$c, t \in \mathbb{Z}_{2^n}$, $C\text{-}V_a|c\rangle_n|t\rangle_n = \begin{cases} |c\rangle_n \cdot |a^c t \bmod N\rangle_n & 0 \le t < N \\ |t\rangle_n & N \le t < 2^n \end{cases}$ 인 quantum circuit을 implement

$i \in \mathbb{Z}_n$, $a_i \equiv a^{2^i} \pmod N \Rightarrow a_i \equiv a_{i-1}^2 \pmod N$, $c = \sum_{i=0}^{n-1} c_i 2^{n-1-i}$ $(0 \le i < n,\ c_i \in \{0,1\})$ 이면 $0 \le i \le n$

$t < N$ 이면 $t_i = \prod_{l=0}^{i-1} a_{n-l-1}^{c_l} t \pmod N$, $t \ge N$ 이면 $t_i = t$ 일 때 $t < N$ 인 경우 : $t_0 = \prod_{l=0}^{-1} a_{n-l-1}^{c_l} t \pmod N$

$= t$, $t_n = \prod_{l=0}^{n-1} a_{n-l-1}^{c_l} t \pmod N = \prod_{l=0}^{n-1} a^{c_l 2^{n-l-1}} \cdot t \pmod N = a^{\sum_{l=0}^{n-1} c_l 2^{n-l-1}} t \pmod N = a^c t \pmod N$ 이다.

$0 \le i \le n-1$ 이면 $t_{i+1} = a_{n-i-1}^{c_i} \cdot t_i \pmod N$ 이다.

$x, y \in \mathbb{Z}_{2^n}$, $U_m|x\rangle|y\rangle = \begin{cases} |x\rangle|xy \bmod N\rangle & (x,y) \in \mathbb{Z}_N^2 \wedge \gcd(y,N)=1 \\ |x\rangle|y\rangle & (x,y) \in \mathbb{Z}_N^2 \cup \gcd(y,N) > 1 \end{cases}$: bijective 라고 unitary, $O(n^2)$

$U_p: |a\rangle_n \otimes \bigotimes_{i=1}^{n-1} |0\rangle_n \to \bigotimes_{i=0}^{n-1} |a_i\rangle_n$, $|\psi\rangle = |a\rangle_n |0\rangle_n^{\otimes n-1}$, $|\psi_{i-1}\rangle|\psi_i\rangle = CNOT_n|\psi_{i-1}\rangle|\psi_i\rangle$,

$|\psi_{i-1}\rangle|\psi_i\rangle \leftarrow U_m|\psi_{i-1}\rangle|\psi_i\rangle$: for $i = 1 \sim n-1$ 이면 $U_p|\psi\rangle = |a_0\rangle \cdots |a_{n-1}\rangle$, $O(n^3)$

pf) $U_m CNOT_n |a\rangle_n|0\rangle_n = U_m |a_0\rangle_n |a_0\rangle_n = |a_0\rangle_n |a_0^2 \bmod N\rangle_n = |a_0\rangle_n |a_1\rangle_n$ $(a_0 = a \pmod N = a$

귀납법에 의해 $|a_0\rangle_n \cdots |a_{i-1}\rangle_n U_m CNOT_n |a_i\rangle_n |0\rangle_n \cdots = |a_0\rangle_n \cdots |a_{i-1}\rangle_n U_m |a_i\rangle_n |a_i\rangle_n = |a_0\rangle_n \cdots |a_{i-1}\rangle_n$

귀납법으로 $|a_0\rangle_n \cdots |a_{i-1}\rangle_n U_m (CNOT_n (|a_i\rangle_n |0\rangle_n) \cdots = |a_0\rangle_n \cdots |a_{i-1}\rangle_n U_m (|a_i\rangle_n |a_i\rangle_n) = |a_0\rangle_n \cdots |a_{i-1}\rangle_n$

