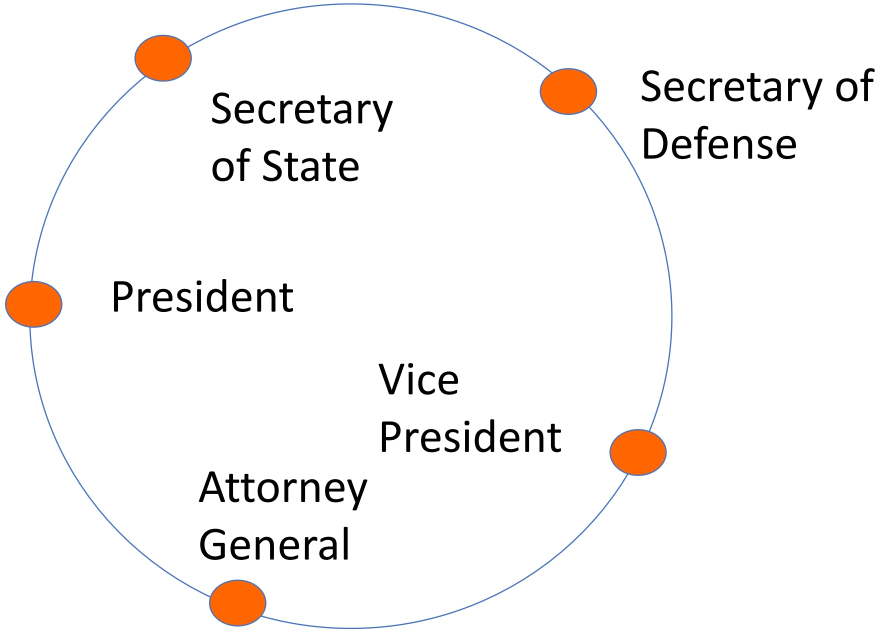
CSCI361

Ring Signatures: How to Leak a Secret

Problem

- How to generate an anonymous signature from a high-ranking White House official
  - ➢ We want to hide who signed the message
- Proposed by Rivest, Shamir and Tauman

Who signed?

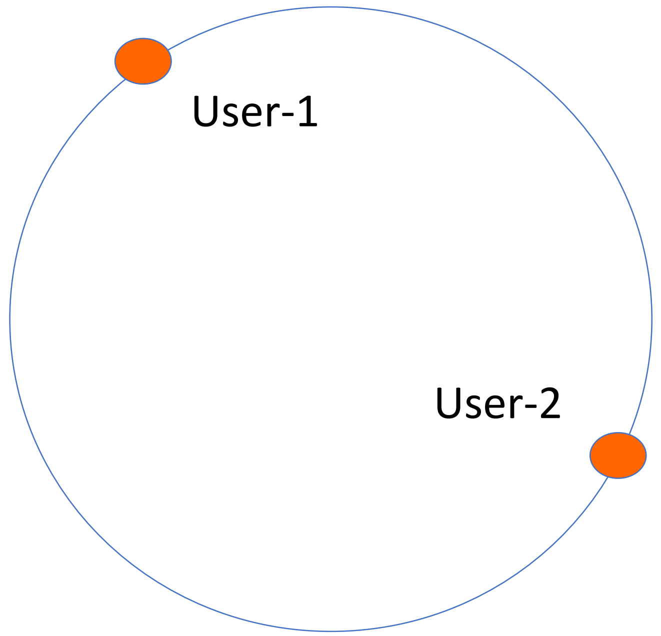


Ring Signature

- A type of digital signature that can be produced by any member of a group of users who have private keys
- A message signed with a ring signature can be verified by anyone
- Important features
  - It is impossible (computationally infeasible) to determine which of the group members' keys was used to produce the signature
  - There is no way to revoke the anonymity of a given ring signature
  - Any members in the ring can produce a ring signature without setup

Realisation of Ring Signature for Two Users

- Setup: User-1 with public key $P_1=(e_1,N_1)$ and private key (d_1,N_1); User-2 with public key $P_2=(e_2,N_2)$ and private key (d_2,N_2)
- They are using RSA for underlying singing algorithm
- H: A cryptographic hash function like SHA
- E: Symmetric encryption. E^{-1}: Symmetric decryption = D → E is called a Pseudo Random Function (PRF).



