10/12/10 QIC 710 Lecture 9: Factoring algorithm, Hidden subgroup problem

Last time: Phase estimation, Discrete Log

Phase estimation error analysis

Traditional symmetric-key crypto.: 0. Alice and Bob share key k
1. Encryption/decryption by $\sigma_k(m)$, σ_k^{-1} secret key SK_A

Public-key cryptography: 0. Alice generates public key PK_A.
1. Alice publishes "Alice, PK_{Alice}, signature"
2. Charlie sends $E_{PK_A}(m)$ to Alice
3. Alice decrypts $D_{SK_A} E_{PK_A}(m) = m$.

Anybody can send a message to Alice, but only Alice can read them.

Necessary condition: one-way functions: easy to apply but hard to invert.

some number theory...

RSA '78 (sketch)

0. secret key: primes p, q
   public key $n = p \cdot q$, $e = 3$
1. encryption $m \bmod n \longmapsto m^e \bmod n$
2. decryption: let $d = e^{-1} \bmod \phi(n)$
   $(m^e)^d = m^{de} = m^{k\phi(n)+1} = m \bmod n$

Best classical algorithm:
Number Field sieve $e^{\sim \sqrt[3]{\log N (\log\log N)^2}}$ time & space
record 768 bits (232 digits) 2009, 3300 1GHz CPU years

Quantum algorithm for Period Finding

Given: $f: \{0,1,\dots,M-1\} \to \{0,\dots,M-1\}$

promise $\exists a \mid M$ s.t. $f(x) = f(x+a \bmod M)$ $\forall x$

and $f(x) \neq f(y)$ if $y - x \neq 0 \bmod a$.

Goal: Find a. (Compare to Simon's problem)

Solution: $0 \xrightarrow{F_M} \sum_{x\in[M]} |x\rangle$

$\xrightarrow{U_f} \sum_x |x\rangle|f(x)\rangle$

measure 2nd register $\sum_{l=0}^{M/a-1} |y + l\cdot a\rangle$ for a uniformly random y (unknown)

$\xrightarrow{F_M} \sum_{x\in[M]} \sum_{l=1}^{M/a} \omega_M^{x\cdot(y+la)} |x\rangle = \sum_{x\in[M]} \omega^{xy} \left(\sum_{l\in[M/a]} \omega_{M/a}^{x\cdot l}\right)|x\rangle$

$= 0$ unless $x = 0 \bmod M/a$

measure $\frac{M}{a}\cdot k$ for a uniformly random $k \in [a]$

Now $\gcd\left(\frac{M}{a}\cdot k, M\right) = \frac{M}{a}\cdot\gcd(k,a)$

$=1$ with probability $\frac{\phi(a)}{a} \geq \frac{1}{\log a} \geq \frac{1}{\log M}$.

Number Theory aside: Euler's phi function (totient function)

$\phi(n) = |\{m : 1 \leq m \leq n, \gcd(m,n) = 1\}|$

$\phi(p) = p-1$, $\phi(p\cdot q) = (p-1)(q-1)$

$\phi(p_1^{n_1}\cdots p_k^{n_k}) = \prod_{j=1}^{k} (p_j - 1) p_j^{n_j - 1}$

$\frac{\phi(n)}{n} = \Omega\left(\frac{1}{\log n}\right)$

Euler's Thm: If $\gcd(a,n) = 1$ then $a^{\phi(n)} = 1 \bmod n$.

(since $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$ is a multiplicative group of order $\phi(n)$)

Order Finding

Given c, N coprime ($\gcd(c,N) = 1$)

Find order(c) = smallest r such that $c^r = 1 \bmod N$.

Since $c^{\phi(N)} = 1 \bmod N$ (Euler-Fermat), order(c) $\mid \phi(n)$.

Algorithm: Let $f(x) = c^x \bmod N$, a function with period order(c).

Now apply Period Finding algorithm.

Problems: 1. Implementing f (easy).

2. Need $QFT_{\phi(N)}$ but $\phi(N)$ need not be a power of 2, & unknown, finding $\phi(N)$ as difficult as factoring

Factoring reduced to order finding

Let $N = p \cdot q$, with p, q prime (for simplicity only)

Algorithm:

1. Pick $a \in_R \{1, 2, \ldots, N-1\}$.
   w.h.p. $\gcd(a, N) = 1$. (otherwise, done!)
2. Let $r = \text{order}(a)$
3. If r is even, then have
   $$a^r - 1 = 0 \mod N$$
   $$(a^{r/2} - 1)(a^{r/2} + 1) = 0 \mod N$$
4. If $a^{r/2} + 1 \neq 0 \mod N$ then
   $\gcd(a^{r/2} + 1, N)$, $\gcd(a^{r/2} - 1, N)$ are nontrivial factors
   ($\neq 0 \mod N$)

e.g. $N = 15 = 3 \cdot 5$
$a = 4$, $r = 2$
$a^{r/2} + 1 = 5$
$\gcd(5, 15) = 5$ ✓

Theorem: For a random x,
$$\mathbb{P}[r = \text{order}(x) \text{ is even, and } x^{r/2} \neq -1 \mod N] \geq \frac{1}{4}.$$
Thus the algorithm succeeds with probability $\geq \frac{1}{4}$.

Proof.

Theorem (Chinese Remainder Theorem):
Let $N = p \cdot q$ for primes p and q, $p \neq q$.
Then $\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$
(recall: $\mathbb{Z}_n^* \doteq (\{x : \gcd(x, n) = 1\}, \text{multiplication})$.)

Proof: Explicit multiplicative homomorphisms in both directions are
$$x \in \mathbb{Z}_N^* \longmapsto (x \bmod p, x \bmod q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$
$$(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^* \longmapsto a \cdot q \cdot (q^{-1} \bmod p) + b \cdot p \cdot (p^{-1} \bmod q).$$ □

Thus picking x u.a.r. from $\mathbb{Z}_N^*$ is equiv. to picking a and b independently and u.a.r. from $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$.

$r = \text{order}(x) = \text{least-common-multiple}(\text{order}_p(a), \text{order}_q(b))$

Claim: $\mathbb{P}[\text{order}_p(a) \text{ even}] = \mathbb{P}[\text{order}_q(b) \text{ even}] = \frac{1}{2}$.

Pf: $\mathbb{Z}_p^*$ is cyclic of order $p-1$. Thus $a = g^m$ for a generator g and $m \in_R \{0, 1, \ldots, p-2\}$ (odd if p is odd) □

Thus $\mathbb{P}[\text{one of } \text{order}_p(a), \text{order}_q(b) \text{ even, the other odd}] = \frac{1}{2}$.

$\Rightarrow r$ is even $\Rightarrow x^{r/2} = (a^{r/2}, b^{r/2}) \in \{(1,1), (-1,-1), (1,-1), (-1,1)\}$

if $\text{order}_q(b)$ odd, then $r = 2 \cdot \text{order}_q(b) \cdot \text{integer}$, so $\frac{r}{2}$ is a multiple of $\text{order}_q(b)$ ✓ $(-1,1)$

✓ □