$|a_i\rangle_n |a_i^2 \bmod N\rangle_n |0\rangle_n \cdots = |a_0\rangle_n \cdots |a_{i+1}\rangle_n |0\rangle_n \cdots$ 이므로 성립. loop (U_m: $O(n^2)$) $\therefore O(n^3)$

(-U_a: $|\psi\rangle = |c\rangle_n |a\rangle_n |0\rangle_n^{\otimes m-1} |1\rangle_n |t\rangle_n$, U_p는 $|\psi\rangle = |c\rangle_n |a_0\rangle_n \cdots |a_{n-1}\rangle_n |1\rangle_n |t\rangle_n$, $i = 1 \sim n$

$|\psi\rangle = CSWAP_{i-1} |\psi\rangle$, $|\psi_{n+1}\rangle |\psi_{n+2}\rangle = U_m |\psi_{n+1}\rangle |\psi_{n+2}\rangle$, $|\psi\rangle = CSWAP_{i-1} |\psi\rangle$

pf) $CSWAP_1 |\psi\rangle = |c\rangle_n \cdots |a_{n-1}\rangle_n |1\rangle_n |t\rangle_n$ if $c_0 = 0$, $|c\rangle_n \cdots |a_{n-2}\rangle_n |1\rangle_n |a_{n-1}\rangle_n |t\rangle_n$ if $c_0 = 1$

$\therefore U_m |1\rangle_n |t\rangle_n = |a_1\rangle |t\rangle_n = |1\rangle_n |a_{n-1}^{c_0} + \bmod N\rangle = |1\rangle_n |t_1\rangle_n$. $U_m |a_{n-1}\rangle_n |t\rangle_n = |a_{n-1}\rangle_n |t\rangle_n$ or

$|a_{n-1}\rangle_n |a_{n-1}^{c_0} + \bmod N\rangle_n = |a_{n-1}\rangle_n |t_1\rangle_n$, 다시 $CSWAP_1$: $\psi = |c\rangle_n |a_0\rangle_n \cdots |a_{n-1}\rangle_n |1\rangle_n |t_1\rangle_n$ 이다.

귀납법으로 $i = n$: $|\psi\rangle = |c\rangle_n |a_0\rangle_n \cdots |a_{n-1}\rangle_n |t\rangle_n |t_n\rangle_n$ $\therefore |c\rangle_n |t_n\rangle_n = (-U_a) |c\rangle_n |t\rangle_n$

Ancilla bit: $O(n^2)$, U_p: $O(n^3)$, loop ($CSWAP_i$: $O(1)$, U_m: $O(n^2)$) $\therefore$ $O(n^3)$ 이다.

$q \geq N^2$로 가정 했을 = 4 (6.4.6) $n = O(\log N)$ ∴ $O(n^3) = O((\log N)^3)$

integer factorization problem : classical, fully analysed Monte Carlo algorithm

: $e^{(1+o(1))(\log N \cdot (\log \log N))^{\frac{1}{2}}}$

heuristic Monte Carlo algorithm: $e^{\left(\frac{4}{3^{2/3}} + o(1)\right) \cdot (\log N)^{\frac{1}{3}} \cdot (\log(\log N))^{\frac{2}{3}}}$

$a \in \mathbb{Z}_n$: select, $d = \gcd(a, N)$ compute, $d = 1 \Rightarrow$ Find order $(N, a, 2\lceil \log N \rceil + 1)$으로

$a^r \equiv 1 \pmod N$인 r을 최소 99.9%의 확률로 $\Rightarrow$ $2|r$이면 $(a^{r/2}-1)(a^{r/2}+1) \equiv 0 \pmod N$ $N \nmid a^{r/2}+1 \Rightarrow \gcd(a^{r/2-1}, N)$:

