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

\[ a \equiv a \mod m \Rightarrow a \equiv a \mod p \text{ and } a \equiv a \mod q. \]

Proof

\[ a \equiv a \mod m \Rightarrow x^2 \equiv a \mod m \Rightarrow x^2 \equiv a \mod p \text{ and } x^2 \equiv a \mod q. \]

\[ x^2 \equiv a \mod p \Rightarrow x \equiv \pm \sqrt{a} \mod p \]

\[ x^2 \equiv a \mod q \Rightarrow x \equiv \pm \sqrt{a} \mod q. \]

\[ x \equiv \pm \sqrt{a} \mod m \Rightarrow \sqrt{a} \mod m \]

\[ \sqrt{a} = \sqrt{a} \mod m \]

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

\[ \left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{if } a \equiv 0 \mod p \\
1 & \text{if } a \equiv a \mod p \\
-1 & \text{otherwise}
\end{cases} \]

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

\[ \left( \frac{a}{m} \right) = \prod_i \left( \frac{a}{p_i} \right)^{k_i}. \]

Remark 9.9

a) For any odd \( n \in \mathbb{N} \):

\[ \left( \frac{ab}{m} \right) = \left( \frac{a}{m} \right) \left( \frac{b}{m} \right). \]

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

Unlike the Legendre symbol, the Jacobi symbol does not reveal whether \( a \equiv a \mod m \). It holds that

\[ a \equiv a \mod m \Rightarrow \left( \frac{a}{m} \right) = 1, \]

however, the reverse is not true in general.
Prop 9.10: Let \( n = p \cdot q \) and \( p \neq q \) prime, \( a \in \mathbb{Z}_n \) with \( (a/n) = 1 \).

Then, \( a \) is a QR mod \( n \) if and only if \( (a/p) = 1 \) and \( (a/q) = 1 \).

Proof:
\[
\left(\frac{a}{p}\right) = 1 \iff \text{a is a QR mod } p.
\]
Suppose \( a \) is not a QR mod \( q \).

Then, \( (a/m) = (a/p)(a/q) \neq 1 \)

\( \Rightarrow \left(\frac{a}{m}\right) \neq 1 \)

Hence, \( a \) is not a QR mod \( m \).

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

QRP \((a,m)\): Decide whether or not \( a \) is a QR mod \( m \).

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

FAC \((n)\): Factoring \( n \).

\([P1] \longrightarrow [P2]\) means: If there exists an efficient alg. to solve \( P1 \) then there is an efficient alg. to solve \( P2 \).

\( P2 \) may be reduced to \( P1 \).
\[\text{QRSP}(a, \alpha, n) \iff \text{FAC}(n)\]

\[\text{QRSP}(a, \alpha, n) \quad \text{obvious}\]

\[\text{QRSP}(a, \alpha, n) \quad \text{General of Prop 8.3}\]

\(a)\ a = x^2 \equiv -x^2 \pmod{n}\)

\(b)\ \left(\frac{a}{n}\right) = 1\), as \(p, q\) are known, calculate \(\left(\frac{a}{n}\right)\) 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 \(x^2 \equiv a \pmod{p, q}\)

\[\text{Remark 9.17}\]

\(a)\) There is no known efficient alg. for solving \(\text{QRSP}(a, \alpha, n)\)
(b) Common belief: \(\text{QRSP}(a, \alpha, n)\) is no harder than factoring, i.e.,
\[\text{QRSP}(a, \alpha, n) \rightarrow \text{FAC}(n)\]

Deterministic PK schemes have the following drawbacks:

- It is sometimes easy to compute partial information. For example in RSA: \(c = m^e \pmod{n}\). It holds
\[(\frac{c}{n}) = (\frac{m^e}{n}) = (\frac{m}{n})^e = (\frac{m}{n})\]

\[\text{Remark 9.9 a)}\]

To avoid such information leakage, probabilistic PK encryption is utilized.

