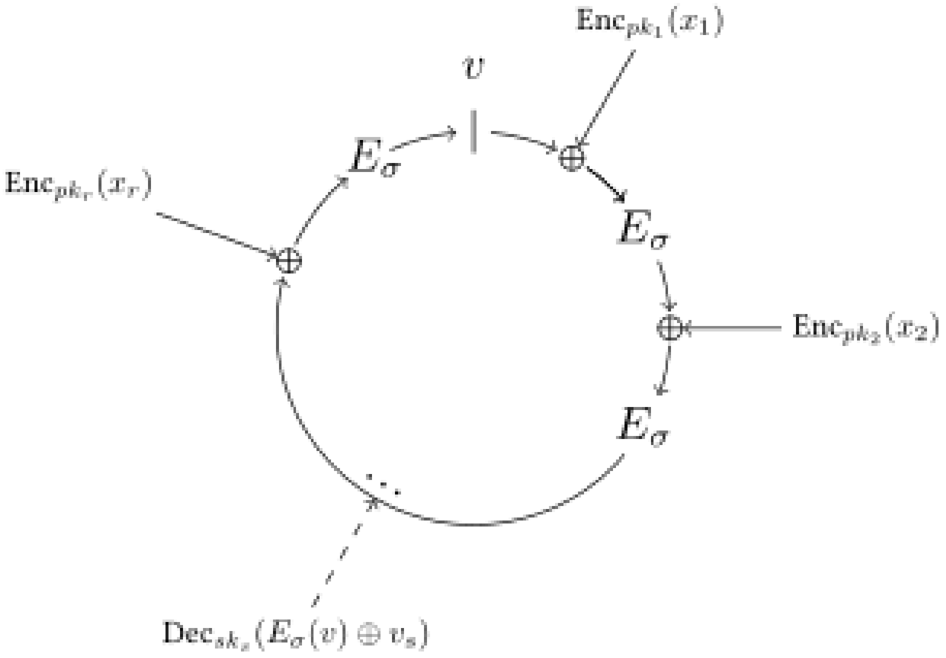
Privacy Network : Ring Signature

What is Ring Signature?

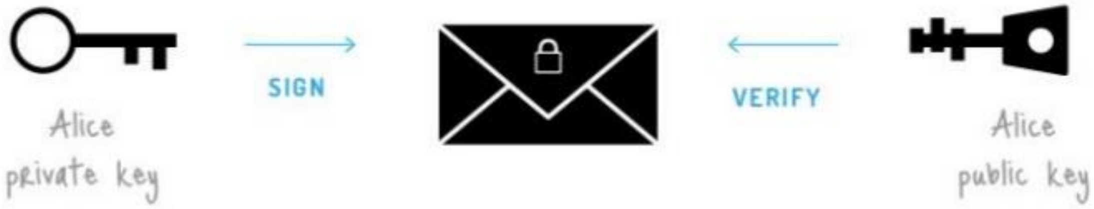

$\mathrm{Enc}_{pk_1}(x_1)$
v
E_σ
$\mathrm{Enc}_{pk_r}(x_r)$
E_σ
$\mathrm{Enc}_{pk_2}(x_2)$
E_σ
$\cdots$
$\mathrm{Dec}_{sk_s}(E_\sigma(v) \oplus v_s)$

Ring Signature is a type of Digital Signature that can be performed by any member of a group of users that each have keys.

