9.4 Probabilistic Public key Encryption

Prop 9.7 Let $n = p \cdot q$, $p \neq q$ prime. Then

a QR mod n ($\Leftrightarrow$) a QR mod p and a QR mod q.

Proof: "$\Rightarrow$" $\exists x : x^2 \equiv a \pmod n \overset{\text{Prop 8.1}}{\Rightarrow} x^2 \equiv a \pmod p \wedge x^2 \equiv a \pmod q$

"$\Leftarrow$" $\exists x : x^2 \equiv a \pmod p$, $\exists y : y^2 \equiv a \pmod q$

$\overset{\text{Prop 9.4}}{\Rightarrow} \exists f : f^2 \equiv a \pmod n$

Def 9.8 Let $p > 2$ be prime, $a \in \mathbb{N}$. The Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod p \\ 1, & a \text{ QR mod } p \\ -1, & \text{otherwise} \end{cases}$$

Let $n = \prod_i p_i^{k_i}$ the prime factorization of an odd $n \in \mathbb{N}$

Then the Jacobi symbol is defined as

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{k_i}$$

Remark 9.9

a) For any odd $n \in \mathbb{N}$: $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

b) There is an efficient algorithm for computing $\left(\frac{a}{n}\right)$ with run time $O((\ln n)^2)$ (see HoV p. 73) without factoring!

Unlike the Legendre symbol, the Jacobi symbol does not reveal whether a is a QR mod n. It holds that

$$a \text{ QR mod } n \Rightarrow \left(\frac{a}{n}\right) = 1$$

however, the reverse is not true in general.

Prop 9.10 Let $n = p \cdot q$ ($p \neq q$ prime), $a \in \mathbb{Z}_n$ with $\left(\frac{a}{n}\right) = 1$

Then a QR mod $n \iff \left(\frac{a}{p}\right) = 1$

Proof "$\Rightarrow$" a QR mod $n \overset{\text{Prop 9.7}}{\Rightarrow} a$ QR mod p and a QR mod q

$\overset{\text{D 9.8}}{\Rightarrow} \left(\frac{a}{p}\right) = 1$ (and $\left(\frac{a}{q}\right) = 1$)

"$\Leftarrow$" $\left(\frac{a}{p}\right) = 1 \Rightarrow a$ QR mod p. Suppose a not QR mod q,

Then $\left(\frac{a}{n}\right) = \underbrace{\left(\frac{a}{p}\right)}_{=1} \cdot \left(\frac{a}{q}\right) \neq 1$ ↯

Hence, a QR mod $q \overset{\text{P 9.7}}{\Rightarrow} a$ QR mod n

The subsequent probabilistic PK systems (Goldwasser-Micali and Blum-Goldwasser) rely on the intractability of the so-called quadratic residuosity problem (QRP).

On the tractability of deciding whether a is QR mod n:

Let $n = p \cdot q$, $p \neq q$, $a \in \mathbb{Z}_n$ with $\left(\frac{a}{n}\right) = 1$ (Otherwise a is a quadratic non-residue mod n)

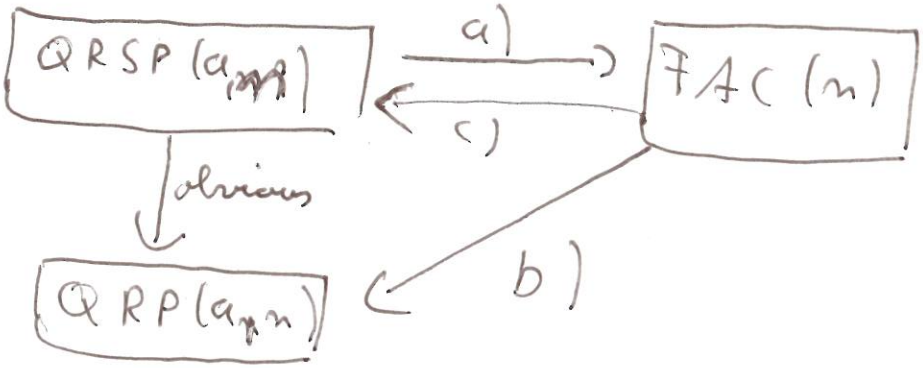
QRP (a, n): Decide whether or not a is a QR mod n

QRSP (a, n): Decide if a is a QR mod n and compute the square roots, i.e., x with $x^2 \equiv a \pmod{n}$

FAC (n): Factoring n

The following relations hold

P1 $\longrightarrow$ P2 means: If there exists an eff. alg to solve P1, then there is a ~~sufficient~~ efficient alg for solving P2. P2 may be reduced to P1.



a) $a \equiv x^2 \equiv y^2 \pmod n$, $x \neq \pm y \pmod n \Rightarrow \gcd(x-y, n) \in \{p, q\}$

b) $\left(\frac{a}{n}\right) = 1$, as p is known calculate $\left(\frac{a}{p}\right)$ see Prop 9.10

c) p, q known. If $p, q \equiv 3 \pmod 4$, see Prop 9.3, otherwise there $\exists$ a prob alg. for solving $x^2 \equiv a \pmod p$ [and $\pmod q$].

