Úvod do kvantového počítání

6. přednáška

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

12. května 2005

Část I

Shorův faktorizační algoritmus

Motivace pro faktorizaci

RSA

Obtížnost faktorizace je základem pro kryptofrafii s veřejným klíče u algoritmu RSA.

Matematické základy pro RSA:

- Grupy, př.: $(Z, +)$, $(Q, \cdot)$, $(Z_n^*, \cdot)$
- Euklidův algoritmus
- Diofantická rovnice: $ax + by = d \quad \in Z$
- Bezoutova věta: $d = gcd(a, b) \Rightarrow \exists x, y \in Z$
- Kongruence (mod N): $a \equiv b \pmod{N}$ iff N dělí $(a - b)$

Matematické pozadí

- Eulerova funkce $\Phi(n)$ - počet invertibilních prvků v Z_n.
  - $\Phi(p) = p - 1$
  - $\Phi(p^k) = p^k - p^{k-1}$
  - $\Phi(m.n) = \Phi(m).\Phi(n)$, iff gcd(m,n)=1

RSA

1. Zvol prvočísla p, q; $N = p.q$, $\Phi(N) = (p-1)(q-1)$
2. Alice vygeneruje e_A, které je nesoudělné s $\Phi(N)$. dopočítá d_A : $e_A d_A \equiv 1 \bmod \Phi(N)$
3. Bob posílá Alici zprávu x: zašifrovaná zpráva $y \equiv x^{e_A} \bmod N$
4. Alice přijímá y: dešifrovaná zpráva $z \equiv y^{d_A} \bmod N$, $z = x$.

Nejslabší místo

Veřejný klíč je tvořen dvojicí (e_A, N). Aby útočník mohl dopočítat d_A a získat obsah dopisu určeného Alici, musí znát $\Phi(N)$. Výpočet $\Phi(N)$ vede přes rozklad N na prvočíselný součin - faktorizace.

Algoritmus pro faktorizaci

Věta

Pokud existuje algoritmus řešící rovnici

$$x^2 \equiv 1 \bmod N$$

pro netriviální řešení $x = \pm 1$, pak existuje algoritmus na prvočíselný rozklad.

Algoritmus pro faktorizaci

Důkaz

- Pro $a \neq \pm 1 \bmod N$ nechť $a^2 \equiv 1 \bmod N$.
- Potom $a^2 - 1 = (a-1)(a+1) = N$; pokud N není provočíslo pak jeho faktor musí dělit $(a+1)$ nebo $(a-1)$.
- Největší faktor $f(N) = max\{\gcd(a+1, N), \gcd(a-1, N)\}$ naleznu v $O(\log N)$ krocích pomocí Euklidova algoritmu.

Shorův faktorizační algoritmus

1. Vyber $0 < y < N$ náhodně.
2. Když $\gcd(y, N) \neq 1$ máme faktor, exit.
3. Nalezneme periodu r funkce $y^k \bmod N$.
   Tedy $y^r = 1 \pmod N$.
4. Když r liché číslo nebo $y^{r/2} = \pm 1$ (triviální řešení) goto 1.
5. $y^{r/2}$ je netriviální řešení rovnice $x^2 \equiv 1 \pmod N$.

Poznámka

Pokud existuje polynomiální algoritmus na nalezení periody funkce $y^k \pmod N$, pak existuje polyomiální algoritmus pro nalezení řešení rovnice $x^2 \equiv 1 \pmod N$.

Kvantové hledání periody funkce

Pomocí kvantového paralelismu provedeme

$$\frac{1}{\sqrt{2^d}} \sum_{k=0}^{2^d-1} |k,0\rangle \rightarrow \frac{1}{\sqrt{2^d}} \sum_{k=0}^{2^d-1} |k, f_{N,y}(k)\rangle, \text{ pro } N = 2^d - 1$$

Kvantové hledání periody funkce

Např. pro číslo $N = 15$ a $y = 7$ dostaneme:

$$\frac{1}{4}\left(|0,1\rangle + |1,7\rangle + |2,4\rangle + |3,13\rangle + \cdots + |14,4\rangle + |15,13\rangle\right)$$

Po měření na druhém qubitu dostaneme jeden ze stavů:

Výsledek	**Stav**	**Offset**
1	$\frac{1}{2}\left(|0\rangle + |4\rangle + |8\rangle + |12\rangle\right)|1\rangle$	0
4	$\frac{1}{2}\left(|2\rangle + |6\rangle + |10\rangle + |14\rangle\right)|4\rangle$	2
7	$\frac{1}{2}\left(|1\rangle + |5\rangle + |9\rangle + |13\rangle\right)|7\rangle$	1
13	$\frac{1}{2}\left(|3\rangle + |7\rangle + |11\rangle + |15\rangle\right)|13\rangle$	3

Sekvence jsou v podstatě stejné, mají periodu 4, liší se pouze offsetem. Fourierovou transformací se nám podaří dostat offset do fáze.

Postup pro výpočet periody

Máme číslo N, které chceme faktorizovat, vybereme pro něj vhodné $q \in O(N^2)$, které je mocninou čísla 2. Náhodně vybereme číslo y v rozsahu $0..N$. Poslední dva registry mají délku $\lceil \log N \rceil$ qubitů.

- Hadamardova rotace na 4. registr

$$|N, y, q, 0, 0\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} |N, y, q, k, 0\rangle$$

- Výpočet $y^k \pmod N$ na 5. registru

$$\frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} |N, y, q, k, 0\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} |N, y, q, k, y^k \bmod N\rangle$$

Postup pro výpočet periody

Poznámka

Měřením na 5. registru získáme hodnotu x. Tj. $x = y^l \pmod N$ pro nejmejnší l splňující tuto rovnici. Pokud r je perioda pak $y^l = x^{jr+l}$ pro libovolné j. Tím ve 4. registru dostaneme seznam "k-ček", která jsou ve tvaru $l, l + 1r, l + 2r, \ldots, l + Ar$.

- Měření na 5. registru

$$\frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} |N, y, q, k, y^k \bmod N\rangle \rightarrow \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |N, y, q, jr + l, x\rangle$$

Převod offsetu do fáze

- Z předcházejícího registru, nás zajíma už pouze 4. registr a pro $A = \frac{q}{r} - 1$ ho přepíšeme do tvaru:

$$\frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr + l\rangle \rightarrow \sqrt{\frac{r}{q}} \sum_{j=0}^{q/r-1} |jr + l\rangle$$

- Aplikace Kvantové Fourierovy transformace

$$\sqrt{\frac{r}{q}} \sum_{j=0}^{q/r-1} |jr + l\rangle \rightarrow \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i l c/q} |c\rangle, \text{ kde } c = j\frac{q}{r}$$

Převod offsetu do fáze

Poznámka

Offset / se tak dostal do fáze, kde nemá význam na pravděpodobnost naměření nebo na hodnotu v registru.

Výpočet periody

Změřím stav $|c\rangle$ o kterém vím, že je násobkem q/r. Tj. $c = \lambda\frac{q}{r}$. Potom platí

$$\frac{c}{q} = \frac{\lambda}{r}$$

. Čísla λ, c znám. Reálné číslo c/q vyjádřím pomocí řetězových zlomků a jeho konvergenty jsou kandidáti na $\frac{\lambda}{r}$, kde $\lambda < r$.