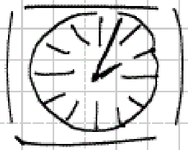
Public-Key Cryptography -L2- 21.10.2009

Notiztitel 15.10.2009

Previously: **Power of quantum computers I**

- Motivation for public-key cryptography
- Quantum computation
- Shor's algorithm



Exercise : 23.10. $9^{\underline{50}}$

Exam : 24.02. $10^{\underline{00}}$

Today: **Power of QC II / Hash-based signatures I**

- Shor's algorithm (cont'd)
- Hash-based one-time signatures

$\boxed{\text{Shor's algorithm classical part}}$ 1^{st} Version 1994 last Version 1996

Input: $n \in \mathbb{N}$ composite

1. Pick $x \in \{2, \dots, n-1\}$ uniformly at random
2. If $\gcd(x, n) \neq 1$: Return $\gcd(x, n)$
3. Find period r of $f(a) = x^a \bmod n$ (quantum part)
4. If r is odd or $\boxed{x^{r/2} \equiv -1 \pmod n}$: Goto 1

   New
5. Return $\gcd(x^{r/2} \pm 1, n)$

Exercise: What is the probability of reaching 5 from 4?

For RSA $\geq 50\%$

$\boxed{\text{Shor's algorithm correctness}}$

Know: (i) r even and (ii) $x^{r/2} \not\equiv -1 \pmod{n}$

$$0 \equiv x^r - 1 \overset{(i)}{\equiv} \underbrace{(x^{r/2}+1)}_{\not\equiv 0 \text{ by (ii)}} \underbrace{(x^{r/2}-1)}_{\not\equiv 0 \text{ since } r \text{ is order of } x} \pmod{n}$$

Let p prime be divisor of n

$$0 \equiv (x^{r/2}+1)\ (x^{r/2}-1) \pmod{p}$$

Now one <u>has</u> to be zero since $\mathbb{Z}_p$ is a field.

Quiz: Which values can $\gcd(a,n)$ take for $n=pq$ and $a \in \mathbb{N}$?

$\gcd(a,n) \in \{1, p, q, n\}$

Assume it's the first factor then $\gcd(x^{r/2}+1, n) = p$.

Shor's algorithm quantum part

Input: x, n from classical part

STATE

1. Set $q = 2^k$, s.t. $n^2 < q < 2n^2$

2. Initialize QR to $\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle$

3. Compute f in 2^{nd} register $\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a \bmod n\rangle$

4. Fourier-Transform 1^{st} reg. q^{th} root of unity $\omega := \exp(2\pi i/q)$

$$|a\rangle \longmapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \omega^{ac} |c\rangle \qquad \frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \omega^{ac} |c\rangle |x^a \bmod n\rangle$$

5. Observe both registers

(6.) Try to compute r from c/q using continued fractions.
(classical again)

How often do I need to run this?

$\Pr[\text{Observing } |c\rangle|x^k \bmod n\rangle] = \left|\frac{1}{q}\sum_{a:\, x^k \equiv x^a \bmod n} \omega^{ac}\right|^2$

$\Pr\left[(1) \quad \exists d \in \mathbb{Z},\ \left|c/q - d/r\right| < \frac{1}{2q} \text{ and } \ldots\right] \geq \frac{1}{3r^2}$

Under condition (1):

- Since $q > n^2$, there is at most one fraction $\frac{d}{r}$ with $r < n$. (Exercise)
  This can be found efficiently from known c/q using continued fractions.
- If d and r are coprime, r is the denominator of the fraction.
  So in this case using continued fractions directly yields r, otherwise not!

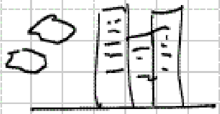
How many favorable states are there?

- There are $\varphi(r)$ working d, each fraction d/r is close to one c/q (1st reg)
- There are also r distinct values of x^k (2nd reg)

$\Rightarrow$ Chance of success $= r\varphi(r)/(3r^2) > \text{const.}/\log\log r$

Digital Signatures

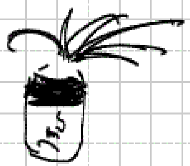
(ANTI-VIR) COMPANY



program
$pk_{COMPANY}$ →

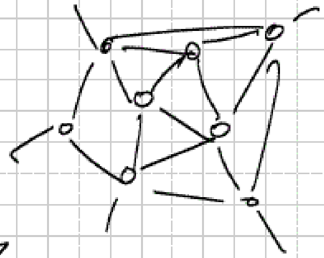
real update
real signature →

EVIL HACKER



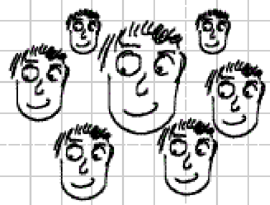
fake update
fake signature →

THE WEB



update
signature →

10^6 USERS
(OF ANTI-VIR)



genuine?

check VER($\boxed{pk_{COMPANY}}$,
update,
signature)

Quiz: What's missing?

