Kvantinio Shor algoritmo klasikinė matematinė analizė

R. Čiegis

Vilniaus Gedimino technikos universitetas
e-mail: rc@vgtu.lt

Balandžio 8 d., 2025, Vilnius

Galėtume pasirinkti ne vieną kvantų tematiką, kurios jau užpildė HPC ir virtualaus modeliavimo mokslinius žurnalus, socialinius tinklus ir net pakeitė šeimininkių pokalbių tematiką populiariuose Vilniaus turguose.

Universiteto kavinėje pokalbiai apie kvantinius algoritmus, pagardinti kvantine kava irgi tapo savaitiniu antradienio renginiu. Kviečiame prisijungti.

Taigi universitetuose matematikams jau kaip ir būtina tapti "raštingais" kvantinių algoritmų teorijoje (o dar geriau ir skaičiavimo įgūdžių srityje).

Reikia išskaidyti duotąjį skaičių n į du pirminius daugiklius $n = pq$.

Reikia išskaidyti duotąjį skaičių n į du pirminius daugiklius $n = pq$.

Tai klasikinis ir labai gražus skaičių teorijos uždavinys.

Reikia išskaidyti duotąjį skaičių n į du pirminius daugiklius $n = pq$.

Tai klasikinis ir labai gražus skaičių teorijos uždavinys.

Pradėjus plačiai naudoti RSA viešojo rakto algoritmą – skaičių faktorizavimas tapo labai aktualiu taikomuoju uždaviniu.

Nagrinėkime paprasčiausią ir dažniausiai naudojamą algoritmą, kuriuo faktorizavimo uždavinį sprendžiame ieškodami mažesniojo pirminio daugiklio p. Iš eilės tikriname visus nelyginius skaičius nuo 3 iki $\sqrt{n}$. Jo sudėtingumas yra $O(\sqrt{n})$.

Nagrinėkime paprasčiausią ir dažniausiai naudojamą algoritmą, kuriuo faktorizavimo uždavinį sprendžiame ieškodami mažesniojo pirminio daugiklio p. Iš eilės tikriname visus nelyginius skaičius nuo 3 iki $\sqrt{n}$. Jo sudėtingumas yra $O(\sqrt{n})$.

Imkime dabartinį RSA šifravimo algoritmo raktą, jo ilgis $2^{2048} = 10^{616}$, tada skaičiavimų apimtis yra $O(10^{308})$.

Nagrinėkime paprasčiausią ir dažniausiai naudojamą algoritmą, kuriuo faktorizavimo uždavinį sprendžiame ieškodami mažesniojo pirminio daugiklio p. Iš eilės tikriname visus nelyginius skaičius nuo 3 iki $\sqrt{n}$. Jo sudėtingumas yra $O(\sqrt{n})$.

Imkime dabartinį RSA šifravimo algoritmo raktą, jo ilgis $2^{2048} = 10^{616}$, tada skaičiavimų apimtis yra $O(10^{308})$.

Galingiausių lygiagrečiųjų kompiuterių skaičiavimo greitis yra net 10^{18} operacijų per sekundę, bet tai tik lašelis jūroje norint "nulaužti" RSA raktą.

Šiandien žinomi sparčiausi faktorizavimo algoritmai yra stochastiniai. Paminėsime bendrąjį skaičių lauko rėtį (The Number Field Sieve).

Jo sudėtingumas yra superpolinominis:

$$O\left(\exp\left(1.9(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)\right).$$

Šiandien žinomi sparčiausi faktorizavimo algoritmai yra stochastiniai. Paminėsime bendrąjį skaičių lauko rėtį (The Number Field Sieve).

Jo sudėtingumas yra superpolinominis:

$$O\left(\exp\left(1.9(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)\right).$$

Tada RSA rakto radimas pareikalaus tik $O(10^{35})$ veiksmų, bet visgi tai neįveikiamas uždavinys šiuolaikiniams kompiuteriams.

Shor atkreipė dėmesį į kitą faktorizacijos algoritmą, paskelbtą Miller, 1976 metais.

Shor atkreipė dėmesį į kitą faktorizacijos algoritmą, paskelbtą Miller, 1976 metais.

1. Atsitiktinai pasirenkame skaičių $x < n$, tokį, kad $\gcd(x, n) = 1$.
2. Apibrėžiame funkciją $f(a) := x^a \pmod{n}$.

Shor atkreipė dėmesį į kitą faktorizacijos algoritmą, paskelbtą Miller, 1976 metais.

1. Atsitiktinai pasirenkame skaičių $x < n$, tokį, kad $\gcd(x, n) = 1$.
2. Apibrėžiame funkciją $f(a) := x^a \pmod{n}$.
3. Randame (kažkaip) funkcijos $f(a)$ periodą $f(a + r) = f(a)$, t.y. tokį r, kad $x^r \equiv 1 \pmod{n}$.

Shor atkreipė dėmesį į kitą faktorizacijos algoritmą, paskelbtą Miller, 1976 metais.

