The Rabin Cryptosystem

Prop. 9.3. If $p \equiv 3 \pmod 4$, i.e., $p = 4k-1$, c QR mod p then

$x^2 \equiv c \pmod p$ has solution $x_{1,2} = \pm c^k \bmod p$. ┘

Th. 6.10. Chinese Remainder Theorem

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \dots, r$$

has a unique solution mod $M = \prod_{i=1}^{r} m_i$, namely

$$x = \sum_{i=1}^{r} a_i M_i y_i ,$$

$$M_i = M/m_i , \quad y_i = M_i^{-1} \pmod{m_i}$$ ┘

Rabin Cryptosystem

(i) $p \neq q$ prime, $p, q \equiv 3 \pmod 4$, $n = p \cdot q$

(ii) Public key: n, private key: (p, q)

(iii) Encryption: $c = m^2 \bmod n$

Decryption:

Solve $x^2 \equiv c \mod p$

$y^2 \equiv c \mod q$ by Prop. 9.3

Determine $f \equiv x \mod p$

$f \equiv y \mod q$

by Th. 6.10 (Chin. Remainder Theorem)

Then $$\left.\begin{array}{l} f^2 \equiv x^2 \equiv c \pmod p \\ f^2 \equiv y^2 \equiv c \pmod q \end{array}\right\} \overset{\text{Prop. 8.1}}{\Longrightarrow} f^2 \equiv c \pmod n$$

There are 4 solutions f, one is the message m.

<u>Remarks 9.6.</u> (Security)

a) From Prop. 8.3: Breaking the Rabin system is equivalent to factoring.

b) The Rabin system is vulnerable against chosen-ciphertext attack.

- O/E chooses m at random, computes $c = m^2 \bmod n$
- c is deciphered with plaintext m'.
- With prob. $\frac{1}{2}$: $m' \not\equiv \pm m$. In this case compute $\gcd(m-m', n) \in \{p, q\}$. (*)
  Otherwise, repeat the above.

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

Since $n \mid x^2 - y^2 \Rightarrow n \mid (x-y)(x+y)$ but $n \nmid (x-y)$
$n \nmid (x+y)$ ∎

Hence, never publish a deciphered message which is not the right one.

c) Broadcasting endangers Rabin system

The same message m is sent to K receivers $1, \ldots, K$, encrypted with public keys $n_1, \ldots, n_K$.

$$c_1 = m^2 \bmod n_1$$
$$\vdots$$
$$c_K = m^2 \bmod n_K$$

O/E eavesdrop the channel and solves

$$x \equiv c_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv c_K \pmod{n_K}$$

The CRT yields a solution

$$x \equiv m^2 \pmod{n_1 \cdots n_K}$$

Since $m < n_i \ \forall i = 1, \ldots, K$, it follows $m^2 < n_1 \cdots n_K$.

Hence $x = m^2$, m may be computed as the real square root.

This attack also applies to RSA with small $e = d^{-1} \bmod \varphi(n)$.

11. Signature Schemes

"digital signature"

Requirements (same as on conventional signatures)

- verifiable (proof of ownership)
- forgery-proof
- firmly connected to the document

Problem for certain applications: repeated use.
(→ use of time stamps)

Attacks on signature schemes:

- Key-only attack
- Known message attack
- Chosen-message attack
  - non-adaptive (message before the sign. is seen)
  - adaptive (message may depend on previous sign.)

Results of attacks:

- Total break: O/E can sign any message
- Selective forgery: O/E can sign a certain class of messages
- Existential forgery: O/E can sign at least one message.

For signature schemes "hash functions" are needed.
Hash functions are denoted by

$$h : \mathcal{M} \to \{0,1\}^K$$

8.1.3. The RSA Signature Scheme

(approved by NIST since Dec. 1998)

A uses $\underbrace{\text{public}}_{\text{key}}$ $(d_A^{-1} = e_A, n_A)$

private key d_A

Signature generation on message m.

$$s = (h(m))^{d_A} \bmod n_A \quad \text{(using A's private key)}$$

s : signature on m.

Verification of s by B.

$$g = s^{e_A} \bmod n_A \qquad \text{(using A's public key)}$$

If $h(m) = g$ B accepts A's signature.

By Prop. 6.2: If s is a valid signature on m,
then $g = h(m)$.

RWTH AACHEN UNIVERSITY

Security:

a) B cannot change m to $\hat{m}$,
otherwise $h(\hat{m}) \neq s^{e_A} \bmod n_A$.
B cannot generate a valid signature on some message $\hat{m}$, since d_A is private.

b) A "random" message by its hash can be generated as
$$h = s^{e_A} \bmod n_A$$
with valid signature s, since
$h^{d_A} \equiv s \pmod{n_A}$.
h will be meaningless with high probability.

11.1. El Gamal signature scheme

Parameters: p : prime, a : PE mod p, h : hash fct.
Select random x, $y = a^x \bmod p$.
Public key: (p, a, y), private key: x

Thinking the Future
Zukunft denken

Signature generation:

Select random k s.t. $k^{-1} \bmod (p-1)$ exists.

$$r = a^k \bmod p$$

$$s = k^{-1}(h(m) - xr) \bmod (p-1)$$

Signature for m: (r,s)

Verification:

Verify $1 \leq r \leq p-1$

$$v_1 = y^r r^s \bmod p$$

$$v_2 = a^{h(m)} \bmod p$$

$v_1 = v_2 \longrightarrow$ accept the signature.

Verification works:

$$ks \equiv h(m) - xr \pmod{(p-1)}$$

$$\Leftrightarrow h(m) \equiv xr + ks \pmod{(p-1)}$$

$$\Leftrightarrow xr + ks = \ell(p-1) + h(m) \text{ for some } \ell \in \mathbb{Z}.$$

$$y^r r^s \equiv a^{xr} a^{ks} \equiv a^{xr+ks}$$

$$\equiv a^{\ell(p-1)} a^{h(m)}$$

$$\equiv \underbrace{(a^{p-1})^{\ell}}_{\equiv 1 \pmod p \text{ (Fermat)}} a^{h(m)} \equiv a^{h(m)} \pmod p$$