Pokročilá kryptologie

Kvantová kryptografie 2

prof. Ing. Róbert Lórencz, CSc., Ing. Miroslav Dobšíček, Ph.D.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

Tato přednáška byla rovněž podpořena z prostředků projektu č. 347/2013/B1a Fondu rozvoje vysokých škol Ministerstva školství, mládeže a tělovýchovy

Obsah přednášky

- Kvantová mechanika
- Hilbertův prostor
- Probalistický registr
- Kvantový registr
- Faktorizace, Shorův algoritmus
- QFT

Kvantová mechanika

- Ke každému uzavřenému kvantovému systému existuje přirazený Hilbertův prostor (definovamý vnitřní skalární součin $\langle\psi|\psi\rangle$)
- $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$ - norma (velikost)

$$H^{(2)} \quad \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \quad \text{- vektor z prostoru } H^{(2)}$$

- Pro bázové vektory platí:

$$|0\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}, \qquad |1\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$$

- Pro libovolný vektor z $H^{(2)}$ platí, že jej můžemem vyjádřit pomocí superpozici bázových vektorů:

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

- **qubit** - kvantový bit - superpozice bázových vektorů

Kvantová mechanika - evoluce

- Evoluce je popsaná Schrödingerovou rovnici

$$H|\psi(t)\rangle = -i\hbar\frac{\partial}{\partial t}(|\psi(t)\rangle)$$

- Časová změna vektoru je rovna součinu vektoru s Hamiltonianem (Hermitovská matice)
- Násobení matici $\rightarrow$ otáčení vektoru

$$|\psi(t)\rangle = e^{\frac{-iHt}{\hbar}}|\psi(0)\rangle$$

$$|\psi(t)\rangle = \mathbf{U}|\psi(0)\rangle,$$

kde $\psi(t)\rangle$ - stav v daném čase, **U** - unitární matice, $\psi(0)$ - výchozí stav

- Transponováná a komplexní sdružená matice k matici **A** je Hermitovská sdružená matice $\mathbf{A}^+$
- Matici **A** označujeme jako unitární, jestliže: $\mathbf{A}^{-1} = \mathbf{A}^H$

Kvantová mechanika ...

- $\mathbf{U}\mathbf{U}^{+} = \mathbf{I}$ - identita, zachovává sklárny součin, vždy je to reverzibilní proces $\Rightarrow$ nemůžu informaci zničit ani ji zkopírovat
- **Lineární operátor** - lineární ve vstupech $\mathbf{U}(\alpha|0\rangle + \beta|1\rangle) = \alpha\mathbf{U}|0\rangle + \beta\mathbf{U}|1\rangle$, kde $\mathbf{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- **U** působí na celý vektor = působí na jeho prvky $\Rightarrow$ kvantový paralelizmus (otáčení vekotoru)

Hilbertův prostor

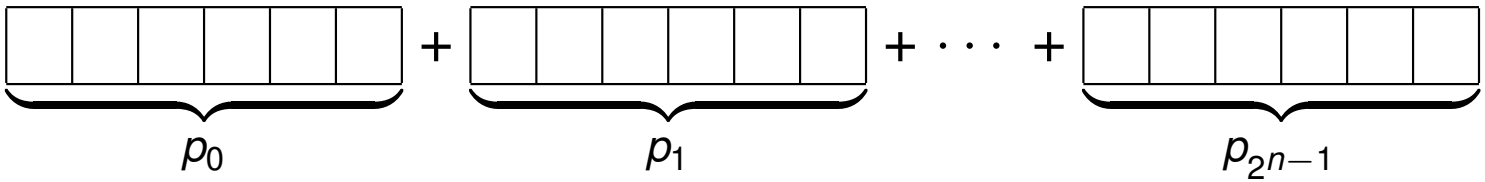
- 2 Hilbertové prostory $\Rightarrow$ výsledný prostor je dán tenzorovým součinem:
  $H^{(AB)} = H^{(A)} \otimes H^{(B)}, \quad \dim(AB) = \dim(A) \cdot \dim(B)$
- n qubitů $\rightarrow H^{2^n}$
- $\underbrace{\alpha|0\rangle + \beta|1\rangle}_{H^2} \otimes \underbrace{\gamma|0\rangle + \delta|1\rangle}_{H^2} =$