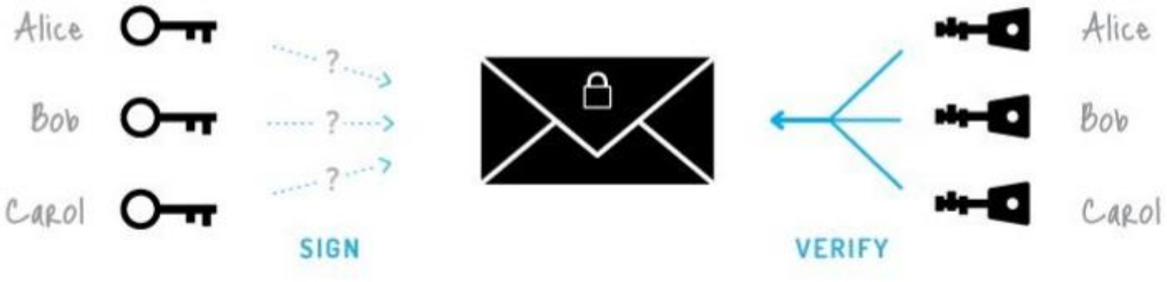
Users can make Ring with their public keys.
And They make Signature using by their own private key.

What is Ring Signature?

- Ordinary signature



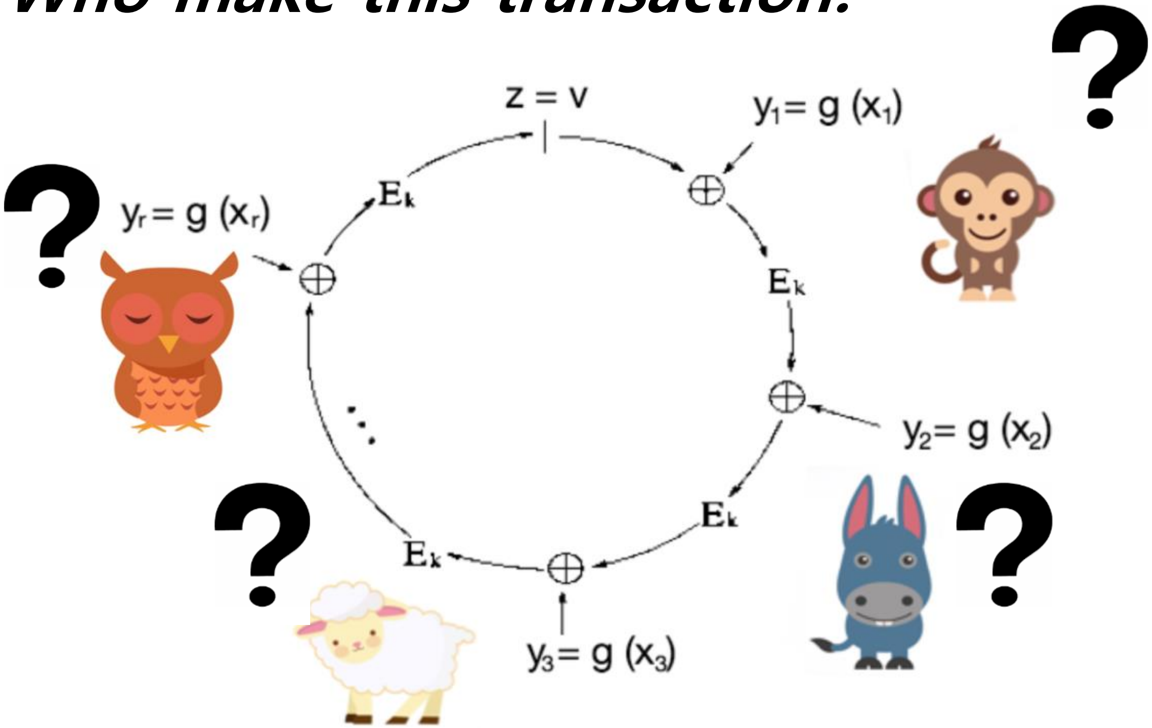
- Ring signature



Why we using Ring Signature?

