Lecture 16 §3.9 & 3.10: Quadratic Residue & Probabilistic encryption

Probabilistic Encryption

Scenario: Plaintext m is very short, e.g. one bit

Problem If plaintext is short, when Eve sees a ciphertext c, she can just encrypt both 0 & 1 & see which gives c.

Soln Choose random padding r & encrypt (m, r).

Goldwasser-Micali Public Key Cryptosystem

Hard problem: Decide whether $x^2 \equiv a \pmod N$ has a solution when $N = pq$, p, q prime.

Like w/ RSA, this is easy to do if we know p & q, hard if we only kno

Def Say a is a quadratic residue mod N if there $\exists$ a solution to $x^2 \equiv a \pmod N$. If a is not a quadratic residue it is called a quadratic nonresidue mod N.

Ex $p = 5$, $a \in (\mathbb{Z}/5\mathbb{Z})^\times$

u	1	2	3	4
u^2	1	4	4	1

$\Rightarrow$ 1 & 4 are quadratic residues

2 & 3 are quadratic nonresidues

Abbreviate Quadratic Residue → QR

Quadratic NonResidue NR

Prop Suppose that a & b are relatively prime to N.

(1) If a & b are both quadratic residues mod N then ab is a quadratic residue mod N.

(2) If a is a quadratic residue mod N & b is a quadratic nonresidue mod N then ab is a quadratic nonresidue mod N.

(3) Only when N is prime!
If a is a nonresidue mod N & b is a nonresidue mod N then ab is a quadratic residue mod N.

In other words:

$$QR \cdot QR = QR$$
$$QR \cdot NR = NR$$
$$NR \cdot NR = QR \leftarrow \text{only when } N \text{ prime.}$$

Pf

(1) If a & b are quadratic residues,

$$a \equiv x^2 \pmod N \qquad b \equiv y^2 \pmod N$$

$\Rightarrow ab \equiv (xy)^2 \pmod N$ is a quadratic residue too.

(2) If a a QR & ab a QR then

$$a \equiv x^2 \qquad\qquad ab \equiv z^2$$

$\Rightarrow b = (ab)(a^{-1}) = (zx^{-1})^2$ is a QR.

(3) If N is prime,

$$\log_g : (\mathbb{Z}/N)^\times \xrightarrow{\cong} \mathbb{Z}/(N-1)$$

$\log_g(x^2) = 2\log_g(x)$ so a is a QR

iff $\log(a)$ is even.

$\log(ab) = \log(a) + \log(b)$

So if a & b are nonresidues,

$\log(a)$ & $\log(b)$ are odd

& so $\log(ab) = \log(a) + \log(b)$ is even

So ab is a quadratic residue. $\square$

Goldwater-Mizali Public key Cryptosystem

Alice

Bob

Private key: p, q

Public key: $N = pq$

a not a quadratic residue mod p or mod q.

$\xrightarrow{(N, a)}$

$m \in \{0,1\}$

Pick random $r \in \mathbb{Z}/N\mathbb{Z}$

$c = a^m r^2$

$= \begin{cases} r^2 & \text{if } m=0 \\ ar^2 & \text{if } m=1 \end{cases}$

$\xleftarrow{c}$

If c a quadratic residue mod p

then $m=0$

if not, $m=1$.

Def If $a \in \mathbb{Z}$ & p is an odd prime then the Legendre Symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ QR mod } p \\ -1 & \text{if } a \text{ NR mod } p \\ 0 & \text{if } p \mid a \end{cases}$$

Proposition says $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

<u>Goal</u> Determine if a is a QR mod p or not.

$\Leftrightarrow$ calculate $\left(\frac{a}{p}\right)$.

<u>Thm</u> (Quadratic Reciprocity)

Let p & q be odd primes.

(1) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$

(2) $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

(3) $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$ ☆

$\square$

(3) is the reciprocity law: it relates $\left(\frac{p}{q}\right)$ to $\left(\frac{q}{p}\right)$ which a priori would seem completely unrelated.

