§ 8.1 RSA

Designers: Ron Rivest, Adi Shamir, and Leonard Adleman, 1977.

Basic assumption. Factorization of $N = pq$ for two prime numbers p and q are hard to do.

Public key crypto-system. Alice(the bank, VISA card co.) can announce a public key for customers (Bob) to encrypt their message and send it to Alice via a public channel, and Alice can easily decrypt the message.

Step 1 Alice: Let $N = pq$, and let $e < N$ be relatively prime to $(p-1)(q-1)$. Here e is known as the exponent, and release N and e. Then compute the modular inverse d of e and keeps d secret.

In group/number theory, we know that this is the group of units in $\mathbb{Z}_N$.

Step 2 Bob: To send Alice a message represented as a number m to Alice, encode the message m by m^e and send it through an open/public channel.

Step 3 Alice: Decode the message by applying $(m^e)^d = m \pmod N$.

[Here one can show that $m^r = m \pmod p$ and $m^r = m \pmod q$ so that $m^r = m (\mathrm{mod}\ N)$.]

Example 1. Let $(p, q) = (61, 53)$ and $N = 3233$.

2. The groups of units has $(p-1)(q-1) = 780$ elements.
3. For instance $e = 17$ is a unit, and $r = 413$ satisfies $er \equiv 1 \pmod N$.
4. Public key $(N, e) = (3233, 17)$.
5. Bob sends a number (message) m as $c(m) = m^e \pmod{3233}$ with $c(m) < 3233$.
6. Alice decrypts $c(m)$ as $m = c(m)^r \pmod{3233}$.

For instance if $m = 65$, then $c = 65^{17} = 2790((\mathrm{mod}\ 3233)$.
Then Alice computes $2790^{413} = 65((\mathrm{mod}\ 3233)$.

§ 8.2 Factorization Algorithm

Step 1 Let N be given. Take a random $m < N$ and compute $\gcd(m, N) = g$ by the Euclidean Algorithm. If $g > 1$, we are extremely lucky. If not, go to Step 2.

Step 2 (Quantum part) Define $f_N : \mathbb{N} \to \mathbb{N}$ by $a = m^a \pmod{N}$. Find the smallest P such that $m^P = 1 \pmod{N}$. (That is, finding the order/period of m in U_N^*.)

Step 3 If P is odd, it cannot be used. Go back to Step 1. Else, go to Step 4.

Step 4 If P is even, then $(m^{P/2} - 1)(m^{P/2} + 1) = m^P - 1 = 0 \pmod{N}$.
If $m^{P/2} + 1 = 0 \pmod{N}$, then $\gcd(m^{P/2} - 1, N) = 1$; go back to Step 1.
If $m^{P/2} + 1 \neq 0 \pmod{N}$, then $m^{P/2} - 1$ has a prime factor of N. [Note that $m^{P/2} \neq 1 \pmod{N}$ as P is the order of m.] Proceed to Step 5.

Step 5 Compute $d = \gcd(m^{P/2} - 1, N)$, which will be p or q.

Example Let $N = 799$.

Step 1. Choose $m = 7$.

Step 2. We find (by quantum computer or conventional computer) that $P = 368$ is the smallest positive number such that $7^P = 1$ ((mod 799)).

Step 3. Set $P/2 = 184$. Then $(7^{184} - 1)(7^{184} + 1) = 0 \pmod{799}$.

Step 4. Now, $\gcd(7^{184} + 1, 799) = 17 \neq 1$. So, we are good and done, namely, $799 = 17 \cdot 47$. [In fact, $\gcd(7^{184} - 1, 799) = 47$.]

§ 8.3 - 8.5 Shor's Algorithm

Designer: Peter Shor (1994).

Complexity: The time taken is polynomial in $\log N$, which is the size of the input).[1] Specifically it takes quantum gates of order $O((logN)2(loglogN)(logloglogN))$ using fast multiplication.

- In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3×5, using an NMR implementation of a quantum computer with 7 qubits.
- After IBM's implementation, two independent groups implemented Shor's algorithm using photonic qubits, emphasizing that multi-qubit entanglement was observed when running the Shor's algorithm circuits.
- In 2012, the factorization of 15 was performed with solid-state qubits. Also in 2012, the factorization of 21 was achieved, setting the record for the largest number factored with Shor's algorithm.
- In April 2012, the factorization of $143 (= 11 \times 13)$ was achieved, although this used **adiabatic quantum computation** rather than Shor's algorithm.
- In November 2014, it was discovered that this 2012 adiabatic quantum computation had also factored larger numbers, the largest being $56153 = 233 \times 241$.