  $\alpha_1|0,0\rangle + \alpha_2|0,1\rangle + \alpha_3|1,0\rangle + \alpha_4|1,1\rangle \in H^4$ "dvojkový zápis"

  $\alpha_1|0\rangle \quad + \alpha_2|1\rangle \quad + \alpha_3|2\rangle \quad + \alpha_4|3\rangle$ "desítkový zápis"
- Axiom měření: $|i\rangle$ stav dostanu s pravděpodobností $|\alpha_i|^2$
  (u měření dostanu jenom jeden z mnoha stavů)

Probalistický registr

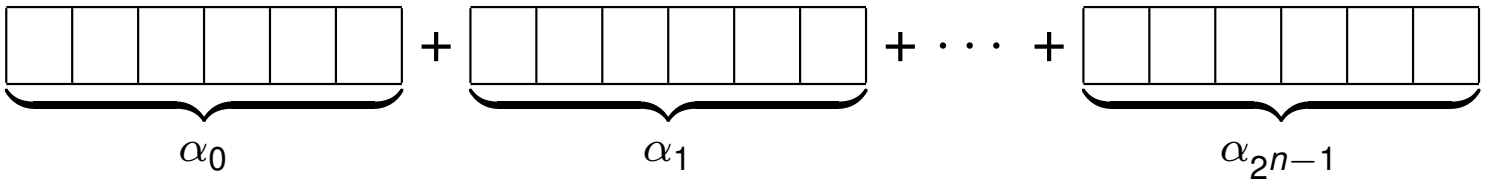
- **Klasický registr** 
  - 1 číslo z 2^{n-1}
  - pokud nějaká operace $\Rightarrow$ zase číslo z 2^{n-1}
- **Probalistický registr**  $\rightarrow$ stochastická matice $\rightarrow$



  - Z 1 čísla $\rightarrow 2^n$ možných výsledků, ale uvidíme jen jeden
  - Konstruktivní interference - probab. výpočet může být rychlejší - může existovat víc cest k výsledkům
  - Snažíme se snížit p cest, které nikam nevedou

Kvantový registr 1

- **Kvantový registr**  $\rightarrow$ unitární matice $\rightarrow$



  - Z 1 čísla $\rightarrow 2^n$ možných výsledků
  - α - amplitúdy
  - Můžou být záporné a tak některé cesty se můžou vyrušit
  - Zvýší se amplitůdy ostatních cest
  - Kromě konstruktivní interference existuji i destruktívní

Kvantová Fourierová transformace - KFT 1

- Základní vlastnosti KFT z pohledu kvantové mechaniky je, že mezi qubity vyvolává kvantovou interferenci a to buď konstruktivní nebo destruktivní.
- Konstruktivní interference v signálu zvýrazňuje jisté charakteristiky (frekvence) nad charakteristikami jinými.
- Takovým způsobem se uvádí registr do stavu, v němž naměříme jeho hodnoty s různými pravděpodobnostmi (tzn. ovlivňuje amplitudy pravděpodobností).
- Toto má zásadní vliv na praktickou použitelnost některých algoritmů.
- Abychom vyhověli požadavku unitárnosti operace definujeme kvantovou diskrétní Fourierovu transformaci (KFT) jako vývoj registru $|a\rangle = |a_0\ a_1 \ldots\rangle$ na $|c\rangle = |c_0\ c_1 \ldots\rangle$ podle :

