17. Ring Signatures

The goal of this part is to study ring signatures.

A signature scheme allows a signer $P$ to authenticate a message $m$ in such a way that anybody can verify it, and nobody can impersonate $P$.

More formally, a signature scheme assumes a PKI (Public-Key Infrastructure): every player $P_i$ owns a pair of signing/verification keys $(sk_i, vk_i)$, such that $vk_i$ is publicly binded to his identity $P_i$. Then, there are two algorithms:

- $\text{Sign}(sk, m)$ takes the signing key $sk$ and the message $m$ as inputs, and outputs the signature $\sigma$;
- $\text{Verify}(vk, m, \sigma)$ takes the verification key $vk$, the message $m$ and the signature $\sigma$ as inputs, and outputs 1 if the signature is valid with respect to $m$ and $vk$, and 0 otherwise.

The unforgeability result says that it is hard to generate a message/signature pair $(m, \sigma)$ that is valid with respect to the verification key $vk$ without the associated signing key $sk$:

$$\text{Succ}_{\text{euf-nma}}(A) = \Pr[(sk, vk) \leftarrow \text{KeyGen}(1^k), (m, \sigma) \leftarrow A(vk) : \text{Verify}(vk, m, \sigma) = 1] = \text{negl}(k).$$

This is the Existential UnForgeability (EUF), without access to any signature, hence the No-Message Attack (NMA).

A ring signature allows a player $P_j$ to anonymously authenticate a message $m$ as a member of an ad-hoc group, called a ring $R$:

- $\text{Sign}(sk, R, m)$ takes a signing key $sk$, a ring $R = \{vk_i\}$ of verification keys containing the verification key $vk$ associated to $sk$, and the message $m$ as inputs, and outputs the signature $\sigma$;
- $\text{Verify}(R, m, \sigma)$ takes a ring $R = \{vk_i\}$, the message $m$ and the signature $\sigma$ as inputs, and outputs 1 if the signature is valid with respect to $m$ and $R$, and 0 otherwise.

The unforgeability result says that it is hard to generate a message/signature pair $(m, \sigma)$ that is valid with respect to a ring $R$ without a signing key associated to one of the verification keys in $R$.

**Q-1.** Explain how a ring signature allows a member of a community to anonymously reveal and authenticate some information, just as a member of this community.

### 17.1 Hash-and-Sign RSA Signature

Let us consider the following generation of signing/verification keys, for a security parameter $k$:

- One chooses 2 random primes $2^k - 2^{k/2} < p, q < 2^k$, such that $65537 = 2^{16} + 1$ does not divides $p - 1$ nor $q - 1$;
- One sets $n \leftarrow pq$, $e \leftarrow 65537$, and $d = e^{-1} \mod (p - 1)(q - 1)$;
- The signing key is set as $sk = (n, d)$ and the verification key is set as $vk = (n, e)$.

**Q-2.** From the fact that the number $\pi(x)$ of prime integers smaller than $x$ is approximately $x/\ln x$, and assuming that one can efficiently check whether an integer is prime or not, explain how efficiently one can generate such key pairs $(sk, vk)$. 
We additionally consider a hash function \( H \) onto \( \{0, 1\}^k \), that can be seen as \( \{0, \ldots, 2^k - 1\} \). We model \( H \) as a random oracle \((i.e., every new query is answered by a truly random value in \( \{0, \ldots, 2^k - 1\}\)).

**Q-3.** Explain why, for any modulus \( n \) generated as above, we can consider that the output space of \( H \) is \( \mathbb{Z}_n^* \), up to a negligible probability. Note that the cardinality of \( \mathbb{Z}_n^* \) is \( \varphi(n) = (p - 1)(q - 1) \).

For a PKI with such RSA keys for any player, we consider the following algorithms:

- **Sign**(sk, m): for a message m and sk = (n, d), one outputs \( \sigma = H(m)^d \mod n \);
- **Verify**(vk, m, \( \sigma \)): for a message m, a signature \( \sigma \), and vk = (n, e), one checks whether \( H(m) = \sigma^e \mod n \).

**Q-4.** Prove that this signature scheme achieves the EUF-NMA security level under the RSA assumption. We stress that we just consider NMA security, and remind that an RSA challenge \((n, e, y)\) expects to get as output an \( x \) such that \( y = x^e \mod n \).

### 17.2 Ring Signature

Still using the same PKI and hash function \( H \) onto \( \{0, 1\}^k \), we want to define a ring signature: we consider a ring \( R = \{vk_i = (n, e), i = 0, \ldots, \ell - 1\} \), among which users, the \( j \)-th user wants to sign in the name of the ring \( R \) and owns the pair \((vk, sk)\), with \( vk = (n, e) = vk_j \) the verification key associated to the signing key \( sk = (n, d) \).

- One initializes the ring with \( v_j \overset{\$}{\leftarrow} \{0, 1\}^k \), and \( h_j \leftarrow H(R, m, j, v_j) \);
- For \( i' = j + 1, \ldots, \ell + j - 1 \), one sets \( i = i' \mod \ell \), chooses a random \( x_i \overset{\$}{\leftarrow} \mathbb{Z}_n^* \) and sets \( y_i \leftarrow x_i^d \mod n, v_i \leftarrow y_i \oplus h_{i-1}, \) and \( h_i \leftarrow H(R, m, i, v_i) \);
- One closes the ring with \( y_j \leftarrow v_j \oplus h_{j-1}, \) and \( x_j \overset{\$}{\leftarrow} y_j^d \mod n \) (if \( y_j \geq n \), one aborts);
- The signature consists of \( \sigma = (v_0, x_0, \ldots, x_{\ell-1}) \) for the ring \( R = \{vk_i, i = 0, \ldots, \ell - 1\} \).

**Q-5.** Explain that this algorithm may fail (abort), but with negligible probability only.

**Q-6.** Describe the verification algorithm.

**Q-7.** Show that \( \sigma \) follows indistinguishable distributions whatever the index \( j \) is. Explain that the signer is perfectly anonymous among the \( \ell \) users in the ring \( R \).
We now show that it is hard for an adversary to generate a ring signature $\sigma = (v_0, x_0, \ldots, x_{\ell-1})$ on any message $m$ on behalf of a ring $R$ of size $\ell$ without being part of this ring.

**Q-8.** First, show that for a signature $\sigma = (v_0, x_0, \ldots, x_{\ell-1})$ to have a chance to be valid, all the queries $h_i \leftarrow \mathcal{H}(R, m, i, v_i)$, for the appropriate $v_i$ must have been asked.

**Q-9.** Second, show that there must exist an index $i$ such that the query $h_i \leftarrow \mathcal{H}(R, m, i, v_i)$ has been asked before $h_{i-1} \leftarrow \mathcal{H}(R, m, i-1, v_{i-1})$, where the indices are modulo $\ell$.

**Q-10.** Eventually, describe in details a reduction that first guesses such an index $i$ and then show that, if $vk_i = (n_i, e)$ is not a key owned by the adversary, there is a good chance to break RSA for the modulus $n_i$ and exponent $e$, by setting the value of $\mathcal{H}(R, m, i-1, v_{i-1})$ appropriately from the RSA challenge ($n = n_i, e, y$).