: N의 proper divisor with probability at least 0.199, $O((\log N)^3)$

p: odd prime number, $e \in \mathbb{N}$, $p = 2^d m + 1$, $2 \nmid m$, $a \in \mathbb{Z}_{p^e}^*$. $a^r \equiv 1 \pmod{p^e}$, $2^d | r$일 확률: 1/2

p의 $\varphi(p^e) = (p-1)p^{e-1}$, $g \in \mathbb{Z}_{p^e}^*$, $g^{\varphi(p^e)} \equiv 1 \pmod{p^e}$이면 $\mathbb{Z}_\varphi \to \mathbb{Z}_{p^e}^*$, $k \mapsto g^k \pmod{p^e}$: bijective,

$a = g^k \pmod{p^e} \Rightarrow$ a의 order $r = \frac{\varphi}{\gcd(k, \varphi)}$ 이므로 k: even $\frac{1}{2}$, odd $\frac{1}{2}$ ∴ $2^d | r$: 1/2

$N=\prod_{i=1}^{m} p_i^{e_i}$, $a\in\mathbb{Z}_N^*$, $a \bmod N$ の order r: $2\mid r,\ a^{r/2}\not\equiv -1 \pmod N$ 2 $1-2^{1-m}$

pf) $a_i\in\mathbb{Z}_{p_i^{e_i}}$, $a\in\mathbb{Z}_N^*$, $a\equiv a_i \bmod p_i^{e_i}$, r: order of $a \bmod N$, r_i: order of $a_i \bmod p_i^{e_i}$

$r=\mathrm{lcm}(r_1,\cdots,r_n)$. $r=2^t m$, $r_i=2^{f_i} m_i$ (m, m_i: odd), r: odd or r: even, $a^{r/2}\not\equiv -1 \pmod N \Rightarrow 1\le i\le m,\ f=f_i$

r: odd: $2\nmid r$, $2\mid r,\ a^{r/2}\not\equiv -1 \pmod N \Rightarrow a^r\equiv 1 \pmod{p_i^{e_i}},\ a^{r/2}\not\equiv -1 \pmod{p_i^{e_i}} \therefore r_i\mid r,\ r_i\nmid r/2 \therefore f=f_i$

$\therefore$ r: odd or $2\mid r,\ a^{r/2}\not\equiv -1 \pmod N \le \forall i,j,\ 1\le i,j\le m,\ f_i=f_j \le \frac{1}{2^{m-1}}$ $\therefore$

$1-\frac{1}{2^{m-1}}\ge\frac{1}{2} \therefore 0.999\cdot\frac{1}{2}\simeq 0.499$, $O((\log N)^3)$

$2\nmid N$, $a,b\in\mathbb{Z}_N^*$, r: order of $a \bmod N$, $a^t\equiv b \pmod N$: t: discrete logarithm of b to base $a \bmod N$, we may assume r is prime by the Oohlig-Hellman algorithm, $t\ge 1$

$n\in\mathbb{N}$, U_a, U_b: $|x\rangle_n \to \begin{cases} |ax \bmod N\rangle_n & 0\le x<N \\ |x\rangle_n & N\le x<2^n \end{cases}$, U_a: 1 eigenvalue: $a^{2\pi i\cdot\frac{k}{r}}$, U_b: 1 eigenvalue: $a^{2\pi i\cdot\frac{k}{r}}$

$0\le k<r$, by quantum phase estimation, $(x,y)\in\mathbb{Z}_{2^n}\times\mathbb{Z}_{2^n}$, $x=\left\lfloor\frac{2^n k}{r}\right\rceil$, $x\equiv t\cdot\left\lfloor\frac{2^n k}{r}\right\rceil \bmod r=\left\lfloor\frac{2^n y}{r}\right\rceil$ $\therefore t\equiv x\left\lfloor\frac{2^n y}{r}\right\rceil^{-1} \bmod r$

$n = \lceil \log_2 r \rceil + 1$: probability $\frac{64(r-1)}{\pi^2 r}$, $O((\log_2 N)^3)$

Pf) $|\psi_0\rangle = |0\rangle_n |0\rangle_n |1\rangle_n$, $|\psi_1\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} |1\rangle_n$, $\subset U_a$ operator $|\psi_{2a}\rangle = \frac{1}{\sqrt{2^n r}} \sum_{x=0}^{r-1} |\psi_a(x)\rangle$