$$|a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q}\ |c\rangle,$$

Kvantová Fourierova transformace 2

- Kde q je počet stavů registru ($0 \leq a < q$) a (a, c) jsou souřadnice prvků unitární matice a jsou rovny $\frac{1}{\sqrt{q}} e^{2\pi i ac/q}$.
- Tato matice (transformace) je základem faktorizačního algoritmu a nazývá se $\boldsymbol{A}_q$.
- Její sloupce a řádky jsou indexovány od 0 jako celá čísla odpovídající binárním reprezentacím stavů.
- Pro návrh efektivních algoritmů založených na KFT, bylo nutné samotnou KFT vymyslet efektivně.
- Shor takovou KFT navrhl pro q, které je mocninou dvou ($q = 2^l$). Pro její výpočet potřeboval jen $\mathcal{O}(l^2)$ kvantových bran, kterých jsou dva typy. Jednou je Hadamardova brána definovaná jako:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ nebo}$$

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ a } |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Kvantová Fourierova transformace 3

- Tato brána vyvíjí stav $|0\rangle$ do vyvážené superpozice všech možných 2^n stavů (pokud je aplikována na n qubitů jako $(\boldsymbol{H} \otimes \boldsymbol{H} \otimes \ldots \otimes \boldsymbol{H})\,|00\ldots0\rangle$ nazývá se Walsh-Hadamardova transformace $\boldsymbol{W}$). Hadamardovu bránu ovlivňující bit na pozici j označujeme $\boldsymbol{H}_j$.
- Druhou bránou je $\boldsymbol{S}_{j,k}$, která operuje s bity na pozicích j a k:

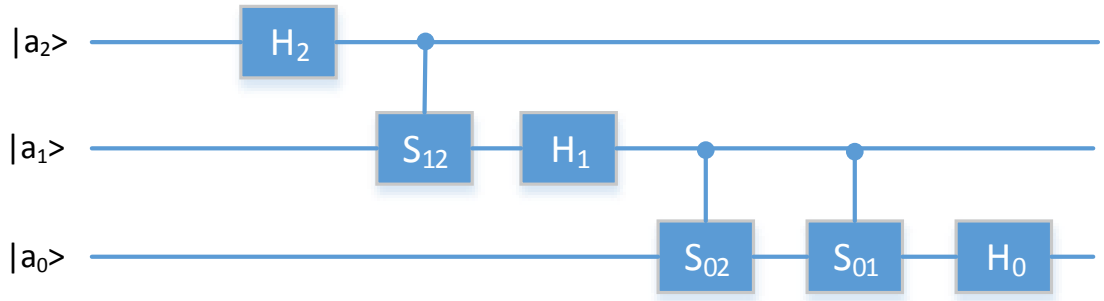
$$\boldsymbol{S}_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{k-j}} \end{pmatrix},$$

kde $\theta_{k-j} = \pi/2^{k-j}$. K provedení KFT aplikujeme brány v pořadí zleva doprava podle obecného schématu:

$$\boldsymbol{H}_{l-1}\boldsymbol{S}_{l-2,l-1}\boldsymbol{H}_{l-2}\boldsymbol{S}_{l-3,l-1}\boldsymbol{S}_{l-3,l-2}\boldsymbol{H}_{l-3}\cdots\boldsymbol{H}_1\boldsymbol{S}_{0,l-1}\boldsymbol{S}_{0,l-2}\cdots\boldsymbol{S}_{0,2}\boldsymbol{S}_{0,1}\boldsymbol{H}_0.$$

Kvantová Fourierová transformace 4

- Například pro tři bity ($l = 3$) aplikujeme brány $\boldsymbol{H}_2\boldsymbol{S}_{1,2}\boldsymbol{H}_1\boldsymbol{S}_{0,2}\boldsymbol{S}_{0,1}\boldsymbol{H}_0$.
- Tato operace vrací registr bitově převrácený $\Rightarrow$
- pro dokončení KFT výsledný registr bitově investujeme nebo čteme z opačné strany (implementačně jednoduchá operace).



- Obvod kvantové Fourierovy transformace: pro $l = 3$; rekurzivně lze obvod rozšiřovat podle obecného vzorce.
- Brány se provádějí zleva doprava (odpovídá uvedenému zápisu)
- Brány $S_{j,k}$ operují nad dvěma qubity.