This is one of the most prized results of classical number thy. Hundreds of proofs have been published & a significant part of modern algebraic number thy concerns generalizations of this result, most notably Class Field theory & Artin Reciprocity.

The reciprocity law is useful for computation b/c if $p<q$, we can replace $\left(\frac{p}{q}\right)$ w/ $\left(\frac{q}{p}\right)$, reduce q mod p & repeat.

Ex $\left(\frac{21}{53}\right) = \left(\frac{3}{53}\right) \cdot \left(\frac{7}{53}\right)$

$$\overset{(3)}{=} \underbrace{(-1)^{\frac{(3-1)(53-1)}{4}}}_{-1} \left(\frac{53}{3}\right) \underbrace{(-1)^{\frac{(7-1)(53-1)}{4}}}_{-1} \left(\frac{53}{7}\right)$$

$$= \left(\frac{2}{3}\right) \cdot \left(\frac{4}{7}\right)$$

$$= \left(\frac{2}{3}\right)\cdot\left(\frac{2}{7}\right)^2 = \left(\frac{2}{3}\right) \overset{(2)}{=} -1$$

So 21 is not a quadratic residue mod 53.

The disadvantage of this approach is that we have to factor the top to proceed, but factoring can be hard. This issue can be fixed:

<u>Def</u> Suppose $N = p_1^{e_1} \cdots p_r^{e_r}$. The <u>Jacobi symbol</u> is

$$\left(\frac{a}{N}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

Jacobi Symbol

Legendre symbol

The Jacobi symbol extends the Legendre symbol to the case when N not prime.

<u>Rmk</u> a a QR mod $N \Rightarrow a$ is a QR mod p_i

$$\Rightarrow \left(\frac{a}{N}\right) = 1.$$

The converse is only true when N prime.

<u>Ex</u> $N = 3\cdot 5$, $a = 8$.

$$\left.\begin{aligned} \left(\frac{8}{3}\right) &= \left(\frac{2}{3}\right) = -1 \\ \left(\frac{8}{5}\right) &= \left(\frac{3}{5}\right) = -1 \end{aligned}\right\} \Rightarrow \left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = 1.$$

So $\left(\frac{8}{15}\right) = 1$ but 8 is not a QR mod 15.

<u>Prop</u> Quadratic reciprocity is also true for the Legendre symbol.

(This can be checked directly)

<u>Ex</u>
$$\left(\frac{21}{53}\right) = \underbrace{(-1)^{\frac{20\cdot 52}{4}}}_{1} \left(\frac{53}{21}\right)$$
$$= \left(\frac{11}{21}\right) = \underbrace{(-1)^{\frac{10\cdot 20}{4}}}_{1} \left(\frac{21}{11}\right)$$
$$= \left(\frac{-1}{11}\right) \overset{(ii)}{=} -1.$$

The Jacobi symbol makes it very easy to determine whether or not a a QR mod N provided that we can factor N.

Returning to the Goldwater - Micali scheme:

Alice receives

$$c = \begin{cases} a r^2 & m = 1 \\ r^2 & m = 0 \end{cases} = a^m r^2$$

Since Alice knows p, she uses Quadratic reciprocity to easily determine

$$\left(\frac{c}{p}\right) = \left(\frac{a^m r^2}{p}\right) = \left(\frac{a}{p}\right)^m \left(\frac{r}{p}\right)^2 = \left(\frac{a}{p}\right)^m = (-1)^m = \begin{cases} 1 & m = 0 \\ -1 & m = 1 \end{cases}$$

Eve may easily calculate $\left(\frac{c}{N}\right)$ but this does her no good:

$$\left(\frac{c}{N}\right) = \left(\frac{a^m r^2}{N}\right) = \left(\frac{a}{N}\right)^m = \left(\frac{a}{p}\right)^m \left(\frac{a}{q}\right)^m$$

$$= (-1)^m \cdot (-1)^m = 1.$$