Assignment-III

Assignments on PKE, Identification Scheme and Digital Signature

Submission Deadline: 31st December, 2022

1. Let $N = pq$ with p, q distinct, odd primes. Fix $z \in QNR_N^{+1}$. Show that choosing random $x \leftarrow QR_N$ and setting $y := [z \cdot x \ mod \ N]$ gives a y that is uniformly distributed in QNR_N^{+1}. I.e., for any $\hat{y} \in QNR_N^{+1}$,

$$Pr[z \cdot x = \hat{y} \ mod \ N] = \frac{1}{|QNR_N^{+1}|}$$

   where the probability is taken over random choice of $x \leftarrow QR_N$.

   Hint: Show $x \in QR_N$ implies $[x^{-1} \ mod \ N] \in QR_N$ and $x \in QNR_N^{+1}$ implies $[x^{-1} \ mod \ N] \in QNR_N^{+1}$.

2. Consider a variant of Goldwasser-Micali encryption scheme:
   GenModulus(1^n) outputs $< N, p, q >$ where $N = pq$ and $p = q = 3 \ mod \ 4$. The Public key being N, Secret key being $< p, q >$. To encrypt $m \in \{0, 1\}$, the sender chooses uniformly $x \in \mathbb{Z}_N$ and computes the cipher text as $c := [(-1)^m \cdot x^2 \ mod \ N]$. Then prove that:

   (a) For N in the above stated form, $[-1 \ mod \ N] \in QNR_N^{+1}$.

   (b) The described encryption scheme achieves CPA security if deciding Quadratic Residuocity is hard relative to **GenModulus**.

3. Assume deciding quadratic residuosity is hard for GenModulus. Show that this implies the hardness of distinguishing a uniform element of QR_N from a uniform element of $\mathcal{J}^{+1}$.

4. Show that plain RSA encryption of a message m leaks $\mathcal{J}_N(m)$.

5. Consider the Lamport signature scheme. Prove that it is one time secure. Moreover describe an adversary who obtains signatures on two messages of its choice and can then forge signatures on any message it likes.

6. Suppose OTS is one-time-secure signature scheme. Now cosider a statefull signautre scheme construted using OTS.
   $GENMODULUS(1^n)$: It runs l independent instances of $OTS.GenModulus$ and gets the corresponding outputs $< pk_i, sk_i >$; $i \in [1, l]$. The final output is: $< PK, SK, 0 >$ where,

$$PK = \{pk_1, pk_2, \cdots, pk_l\}$$
$$SK = \{sk_1, sk_2, \cdots, sk_l\}$$

   and 0 is the initial state. $SIGN_{PK}(m, i) = \Big(OTS.Sign_{pk_i}(m), i), i + 1\Big)$
   $VRFY_{SK}((\sigma_{11}, \sigma_{12}), m) = Vrfy_{sk_{\sigma_{12}}}(\sigma_{11}, m)$
   Prove that if OTS one time secure then the newly constructed statefull signature scheme is also secure.

7. Assume the RSA problem is hard. Show that the plain RSA signature scheme satisfies the following weak definition of security: An attacker is given the public key $< N, e >$ and a uniform message $m \in Z_N^*$. The adversary succeeds if it can output a valid signature on m without making any signing queries.

8. Show how an atacker can forge a plain RSA signature on an arbitrary message using a single signing query.

9. Consider a variant of the Fiat-Shamir transform in which the signature is (I, s) rather than (r, s) and the verification is changed in the natural way. Show that if the underlying identification scheme is secure, then the resulting signature scheme is also secure.