1. Atsitiktinai pasirenkame skaičių $x < n$, tokį, kad $\gcd(x, n) = 1$.
2. Apibrėžiame funkciją $f(a) := x^a \pmod{n}$.
3. Randame (kažkaip) funkcijos $f(a)$ periodą $f(a + r) = f(a)$, t.y. tokį r, kad $x^r \equiv 1 \pmod{n}$.
4. Jeigu r yra lyginis ir $x^{\frac{r}{2}} \not\equiv -1 \pmod{n}$, tai skaičiuojame skaičiaus n pirminius daugiklius

$$p, q := \gcd(x^{\frac{r}{2}} \pm 1, n),$$

nes

Shor atkreipė dėmesį į kitą faktorizacijos algoritmą, paskelbtą Miller, 1976 metais.

1. Atsitiktinai pasirenkame skaičių $x < n$, tokį, kad $\gcd(x, n) = 1$.
2. Apibrėžiame funkciją $f(a) := x^a \pmod{n}$.
3. Randame (kažkaip) funkcijos $f(a)$ periodą $f(a + r) = f(a)$, t.y. tokį r, kad $x^r \equiv 1 \pmod{n}$.
4. Jeigu r yra lyginis ir $x^{\frac{r}{2}} \not\equiv -1 \pmod{n}$, tai skaičiuojame skaičiaus n pirminius daugiklius

$$p, q := \gcd(x^{\frac{r}{2}} \pm 1, n),$$

nes

$$(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = x^r - 1 \equiv 0 \pmod{n}.$$

Tada turime gauti atsakymus į tokius klausimus:

1. Ar sudėtinga parinkti tinkamą skaičių x?

Tada turime gauti atsakymus į tokius klausimus:

1. Ar sudėtinga parinkti tinkamą skaičių x?

Shor parodė, kad atsitiktinai parenkant x tokį, kad $\gcd(x, n) = 1$, tikimybė, jog x yra tinkamas periodo paieškai,
t.y. r yra lyginis skaičius ir $x^{\frac{r}{2}} + 1 \not\equiv 0 \pmod{n}$

yra lygi $\frac{1}{2}$.

$n = 15 = 3x5$

Imkime $x = 8$.

a :	0	1	2	3	4
$8^a \mod 15$:	1	8	4	2	1

Tada $r = 4$, $x^2 + 1 = 5 \not\equiv 0 \mod 15$, $p, q = \gcd(4 \pm 1, 15) = \{3, 5\}$.

$n = 15 = 3x5$

Imkime $x = 8$.

a :	0	1	2	3	4
$8^a \mod 15$:	1	8	4	2	1

Tada $r = 4$, $x^2 + 1 = 5 \not\equiv 0 \mod 15$, $p, q = \gcd(4 \pm 1, 15) = \{3, 5\}$.

Imkime $x = 4$.

a :	0	1	2
$4^a \mod 15$:	1	4	1

Tada $r = 2$, $x^1 + 1 = 5 \not\equiv 0 \mod 15$, $p, q = \gcd(4 \pm 1, 15) = \{3, 5\}$.

Imkime $x = 14$.

a :	0	1	2
$14^a \bmod 15$:	1	14	1

Tada $r = 2$, $x^1 + 1 = 15 \equiv 0 \bmod 15$ – netinka.

Turime 2 registrus, kiekviename po j kubitų

$$|0\rangle|0\rangle := |00\ldots0\rangle|00\ldots0\rangle\,.$$

Turime 2 registrus, kiekviename po j kubitų

$$|0\rangle|0\rangle := |00\ldots0\rangle|00\ldots0\rangle\,.$$

Pirmojo registro kiekvienam kubitui pritaikome Hadamar transformaciją, kuri perveda kubitą į superpoziciją $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|0\rangle\,.$$

Turime 2 registrus, kiekviename po j kubitų

$$|0\rangle|0\rangle := |00\ldots0\rangle|00\ldots0\rangle\,.$$

Pirmojo registro kiekvienam kubitui pritaikome Hadamar transformaciją, kuri perveda kubitą į superpoziciją $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a\rangle|0\rangle\,.$$

Tada kiekvienam a skaičiuojame $x^a(\mod n)$ ir rezultatą saugome antrame registre

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a\rangle|x^a(\mod n)\rangle\,.$$

Tai svarbiausia Shor algoritmo dalis: jis sukonstravo efektyvią kvantinę unitariąją funkciją, jos sudėtingumas yra logaritminis, t.y. kvadratinė polinominė funkcija $(\log n)^2 \log\log n$.

Tai svarbiausia Shor algoritmo dalis: jis sukonstravo efektyvią kvantinę unitariąją funkciją, jos sudėtingumas yra logaritminis, t.y. kvadratinė polinominė funkcija $(\log n)^2 \log\log n$.

Užbaigus šį žingsnį, jau suradome periodą r, bet negalime jį išskirti ir spausdinti...

