Blind Signature

Suppose Bob has mad an important discovery.

He wants to record publicly what he has done, but he does not want anyone else to know.

Goal: allow Alice to sign a document without knowing its contents.

1. Alice
   - execute $\mathsf{RSA.KeyGen}(1^\lambda)$
   - $vk = \{n, e\}$ and $sk = \{p, q, d\}$.
2. Bob
   - Choose a random $r \leftarrow \mathbb{Z}_n$ with $\gcd(r, n) = 1$
   - Compute $t \equiv r^e m \bmod n$
3. Alice
   - Compute $s \equiv t^d \bmod n$
4. Bob
   - Compute $\sigma := s/r$

- σ is a digital signature of m since $s/r \equiv t^d/r \equiv (r^e m)^d/r \equiv m^d \bmod n$,

Dangers of RSA Blind Signature

- Suppose Bob has a ciphertext $c = \mathsf{Enc}(m)$ which is encrypted through RSA.
- In Step 2,
  - $t \equiv r^e c \equiv (m^e \bmod n) r^e \bmod n \equiv (mr)^e \bmod n$
- In Step 3,
  - $s \equiv t^d \equiv mr \bmod n$
- In Step 4,
  - Bob can obtain $\sigma = s/r \equiv m \bmod n$ since $\gcd(r, n) = 1$

Ring Signature

Def. Ring signature consists of $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$:

- $(vk_1, sk_1), \ldots, (vk_n, sk_n) \leftarrow \mathsf{KeyGen}(1^\lambda, n)$;
  - Input: a security parameter λ and a number of ring users n
  - Output: a verification key vk_i and a signing key sk_i for each ring users
- $\sigma \leftarrow \mathsf{Sign}(m, vk_1, \ldots, vk_n, sk_i)$ for some $1 \leq i \leq n$;
  - Input: a message m, all verification keys $vk_1, \ldots, vk_n$ and a signing key sk_i for some user
  - Output: a signature σ of m
- $b \leftarrow \mathsf{Verify}(m, \sigma, vk_1, \ldots, vk_n)$;

  - Input: a message m, a signature σ and all verification keys $vk_1, \dots, vk_n$
  - Output: a bit $b = 1$ if σ is a valid siganture of m signed by sk_i for $1 \le i \le n$

Group Signature

Def. Group signature consists of $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Open})$:

- $(vk, msk, sk_1, \dots, sk_n) \leftarrow \mathsf{KeyGen}(1^\lambda, n)$;
  - Input: a security parameter λ and a number of group users n
  - Output: a verification key vk, a master secret key msk, a signing key sk_i for each group users
- $\sigma \leftarrow \mathsf{Sign}(m, sk_i)$ for some $1 \le i \le n$;
  - Input: a message m and a signing key sk_i
  - Output: a signature σ of m
- $b \leftarrow \mathsf{Verify}(m, \sigma, vk)$;
  - Input: a message m, a signature σ and a verification key vk
  - Output: a bit $b = 1$ if σ is a valid signature of m signed by sk_i for $1 \le i \le n$
- $i \leftarrow \mathsf{Open}(m, \sigma, msk)$;
  - Input: a message m, a signature σ and a master secret key msk
  - Output: a user i or $\perp$