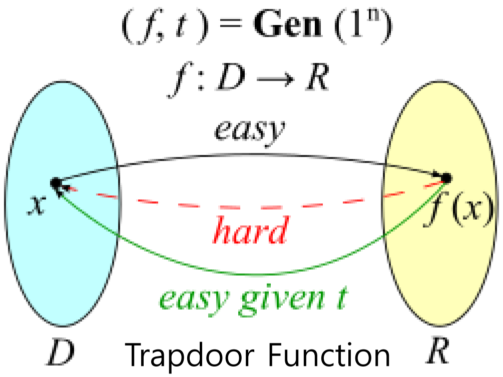
So, No one know who is Signature's owner.
The only thing we know is that "owner is member of that ring"

"Who make this transaction!"



How to make sign in Ring Signature

1. $K = h(m, P_1, P_2, \dots, P_r)$, $h =$ *Hash Function*, $P =$ *Ring Member's Public Keys*.
2. *Set Random* V *value*
3. $y_i = g_i(x_i)$, $x_i =$ *Random Value(with Seed)*, $g_i =$ *Trapdoor Permutation*
4. *Compute* y_s *that* $C_{K,v}(y_{1,}y_2, \dots, y_r) = V$
5. $C_{K,v}(y_{1,}y_2, \dots, y_r) = V$ *is same* $\dots . E_K[E_K[E_K[E_K[V \oplus y_1]] \oplus y_2] \oplus y_3] = V$
6. *Compute* $x_s = g_s{}^{-1}(y_s)$
7. $(P_1, P_2, \dots, V, x_1, x_2, \dots, x_r)$ *is Signature*!



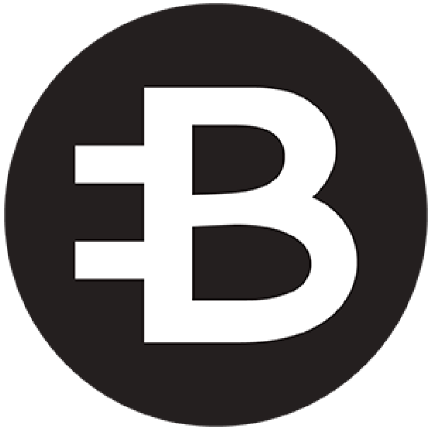
Trapdoor Function

How to make verify in Ring Signature

1. $Compute\ y_i =\ g_i(x_i)$
2. $Compute\ K = h(m, P_1, P_2, \ldots, P_r)$
3. $Verify\ that\ C_{K,v}(y_{1,} y_2, \ldots, y_r) = V$
4. $If\ it\ satisfied,\ verify\ Signature.$

If Signature's owner want to verify he is owner,
Then he can verify by his own seed value and x_s value.
Identifier can compute x_i by his own seed value.
And compared computed $x_s\ with\ his\ x_s$

Using Ring Signature



Many Cryptocurrency use Traceable Ring Signature to anonymize the sender of transaction.

References

1. How to leak a secret, Ron Rivest, Adi Shamir, and Yael Tauman, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science, pages 552–565.
2. Debnath, Ashmita; Singaravelu, Pradheepkumar; Verma, Shekhar (19 December 2012). "Efficient spatial privacy preserving scheme for sensor network". Central European Journal of Engineering.
3. E. Bresson; J. Stern; M. Szydlo (2002). "Threshold ring signatures and applications to ad-hocgroups" (PDF). Advances in Cryptology: Crypto 2002
4. Liu, Joseph K.; Wong, Duncan S. (2005). "Linkable ring signatures: Security models and new schemes“
5. Fujisaki, Eiichiro; Suzuki, Koutarou (2007). "Traceable Ring Signature". Public Key Cryptography
6. Fujisaki, Eiichiro (2011). "Sub-linear size traceable ring signatures without random oracles".

References

7. Au, Man Ho; Liu, Joseph K.; Susilo, Willy; Yuen, Tsz Hon (2006). "Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature". Lecture Notes in Computer Science.
8. CryptoNote Technology - Untraceable payments
9. Bytecoin profile
10. Shadow - Zero-knowledge Anonymous Distributed Electronic Cash via Traceable Ring Signatures.
11. Broken Crypto in Shadowcash