Tai svarbiausia Shor algoritmo dalis: jis sukonstravo efektyvią kvantinę unitariąją funkciją, jos sudėtingumas yra logaritminis, t.y. kvadratinė polinominė funkcija $(\log n)^2 \log\log n$.

Užbaigus šį žingsnį, jau suradome periodą r, bet negalime jį išskirti ir spausdinti...

Shoro algoritme su pirmojo registro kubitais atliekame kvantinę Furje transformaciją, jos apibrėžimas yra analogiškas klasikinei diskrečiajai FT (atvaizduojame kubitą a):

$$\frac{1}{q^{1/2}} \sum_{c=0}^{q-1} \exp(2i\pi ac/q)\,|c\rangle\,.$$

Tada gauname tokią kvantinę būseną

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2i\pi ac/q)\,|c\rangle\,.$$

CFT realizavimo algoritmo sudėtingumas vėl logaritminis.

Tada gauname tokią kvantinę būseną

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2i\pi ac/q)\,|c\rangle\,.$$

CFT realizavimo algoritmo sudėtingumas vėl logaritminis.

Laikas nuspręsti, kiek kubitų naudosime kiekviename registre.

Tada gauname tokią kvantinę būseną

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2i\pi ac/q)\,|c\rangle\,.$$

CFT realizavimo algoritmo sudėtingumas vėl logaritminis.

Laikas nuspręsti, kiek kubitų naudosime kiekviename registre.

Pasirinktas sprendimas atrodo nelogiškas: surandame q tokį, kad

$$q = 2^m, \quad n^2 \le q < 2n^2.$$

Dabar atliekame matavimą ir gauname rezultatą

$$\left| c, 2^k (\mod n) \right\rangle .$$

Faktiškai mums svarbus tik pirmojo registro rezultatas.

Dabar atliekame matavimą ir gauname rezultatą

$$\left| c, 2^k (\mod n) \right\rangle .$$

Faktiškai mums svarbus tik pirmojo registro rezultatas.

Apskaičiuokime tikimybę, kad bus gautas kaip tik toks matavimo rezultatas.

Dabar atliekame matavimą ir gauname rezultatą

$$\left| c, 2^k (\mod n) \right\rangle .$$

Faktiškai mums svarbus tik pirmojo registro rezultatas.

Apskaičiuokime tikimybę, kad bus gautas kaip tik toks matavimo rezultatas.

Funkcija $f(a)$ yra periodinė, jos periodas r (deja, jo reikšmės mes nežinome, jį norime rasti).
Sumuojame visus galimus tokio rezultato variantus

$$\left| \frac{1}{q} \sum_{a:\ x^a \equiv x^k} \exp(2i\pi ac/q) \right|^2 .$$

Pažymėję $a = br + k$, šią formulę galime užrašyti ir taip

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2i\pi (br + k)c/q) \right|^2 .$$

Shor pateikia nesudėtingą matematinę analizę, kokia yra tikimybė matavimuose gauti atskiras modas $\left|c, x^k \ (\mod n)\right\rangle$.

Ši tikimybė yra didelė tik toms modoms, kurioms liekana $\{rc\}_q$ (ji ekvivalenti $rc \ (\mod q)$), yra pakankamai maža:

$$|\{rc\}_q| \leq r/2,$$

Atkreipiame dėmesį, kad

$$|\{rc\}_q| \leq q/2.$$

Shor pateikia nesudėtingą matematinę analizę, kokia yra tikimybė matavimuose gauti atskiras modas $\left|c, x^k \ (\mod n)\right\rangle$.

Ši tikimybė yra didelė tik toms modoms, kurioms liekana $\{rc\}_q$ (ji ekvivalenti $rc \ (\mod q)$), yra pakankamai maža:

$$|\{rc\}_q| \leq r/2,$$

Atkreipiame dėmesį, kad

$$|\{rc\}_q| \leq q/2.$$

Taip bus tik tada, kai egzistuoja toks d, jog

$$-\frac{r}{2} \leq rc - dq \leq \frac{r}{2}.$$

Padaliję iš rq ir pertvarkę narius, gauname

$$\left| \frac{c}{q} - \frac{d}{r} \right| \leq \frac{1}{2q}.$$

Padaliję iš rq ir pertvarkę narius, gauname

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}.$$

Mes žinome c ir q. Kadangi $q > n^2$, tai egzistuoja ne daugiau kaip viena tokia trupmena d/r su $r < n$, kuri tenkina duotąją nelygybę.

Padaliję iš rq ir pertvarkę narius, gauname

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}.$$

Mes žinome c ir q. Kadangi $q > n^2$, tai egzistuoja ne daugiau kaip viena tokia trupmena d/r su $r < n$, kuri tenkina duotąją nelygybę.

Taigi reikia rasti mažiausią trupmenos vardiklį r, tarpusavyje pirminį su skaitikliu d.

Tokį uždavinį efektyviai sprendžiame naudodami tęstinių trupmenų metodą, kai skleidžiame c/q.

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \ddots}}}$$