Remark 9.11 a) There is no known efficient alg for solving QRP(a, n)

b) (common belief: QPP(a, n) is no easier than factoring, i.e., QRP(a, n) $\longleftrightarrow$ FAC(n)

Deterministic PK schemes have the following drawbacks

- A particular plaintext m is always encrypted to same ciphertext. It is easy to detect if the same message is sent twice.
- It is sometimes easy to compute partial information. For example, in RSA $c = m^e \bmod n$. It holds

$$\left(\frac{c}{n}\right) = \left(\frac{m^e}{n}\right) \overset{\text{Rem 9.9 a)}}{=} \left(\frac{m}{n}\right)^e \overset{\text{because } e \text{ is odd}}{=} \left(\frac{m}{n}\right)$$

To avoid such information leakage probabilistic PK encryption is utilized.

9.4.1 The Goldwasser-Micali Cryptosystem (1984)

- Key generation

(i) Choose large primes $p \neq q$, $n = p \cdot q$

(ii) Choose $y \in \mathbb{Z}_n$, with a quadratic non-residue (QNR) mod n and $\left(\frac{y}{n}\right) = 1$ (such y is called pseudo square)

(iii) Public key (n, y) private key p, q

- Encryption (with the public key (n, y))

Message $m = (m_1, \dots, m_t) \in \{0,1\}^t$ (Bitstring)

Choose stoch. indep. random numbers $x_1, \dots, x_t \in \mathbb{Z}_n^*$

Let $c_i = \begin{cases} y \cdot x_i^2 \bmod n, & \text{if } m_i = 1 \\ x_i^2 \bmod n, & \text{if } m_i = 0 \end{cases}$ $\quad i = 1, \dots, t$

Cryptotext: $c = (c_1, \dots, c_t)$

- Decryption (with the private key (p, q))

Let $m_i = \begin{cases} 0, & \text{if } \left(\frac{c_i}{p}\right) = 1 \\ 1, & \text{otherwise} \end{cases}$ $\quad i = 1, \dots, t$

Prop 9.12 The decryption above is correct

Proof: (i) $m_i = 0 \Rightarrow c_i = x_i^2 \bmod n$, c_i QR mod n

$\overset{\text{Prop 9.7}}{\Rightarrow}$ c_i QR mod p $\Rightarrow$ $\left(\frac{c_i}{p}\right) = 1$

(ii) $m_i = 1 \Rightarrow c_i = y x_i^2 \bmod n$

c_i is pseudo square mod n since

$$\left(\frac{c_i}{n}\right) \overset{\text{Rem 9.9}}{=} \underbrace{\left(\frac{y}{n}\right)}_{=1} \left(\frac{x_i^2}{n}\right) = \left(\frac{x_i^2}{p}\right)\left(\frac{x_i^2}{q}\right) = 1$$

• Suppose $\exists\, v : v^2 \equiv \gamma \cdot x_i^2 \pmod n$

$\Rightarrow \gamma \equiv v^2 \left((x_i)^2\right)^{-1} \equiv \left(v x_i^{-1}\right)^2 \bmod n$

$\Rightarrow \gamma$ QR mod n ↯

Hence: c_i QNR mod and $\left(\frac{c_i}{n}\right) = 1$

Prop 9.10 $\Rightarrow \left(\frac{c_i}{p}\right) \neq 1$

Determining pseudosquares

Prop 9.13 | Let $p > 2$, prime, g a PE mod p (a generator of $\mathbb{Z}_p^*$)

Then: a QR mod $p \Leftrightarrow a = g^i \bmod p$ for some even integer i

Proof: Ex

Hence, half ~~of~~ of the elements in $\mathbb{Z}_p^*$ are QR and the other half are QNR mod p.

Alg for finding QNR γ with $\left(\frac{\gamma}{n}\right) = 1$ (γ a pseudo square)

1. Choose $a \in \mathbb{Z}_p^*$, a QNR mod p
   Choose $b \in \mathbb{Z}_q^*$, b QNR mod q

   By: Choose a (b) at random until $\left(\frac{a}{p}\right) = -1$ ($\left(\frac{b}{q}\right) = -1$)

   Success probability is $\frac{1}{2}$ in each trial

2. Compute $\gamma \in \{0, \dots, n-1\} = \mathbb{Z}_n$ with

   $\gamma \equiv a \pmod p$

   $\gamma \equiv b \pmod q$

   by the CRT. It follows

   γ QNR mod $p \overset{\text{Prop 9.7}}{\Rightarrow} \gamma$ QNR mod n

   $\left(\frac{\gamma}{n}\right) = \left(\frac{\gamma}{p}\right) \cdot \left(\frac{\gamma}{q}\right) = (-1)(-1) = 1$

   Hence γ is a pseudo square.