Realisation of Ring Signature for Two Users

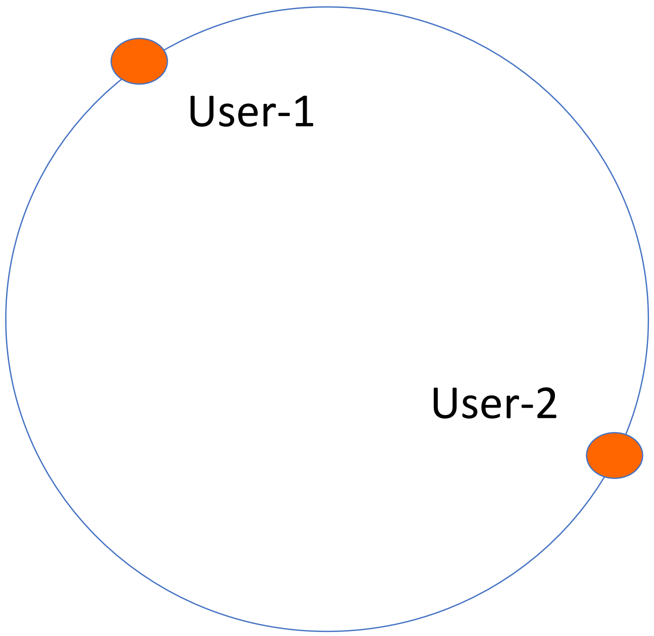
- Assume that User-2 is the signer
  - User-2 gets his message m and calculate the key $k = H(m)$.
  - Pick a random glue value v.
  - Pick a random x_1 for User-1 and calculate $y_1 = x_1^{e_1} \bmod N_1$.
  - Solve an equation for $E_k(y_2 \oplus E_k(y_1 \oplus v)) = v$, where E is symmetric encryption, to get y_2: $y_2 = E^{-1}_k(v) \oplus E_k(y_1 \oplus v)$
  - Calculate $x_2 = y_2^{d_2} \bmod N_2$.
  - The ring signature is now (P_1, P_2, v, x_1, x_2).

Realisation of Ring Signature for Two Users

- Signature Verification
  - Calculate $y_1 = x_1^{e_1} \bmod N_1$ and $y_2 = x_2^{e_2} \bmod N_2$.
  - Calculate $k = H(m)$.
  - Check whether $E_k(y_2 \oplus E_k(y_1 \oplus v)) = v$. If yes, the ring signature on m is valid, otherwise, it is invalid.

Example: Realisation of Ring Signature for Two Users

- Setup: User-1 with public key P_1=(3,55) and private key (27,55); User-2 with public key P_2=(5,65) and private key (29,65)
- They are using RSA for underlying singing algorithm
- H: SSHA (4 bit output)
- E: Symmetric encryption. E^{-1}: Symmetric decryption = D



Example: Realisation of Ring Signature for Two Users

- Assume that User-2 is the signer
  - User-2 gets his message m=5 and calculate the key k= 1101 = H(5).
  - Pick a random glue value v=1010001.
  - Pick a random x_1 =3(=0000011) for User-1 and calculate $y_1=x_1^{e_1} \bmod N_1 = 3^3 \bmod 55$ =27=0011011.
  - Solve an equation for $E_k(y_2 \oplus E_k(y_1 \oplus v)) = v \rightarrow E_{1101}(y_2 \oplus E_{1101}(0011011 \oplus 1010001)) = 1010001$ to get y_2:
    - ✓ $y_2 = E^{-1}_{1101}(1010001) \oplus E_{1101}(0011011 \oplus 1010001) = E^{-1}_{1101}(1010001) \oplus E_{1101}(1001010) = 1010111 \oplus 0100101 = 1110010 \bmod 65 = 114 \bmod 65 = 49 = 0110001$ (Assume that $E^{-1}_{1101}(1010001) = 1010111$) and $E_{1101}(1001010) = 0100101$)
    - ✓ After y_2 is calculated, we know that $E_{1101}(0110001 \oplus 0100101) = E_{1101}(0010100) = 1010001$