Kvantová Fourierová transformace 5

- Hadamardova rotace $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

  $|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

  $= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

  $= |0\rangle$ dokáže se vrátit na začátek

Faktorizace, Shorův algoritmus 1 - úvod

- Shorův algoritmus na faktorizaci velkých celých čísel využívá kvantový paralelismus.
- Na kvantovém počítači běží v asymptotickém čase $\mathcal{O}(L^2 \log L \log\log L)$, kde L je počet bitů faktorizovaného čísla. Čas je omezen shora polynomem.
- Algoritmus nehledá přímo součinitele, převádí faktorizaci čísel se na hledání **periody určité periodické funkce**.
- Pro faktorizované číslo N vytvoříme periodickou funkci

$$f_{y,n}(a) = y^a \bmod n,$$

kde y je náhodné celé číslo nesoudělné s n.

Faktorizace, Shorův algoritmus 2 - úvod

- Na této funkci je zajímavá její periodicita. Její perioda modulo n se obvykle značí r. Protože je každá r-tá hodnota funkce stejná ($f_{y,n}(a) = f_{y,n}(a+r)$), platí

$$y^r \equiv 1 \bmod n.$$

- Po úpravě

$$(y^{r/2} - 1)(y^{r/2} + 1) \equiv 0 \bmod n,$$

- kde r je sudá perioda (pro lichou náhodně vybíráme jiné y).
- Dělení členů na levé straně rovnice číslem n je bezezbytkové. Proto, pokud není triviálně $y^{r/2} \equiv \pm 1 \bmod n$, pak musí mít některý z členů na levé straně společný faktor s n.
- Tímto se vlastně úloha převádí na problém hledání největšího společného dělitele (gcd) čísel $(y^{r/2} - 1, n)$ a $(y^{r/2} + 1, n)$. EA řeší tento problem efektivně i na klasickém počítači.

Faktorizace, Shorův algoritmus 3 - úvod

Příklad: Faktorizujme číslo $n = 21$ na součin jeho prvočinitelů. Pak si zvolíme $1 < y < 21$ takové, že $gcd\,(y, 21) = 1$.

- Potom množina čísel y je 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.
- Z ní si náhodně zvolíme $y = 10$.
- Nyní chceme zjistit periodu funkce $f_{y,N}(a) = 10^a \bmod 21$.
- Funkční hodnoty pro celé $a = 1, 2, \ldots$ jsou $10, 16, 13, 4, 19, 1, 10, 16, \ldots$.
- Tato funkce má sudou periodu 6 a nevrací triviální faktory.
- Jestliže $y^{r/2} = 1000$, pak chceme ověřit, zda $1000 \equiv^{?} \pm 1 \pmod{21}$. To neplatí, protože $999 \nmid 21$ a $1001 \nmid 21$. Pokud by se tak stalo, museli bychom zvolit jiné y.
- Na závěr nalezneme faktory pomocí $gcd\,(1001, 21) = 7$ a $gcd\,(999, 21) = 3$.

Faktorizace, Shorův algoritmus 4 - úvod

- Dále např. pro $y = 20$ algoritmus neuspěje, protože perioda $r = 2$ (20,1,20,1,...). Zajímá nás tedy, zda $20 \equiv^{?} \pm 1 \pmod{21}$ a vidíme, že $21 \mid 21$.
- Nyní nám zbývá problém - **jak vypočítat efektivně periodu** r dané funkce.
- Tento problém není klasicky řešitelný v polynomiálním čase. Shor ale ukázal, že na kvantovém počítači periodu efektivně nalézt lze s využitím kvantového paralelismu.

Algoritmus

- Připravme si dále kvantový registr, který bude mít 2 části nazvané $R1$ a $R2$, a jehož stav budeme zapisovat $|r1, r2\rangle$.
- Krok 1: Zvolíme si náhodně y nesoudělné s n a vybereme q, pro které platí $2n^2 \leq q \leq 3n^2$.