Let $N = pq$, and choose n so that $N^2 \le 2^n < 2N^2$ so that $S_n = \{0, \ldots, Q-1\}$ with $Q = 2^n$. Define $f : S_n \to \mathbb{Z}/N\mathbb{Z}$ by $f(a) = m^a \pmod N$. Apply the following.

Step 2.0 Set up $|\psi_0\rangle = |0\rangle|0\rangle$ in $S_n \otimes S_n$.

Step 2.1 Apply QFT to the first register to get $|\psi_1\rangle = T|0\rangle \otimes |0\rangle$.

Step 2.2 Apply f using the unitary U_f so that $U_f|\psi_1\rangle = |\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|f(x)\rangle$.

Step 2.3 Apply QFT to the first register to get $\Upsilon(y) = \sum_{x=0}^{Q-1} w_n^{-xy}|f(x)\rangle$ and

$$|\psi_3\rangle = \frac{1}{Q}\sum_{x=0}^{Q-1} T|x\rangle|f(x)\rangle = \frac{1}{Q}\sum_{y=0}^{Q-1} \|\Upsilon(y)\|\, |y\rangle \frac{|\Upsilon(y)\rangle}{\|\Upsilon(y)\|}.$$

Step 2.4 Measure the first register. The probability of $y \in S_n$ will be

$$\mathrm{Prob}(y) = Q^{-2}\|\Upsilon(y)\|^2/Q^2 = Q^{-2}|\sum_b w^{bPy}|^2,$$

and the state collapses to $|y\rangle(\|\Upsilon(y)\|/Q)$, where $w = e^{2\pi i/Q}$.

Step 2.5 Find the order P from the measurement outcome.

Here, because f is periodic, $f(x) = f(x+P)$ we see that $\|\Upsilon(y)\|^2/Q^2$ is larger if (w^{Py}) is near the to ± 1, i.e., yP/Q is close to an integer c.

By the theory of of continued fractions of rational number, we need to find d/s such that

$$|d/s - y/Q| \le 1/(2Q), \qquad \gcd(d,s) = 1,\ s < N.$$

If $f(x) = f(x+s)$ then $s = P$.

If not, try ms or other fraction d'/s' to approximate y/Q.

Else, repeat the algorithm.

Exercise 8.2 (Optional Homework)

Let $N = 21$ and $m = 11$. Then $n = 9$ so that $N^2 < 2^9 < (N+1)^2$. The period is 6.

§8.4 Probability Distribution (Details)

Proposition 8.1 Let $Q = 2^n = Pq + r$ with $0 \le r < P$, and let $Q_0 = Pq$.

(a) If Py is not a multiple of Q, then

$$\|\Upsilon(y)\|^2 = \frac{r\sin^2\left(\frac{\pi Py}{Q}\left(\frac{Q_0}{P}+1\right)\right) + (P-r)\sin^2\left(\frac{\pi Py}{Q}\cdot\frac{Q_0}{P}\right)}{\sin^2\left(\frac{\pi Py}{Q}\right)}.$$

(b) If Py is a multiple of Q, then

$$\|\Upsilon(y)\|^2 = \frac{r(Q_0+P)^2 + (P-r)Q_0^2}{P^2}.$$

Remark Only those $y \in \{0, \ldots, Q-1\}$ satisfying $y = Pr$ has high $\mathrm{Prob}(y)$.

Limitation One may do a number of measurements to determine P by finding the minimum distance between those $|y\rangle$ with high probability. But this is impractical if N is large.

§8.5 Continued Fractions and Order Finding (Details)

1. Every rational number $x = y/Q$ can be expressed as continued fractions.

2. The jth convergent is useful in approximating the rational number $x = y/Q$.

3. To find the order P in our problem, use the jth convergent to construct the sequence

$$(p_0, q_0), \ldots, (p_M, q_M).$$

   Determine the smallest k such that $|p_k/q_k - y/Q| \le 1/(2Q)$. Then $P = q_k$.

   [Here we use the fact that $y/Q = r/P$ for some integer r and the choice of $N^2 \le Q \le 2N^2$.]

§8.6 Modular Exponential Function

To that the Shor's algorithm is polynomial time, one needs to implement the computation of $f(x) = m^x$ efficiently using quantum gates. This can be done.