The lecture and exercise on AMC on 14th of December is cancelled.

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

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

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

Def 9.8 Let $p > 2$ be prime, $a \in \mathbb{N}$. The <u>Legendre symbol</u> 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 <u>Jacobi symbol</u> 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 alg. for computing $\left(\frac{a}{n}\right)$ with run time $O(\ln(n)^2)$ (see MOV p. 73) without factoring!

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

a 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 $\Leftrightarrow$ $\left(\frac{a}{p}\right) = 1$

Proof: „$\Rightarrow$" a QR mod n $\overset{\text{Prop 9.7}}{\Longleftrightarrow}$ 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 is not a QR mod q.
Then $\left(\frac{a}{n}\right) = \underbrace{\left(\frac{a}{p}\right)}_{=1}\left(\frac{a}{q}\right) \neq 1$ ↯

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

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

On the tractability of deciding whether a is QR mod n:
Let $n = p \cdot q$, $p \neq q$ prime, $a \in \mathbb{Z}_n$ with $\left(\frac{a}{n}\right) = 1$
(Otherwise a is a quadratic non residue mod n, cf. Prop 9.10)

QRP(a, n) : Decide whether or not a is a QR mod n
QRSP(a, n) : Decide if a is a QR mod n <u>and</u> compute the square roots, i.e., x with $x^2 \equiv a \pmod{n}$
FAC(n) : Factoring n

$\boxed{P1} \longrightarrow \boxed{P2}$ means: If there exists an efficient alg. to solve P1 then there is an efficient alg. to solve P2.
P2 may be reduced to P1.

$$\begin{tikzcd}
\boxed{QRSP(a,n)} \arrow[r, shift left, "a)"] \arrow[d, "\text{obvious}"] & \boxed{FAC(n)} \arrow[l, shift left, "c)"] \arrow[dl, "b)"] \\
\boxed{QRP(a,n)} &
\end{tikzcd}$$

General. of Prop. 8.3

a) $a \equiv x^2 \equiv y^2 \pmod{n}$, $x \not\equiv \pm y \pmod{n} \Rightarrow \gcd(x-y, n) \in \{p, q\}$

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

c) p, q are known. If $p, q \equiv 3 \pmod{4}$, see Prop 9.3 / Prop 9.4), otherwise there exists a probabilistic alg. for solving $x^2 \equiv a \pmod{p, q}$

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

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

Deterministic PK schemes have the following drawbacks.

- A particular plain text m is always encrypted with the 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

$$\left(\frac{c}{n}\right) = \left(\frac{m^e}{n}\right) \underset{\substack{\uparrow \\ \text{Remark 9.9 a)}}}{=} \left(\frac{m}{n}\right)^e = \left(\frac{m}{n}\right), \text{ because } e \text{ is odd}$$

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 <u>quadratic non-residue</u> (QNR) mod n and $\left(\frac{y}{n}\right) = 1$ (such y is called <u>pseudo-square</u>)

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

- Encryption

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

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

- Decryption

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

<u>Prop 9.12</u> | The decryption above is valid

<u>Proof</u>: (i) $m_i = 0 \Rightarrow c_i = x_i^2 \mod n$, c_i is QR mod n

$\overset{\text{Prop 9.7}}{\Rightarrow} c_i$ QR mod $p \Rightarrow \left(\frac{c_i}{p}\right) = 1 \Rightarrow m_i = 0$

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

c_i is pseudo square mod n, since

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

Suppose c_i is QR mod n $\Rightarrow \exists\, v : v^2 \equiv y \cdot t_i^2 \pmod n$

$\Rightarrow y \equiv v^2 (t_i^2)^{-1} \equiv \left(v \cdot (t_i)^{-1}\right)^2 \pmod n$

$\Rightarrow y$ QR mod n $\lightning$

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

$\overset{\text{Prop 9.10}}{\Rightarrow}$ $\left(\frac{c_i}{p}\right) \not\equiv 1 \Rightarrow m_i = 1$ is decrypted

<u>Determining pseudosquares</u>

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

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

<u>Proof</u>: Ex

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

Alg. for finding QNR y with $\left(\frac{y}{n}\right) = 1$ (y is 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 (or b) at random until $\left(\frac{a}{p}\right) = -1$ $\left(\left(\frac{b}{q}\right) = -1\right)$

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

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

$y \equiv a \pmod p$

$y \equiv b \pmod q$

by the CRT. It follows

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

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

Hence y is a pseudo square.

Security of the GM Cryptosystem

An opponent intercepts $c_i = \begin{cases} y \cdot t_i^2 \bmod n & , \text{if } m_i = 1 \\ t_i^2 \bmod n & , \text{if } m_i = 0 \end{cases}$

hence, a random QR or pseudosquare mod n

To decide whether $m_i = 0$ or 1, Oscar needs to solve $QRP(c_i, n)$. If QRP is computational infeasible, then O cannot do better than guessing m_i

Remark 9.14

A major drawback of the GM cryptosystem is the message expansion by a factor of $\log_2(n)$ bits. To assure security we should have 1024 bits.