$\cdot \left(\sum_{y=0}^{2^n-1} |y\rangle\right) \cdot |u_n\rangle$ $\subset U_b$ operator: $|\psi_{3a}\rangle = \frac{1}{r} \sum_{x=0}^{r-1} \left(|\psi_a(x)\rangle |\psi_a(x+1)\rangle |u_n\rangle\right)$, $|\psi_3\rangle = \left(\left(\frac{1}{r}, |\psi_a(x)\rangle, |\psi_a(x+1)\rangle\right)\right)_{\text{distinct } x}$

apply QFT_n^{-1} : $|\psi_4\rangle = \left(\left(\frac{1}{r}, QFT_n^{-1} |\psi_a(x)\rangle QFT_n^{-1} |\psi_a(x+1)\rangle\right)\right)_{\text{distinct } x}$ probability $\frac{64}{\pi^2 r}$. $(x,y) \in \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n}$,

$|\alpha(x,n,x)| < \frac{1}{2^n} < \frac{1}{2r}$, $|\alpha(x+mr, n, y)| < \frac{1}{2^n} < \frac{1}{2r}$ 이므로 $K = \lfloor \frac{2^n}{r} \rfloor$, $x+mr = \lfloor \frac{N}{r} \rfloor$

Classical public-key cryptography is vulnerable. Quantum-resistant cryptography

Group G, $H < G$, set X, $f: G \to X$, $\forall g, g' \in G$, $gH = g'H \iff f(g) = f(g')$ only if f: hides subgroup H

$\therefore f$ has the same value for all elements of a coset of H,

input: f, output: finite generating system for H

Deutsch: $f: \{0,1\} \to \{0,1\}$, f is constant: f hides $\{0,1\}$, f is balanced: f hides $\{0\}$

Simon's problem: $f:\{0,1\}^n \to \{0,1\}^n$. $\vec{s}\in\{0,1\}^n$, $\vec{s}\neq\vec{0}$, $\forall \vec{x},\vec{y}\in\{0,1\}^n$, $\vec{y}=\vec{x}\oplus\vec{s} \Leftrightarrow f(\vec{x})=f(\vec{y})$

: $H=\{\vec{0},\vec{s}\}$; generating system $(\vec{s})$, $(\vec{0},\vec{s})$

$N=3, 2\nmid N$, $a\in\mathbb{Z}_N^*$, $\gcd(a,N)=1$. $f:(\mathbb{Z},+)\to\mathbb{Z}_N$, $f(j)=a^j \pmod N$, $H=r\mathbb{Z}:(r)$

$a,b\in\mathbb{Z}_N^*$, r: order of $a \bmod N$. $f:(\mathbb{Z}_r\times\mathbb{Z}_r,+)\to\mathbb{Z}_N$, $(x,y)\mapsto a^x b^y$, $H=\mathbb{Z}_r(1,-t)$

r,t,m of $H=\mathbb{Z}_r(1,-t)$ generating system $(x_0,y_0),\cdots,(x_{m-1},y_{m-1})$, $d=\gcd(x_0,\cdots,x_{m-1})$

$\gcd(d,r)=1$. $t=d^{-1}\gcd(y_0,\cdots,y_{m-1}) \bmod r$

$P(\exists u_0,\cdots,u_{m-1}\in\mathbb{Z}$. $\sum_{i=0}^{m-1} u_i(x_i,y_i)\equiv(1,-t) \bmod r$, $(x_i,y_i)\in\mathbb{Z}_r(1,-t)$, $\sum_{i=0}^{m-1} u_i x_i:(y_i-t)\equiv(1,-t) \bmod r$

$\therefore x_i'=x_i/d$ of mod $d\sum_{i=0}^{m-1} u_i x_i'\equiv 1 \pmod r$ $\therefore \gcd(d,r)=1$, $\gcd(y_0,\cdots y_{m-1})\equiv td \bmod r$