**Blockchain Privacy
Ring Signatures**

Ring Signatures - Rivest, Shamir, Tauman

Signature solutions:

- Digital signatures → verifies against a specific public key

- Group signatures

- Ring signatures → verify against a set of public keys

- Linkable Ring signatures

"Set" Signatures

- Group signatures   ➡️   well defined group

- Ring signatures   ➡️   ad-hoc groups (great for cryptocurrencies)

- *Linkable* Ring signatures ➡️   reveal if a signer **already** produced a signature

- **Anonymity**
  An adversary cannot identify which ring signature
  corresponds to which of the public keys in the ring.
- **Unforgeability**
  An adversary cannot produce a valid signature, if it does not know a secret
  key corresponding to a public key included in the ring.
- **Exculpability**
  An adversary cannot produce a valid signature that links to the signature of
  another member of the ring, whose key the adversary does not control.
- **Linkability**
  Any two signatures produced by the same signer within the same ring are
  publicly linkable (i.e., anyone can detect that they were produced by the
  same signer).

"Set" Signatures

- Group signatures   ➡   well defined group

- Ring signatures   ➡   ad-hoc groups (great for cryptocurrencies)

- *Linkable* Ring signatures   ➡   reveal if a signer **already** produced a signature

- **Anonymity**
An adversary cannot identify which ring signature corresponds to which of the public keys in the ring.
- **Unforgeability**
An adversary cannot produce a valid signature, if it does not know a secret key corresponding to a public key included in the ring.
- **Exculpability**
An adversary cannot produce a valid signature that links to the signature of another member of the ring, whose key the adversary does not control.
- **Linkability**
Any two signatures produced by the same signer within the same ring are publicly linkable (i.e., anyone can detect that they were produced by the same signer).

Ring Signatures - Rivest, Shamir, Tauman

- Verify against **a set** of public keys. Computationally infeasible to determine <u>which</u> of the group members signed.

- Groups can be formed on an ad-hoc basis (vs. group signatures)

- *O(n)* for the resulting signature size
  n == number of public keys

- Does not hide transaction amounts!

Ring Signatures - Rivest, Shamir, Tauman

- Verify against **a set** of public keys. Computationally infeasible to determine <u>which</u> of the group members signed.

- Groups can be formed on an ad-hoc basis (vs. group signatures)

- *O(n)* for the resulting signature size n == number of public keys

RingCT ⟶ https://ww.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

- Does not hide transaction amounts!