Example: Realisation of Ring Signature for Two Users

(continued)

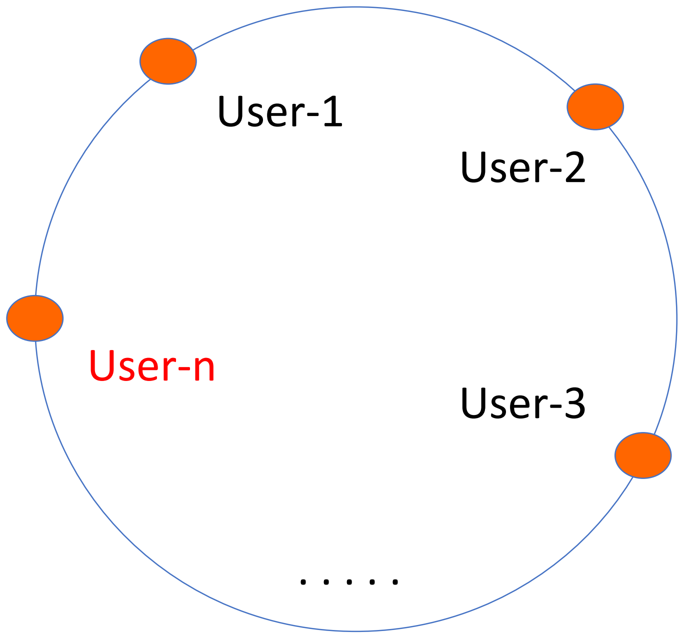
- Calculate $x_2 = y_2^{d_2} \bmod N_2 = 49^{29} \bmod 65 = 4 = 0000100$.
- The ring signature is now $(P_1, P_2, v, x_1, x_2) = ((3,55)(5,65), 1010001, 0000011, 0000100)$.

Realisation of Ring Signature for Two Users

- Signature Verification
  - Calculate $y_1 = x_1^{e_1} \bmod N_1 = 0000011^3 \bmod 55 = 3^3 \bmod 55 = 27$ (=0011011) and $y_2 = x_2^{e_2} \bmod N_2 = 0011101^5 \bmod 65 = 4^5 \bmod 65 = 49$ (=0110001).
  - Calculate k = H(m)=H(5)=1101.
  - Check whether $E_k(y_2 \oplus E_k(y_1 \oplus v)) = v$. → $E_{1101}(0110001 \oplus E_{1101}(0011011 \oplus 1010001)) \rightarrow E_{1101}(0110001 \oplus E_{1101}(1001010)) \rightarrow E_{1101}(0110001 \oplus 0100101) \rightarrow E_{1101}(0010100) = 1010001$ (See page 8)

Realisation of Ring Signature for n Users

- Before we desribe n user scheme, assume (without loss of generality) that among n users, “User-n” is always a name for the group member who generates a ring siganture.
  - ✓ Of course anyone in the group can be “User-n”



Realisation of Ring Signature for n Users

- User-1 with public key $P_1=(e_1,N_1)$ and private key (d_1,N_1); User-2 with public key $P_2=(e_2,N_2)$ and private key (d_2,N_2);…, User-(n-1) with public key $P_{n-1}=(e_{n-1},N_{n-1})$ and private key (d_{n-1},N_{n-1})
  - User-n gets her message m and calculate the key k = H(m).
  - Pick a random glue value v.
  - Pick a random x_1 for User-1, x_2 for User-2, …, x_{n-1} for User-(n-1) and calculate $y_1=x_1^{e_1} \bmod N_1$, $y_2=x_2^{e_2} \bmod N_1$, …, $y_{n-1}=x_{n-1}^{e_{n-1}} \bmod N_{n-1}$.

Realisation of Ring Signature for n Users

- Solve an equation for $E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\bullet\bullet\bullet E(_k(y_1 \oplus v) \bullet\bullet\bullet)))=v$, where E is symmetric encryption.
- Calculate $x_n = y_n^{d_n} \bmod N_n$.
- The ring signature is now $(P_1, P_2, \ldots, P_n, v, x_1, x_2, \ldots, x_n)$.