MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Random self-reducibility of Quadratic Residuosity). *Show that Quadratic Residuosity problem for a fixed $N = pq$ where p and q are some Blum primes is randomly self-reducible. Recall that a prime p is a Blum prime if $p \equiv 3 \mod 4$ and an element $y \in \mathbb{Z}_n$ is a quadratic residue if there exists x such that $y = x^2 \mod n$. The element y can be quadratic residue only if its Jacobi symbol $\left(\frac{y}{n}\right) = 1$. However, only half of the elements with Jacobi symbol one*

$$J_n = \left\{ y \in \mathbb{Z}_N : \left(\frac{y}{n}\right) = 1 \right\}$$

belong to the set of quadratic residues

$$QR_n = \left\{ y \in \mathbb{Z}_n : \exists x \in \mathbb{Z}_n : x^2 \equiv y \pmod N \right\} \ .$$

The Quadratic Residuosity problem is to distinguish between random elements of QR_n and $J_n \setminus QR_n$.

Solution. Advantage against Quadratic Residuosity.

Define advantage

$$\mathsf{Adv}^{\mathsf{qrp}}_n(\mathcal{A}) = ??$$

where

$$\begin{array}{ll} \mathcal{Q}_0^{\mathcal{A}} & \qquad \mathcal{Q}_1^{\mathcal{A}} \\ \left[\begin{array}{l} x \xleftarrow{u} QR_n \\ ?? \end{array}\right. & \qquad \left[\begin{array}{l} x \xleftarrow{u} J_n \setminus QR_n \\ ?? \end{array}\right. \end{array}$$

Number theoretic properties of Quadratic Residues. One can show that Jacobi symbols satisfies following equations

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) \qquad \text{and} \qquad \left(\frac{a^2}{n}\right) = 1 \ .$$

Explain how one can rerandomise Quadratic Residues

Reduction construction.

Give a reduction construction

Analyse it success and running-time.