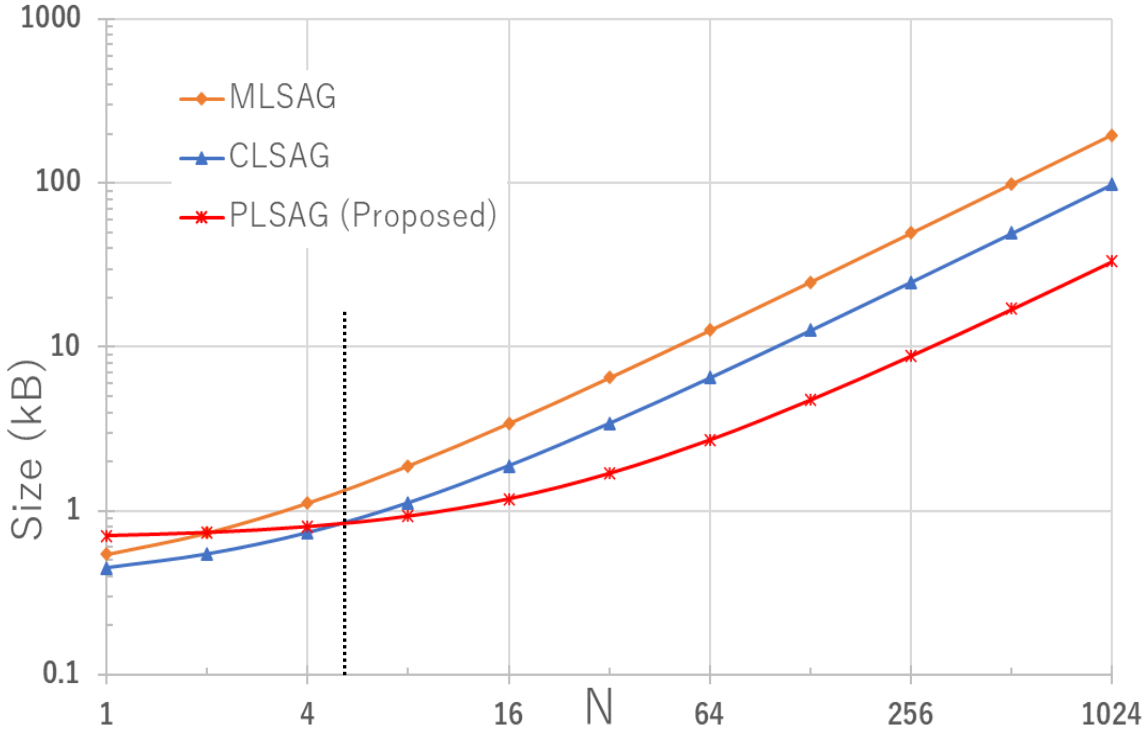


Fig1. Signature sizes for anonymity set size N with 3 inputs