- Key generation
  (i) Choose large primes $p, q$, $n = p \cdot q$
  (ii) Choose $y \in \mathbb{Z}_n$, with a quadratic non-residue (QNR) mod $n$ and $(\frac{y}{n}) = 1$ (such $y$ is called pseudo-square)
  (iii) Public key $(n, y)$, private key $(p, q)$

- Encryption
  Message $m = (m_1, ..., m_t) \in \mathbb{Z}_n^t$ (Bitstring)
  Choose $\delta_k$, independent random numbers $x_1, ..., x_t \in \mathbb{Z}_n$
  Let $c_i = \begin{cases} y \cdot x_i^2 \mod n & \text{if } m_i = 1 \\ x_i^2 \mod n & \text{if } m_i = 0 \end{cases}$

- Decryption
  Let $m'_i = \begin{cases} 0 & \text{if } (\frac{c_i}{p}) = 1 \\ 1 & \text{otherwise} \end{cases}$

Prop. 9.12! The decryption above is verified
Proof: (i) $m_i = 0 \Rightarrow c_i = x_i^2 \mod n$, $c_i$ is QNR mod $n$

Prop. 9.7 $c_i$ (QR mod $p$) = $(\frac{c_i}{p}) = 1$ $\Rightarrow$ $m_i = 0$
(ii) $m_i = 1 \Rightarrow c_i = y \cdot x_i^2 \mod n$

$c_i$ is pseudo-square mod $n$, since

$\left( \frac{c_i}{n} \right) = \left( \frac{y}{n} \right) \left( \frac{x_i^2}{n} \right) = \left( \frac{y}{p} \right) \left( \frac{x_i^2}{q} \right) = 1$

Rem. 9.8 $= 1$ Def. Jacobi symbol

-1-
Suppose \( c_i \equiv AR \mod p \Rightarrow \forall \epsilon_1 \in \mathbb{R} \cdot \epsilon_i^2 \mod n \)

\[
\Rightarrow y^2 \equiv \epsilon_i^2 \mod n \\
\Rightarrow y \equiv \epsilon_i \mod n
\]

Hence: \( c_i ' \equiv AR \mod p \) and \( \left( \frac{c_i '}{p} \right) = 1 \)

Prop 9.10: \( \left( \frac{c_i '}{p} \right) \neq 1 \Rightarrow m_i = 1 \text{ is decrypted} \)

Determining pseudo-squares: \( \quad \)

Prop 9.13: Let \( p \geq 2 \) be prime, \( g \equiv PG \mod p \) (a generator of \( \mathbb{Z}_p^* \))

Then: \( a \equiv AR \mod p \Rightarrow a = g^i \mod p \) for some even integer \( i \)

Proof: \( \quad \)

Hence, half of the elements in \( \mathbb{Z}_p^* \) are \( AR \) and the other half are \( QN \mod p \)

Alg. for finding \( QN \ mod \ y \) with \( \left( \frac{y}{p} \right) = 1 \) \( y \) as a pseudo square:

1. Choose \( a \in \mathbb{Z}_p^* \), \( a \equiv AR \mod p \)
2. Choose \( b \in \mathbb{Z}_q^* \), \( b \equiv QN \mod q \)

By choose \( a \) \( (a, b) \) 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 \( y \in \{0, 1, \ldots, 2^n - 1\} \) \( \mathbb{Z}_n \), with

\[
y \equiv a \mod p
\]

\[
y \equiv b \mod q
\]

by the CRT. It follows

\[
y \equiv \left( \frac{y}{p} \right) \cdot \left( \frac{y}{q} \right) \equiv (1) \cdot (-1) = -1
\]

Hence \( y \) is a pseudo square.
Security of the GM cryptosystem

An opponent intercepts $c_i = \left\{ \begin{array}{ll} Y \cdot t_i^1 \mod n & \text{if } m_i = 1 \\ t_i^2 \mod n & \text{if } m_i = 0 \end{array} \right.$

hence, a random QR or pseudosquare mod $n$.

To decide whether $m_i = 0$ or $1$, one needs to solve $QR P (t_i \mod n)$. If $QR P$ is computationally infeasible then $O$ cannot do better than guessing $m_i$.

Lemma 3.14

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