You know authenticity and integrity

Lamport and Diffie (1979) one-time signature

Let $n > 0$, $f: \{0,1\}^n \to \{0,1\}^n$ one way.

KEY GEN:

$X \xleftarrow{\$} \left(\{0,1\}^n\right)^{2 \times n}$ random

$$\begin{array}{cccc} & 1 & 1 & 0 \\ & 0 & 1 & 0 \\ X = & \left(\begin{array}{c} 001 \\ 110 \end{array}\right. & \begin{array}{c} 100 \\ 110 \end{array} & \left.\begin{array}{c} 000 \\ 101 \end{array}\right) \end{array} = \text{secret key}$$

$Y \in \left(\{0,1\}^n\right)^{2 \times n}$, $y_{ij} = f(x_{ij})$

$$Y = \begin{pmatrix} f(001) & f(100) & f(000) \\ f(110) & f(110) & f(101) \end{pmatrix} = \text{public key}$$

SIGN:

Message $m \in \{0,1\}^n$

$m = (0\,1\,0)$ $\quad s = (001 \;\; 110 \;\; 000)$

Quiz: VER?

Signature $s = (x_{m_0,0}, x_{m_1,1}, \ldots, x_{m_{n-1},n-1})$

VER:

Check $y_{m_i,i} \stackrel{?}{=} f(x_{m_i,i})$ for all $0 \le i < n$

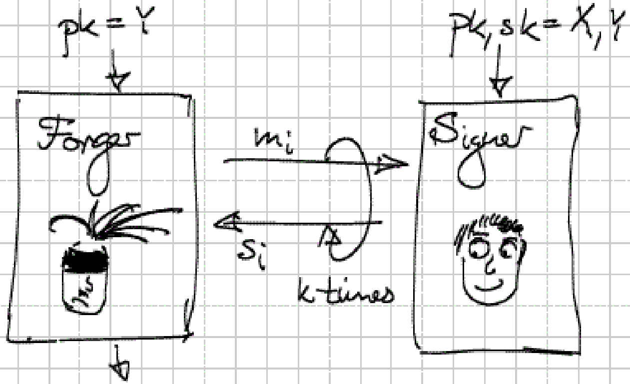
Keysize $(n = 256)$ $\quad pk, sk = 2n^2$ Bit (16 KByte) Exercise

$Sig = n^2$ Bit (8 KByte)

Security of LD-OTS

Model: Existentially unforgeable under adaptive chosen message attacks (EU-CMA)

$(pk, sk) = KEY(1^n)$



$m_{k+1} \neq m_i$ for all $i = 1, \ldots, k$

For one-time signatures $k = 1$.

Security

Given a signing oracle S', a forger may

- see $pk = Y = \begin{pmatrix} f(x_{0,0}) & \cdots & \\ f(x_{1,0}) & \cdots & \end{pmatrix}$
- choose some message m
- get $s = S'(m)$

and must produce $m' \neq m$ which verifies correctly.

Let messages differ in i^{th} bit, then the attacker must have inverted f! Quiz: For which image of f?

Say $m_i = 0$, $X = \begin{pmatrix} x_{0,0} & \cdots & \overset{\text{known} = s_i}{x_{m_i,i}} & \cdots & x_{0,n-1} \\ x_{1,0} & \cdots & \underset{\text{unknown} = s_i'}{x_{m_i',i}} & \cdots & x_{1,n-1} \end{pmatrix}$ preimage of $y_{m_i',i}$

$\boxed{\text{Why one time?}}$

$$Y = \begin{pmatrix} 010 & 110 & 001 \\ 101 & 001 & 010 \end{pmatrix}$$

$m_1 = 101$

$S_1 = (111 \quad 101 \quad 100)$

$m_3 = 101$

$m_2 = 011$

$S_2 = (010 \quad 110 \quad 100)$

$m_4 = 001$

$S_4 = (010 \quad 101 \quad 100)$

Quiz: For which message can we forge a signature?

$m_3 = 111$

$S_3 = (111 \quad 110 \quad 100)$

Quiz: Can we forge if m_1 and m_2 differ in only <u>one bit</u>?

Advertisement

All practical signature schemes

- Use cryptographic hash function $h: \{0,1\}^* \to \{0,1\}^n$ on data before signing (need collision-resistance)
- Generate keys from secure randomness.

All <u>non hash-based</u> schemes have more (unnecessary?) security assumptions. Quiz: Give an example!

Thank you

Questions?