Faktorizace, Shorův algoritmus 5

- Krok 2: Připravíme kvantový registr do superpozice čísel $|\psi\rangle$ tak, že v $R1$ máme superpozici čísel 0 až $q-1$, a v $R2$ samé nuly.

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

- Krok 3: Z hodnot v $R1$ vypočteme (paralelně) funkční hodnoty funkce $f_{y,n}(a)$ a zapíšeme je do $R2$.

$$|\Psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, y^a \bmod n\rangle.$$

- Krok 4: Změříme pouze část $R2$ jako hodnotu k. Tím uvedeme celý registr do superpozice čísel, které mají funkční hodnotu k a představují projekci registru, v němž předtím byly vyváženě zastoupeny všechny hodnoty periodické funkce $f_{y,n}(a)$.

$$|\Psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a', k\rangle,$$

Faktorizace, Shorův algoritmus 6

- kde $A = \{a' : y^{a'} \bmod n = k\}$ a $|A|$ je počet prvků množiny A.
  Použijme nyní příkladu s faktorizací čísla 21 a uvědomme si, v jakém stavu se registr před tímto krokem nacházel. Po 3. kroku byl registr v superpozici
  $\frac{1}{\sqrt{22}}(|0,1\rangle + |1,10\rangle + |2,16\rangle + ...4\rangle + |5,19\rangle + |6,1\rangle + \ldots + |21,13\rangle)$.
  Provedením měření podle kroku 4 se vyselektují pouze stavy příslušející naměřené hodnotě (se stejnou vlastní hodnotou).
  Podle výsledku měření tak dostaneme jednu z 6 možných superpozic:

Faktorizace, Shorův algoritmus 7

Změřeno	Nový stav
1	$\frac{1}{2}(\|0,1\rangle + \|6,1\rangle + \|12,1\rangle + \|18,1\rangle)$
10	$\frac{1}{2}(\|1,10\rangle + \|7,10\rangle + \|13,10\rangle + \|19,10\rangle)$
16	$\frac{1}{2}(\|2,16\rangle + \|8,16\rangle + \|14,16\rangle + \|20,16\rangle)$
13	$\frac{1}{2}(\|3,13\rangle + \|9,13\rangle + \|15,13\rangle + \|21,13\rangle)$
4	$\frac{1}{\sqrt{3}}(\|4,4\rangle + \|10,4\rangle + \|16,4\rangle)$
19	$\frac{1}{\sqrt{3}}(\|5,19\rangle + \|11,19\rangle + \|17,19\rangle)$

- K odhadu periody z těchto stavů bylo by potřeba první 3 kroky několikrát opakovat ke změření několika hodnot. Není to ale možné v důsledku různého počátečního offsetu periody u každého výsledku měření.
  Tento offset nám neumožňuje mít při opakovaných měřeních jistotu, že dosáhneme stejného výsledku a tak určíme periodu jednoznačně.
  To proto, že pravděpodobnosti změření všech 6 výsledků jsou přibližně stejné. Pro správné určení periody je zapotřebí ji nějakým způsobem zvýraznit tak, aby nebyla závislá na počátečním offsetu.

Faktorizace, Shorův algoritmus 8

- Krok 5: Proto nyní provedeme kvantovou Fourierovu transformaci (QFT) na $R1$ a výsledek vrátíme tamtéž.

$$|\Psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c/q} |c, k\rangle.$$

  QFT převedla stav registru $|a'\rangle$ na $|c\rangle$, tentokrát již s různými amplitudami. Ty stavy, které se vyskytují v okolí násobků převrácené periody $1/r$ tak naměříme s větší pravděpodobností než ty, které jsou od násobků více vzdáleny. Důležité je, že stav $|a'\rangle$ obsahující problematický offset periody funkce se přesunul do fázového faktoru.

- Krok 6: Nyní registr změříme s výsledkem c'. Abychom byli schopni určit periodu, je nutné kroky 2 - 6 opakovat do chvíle, než máme k dispozici dostatek vzorků, které jsou s velkou pravděpodobností v okolí různých násobků převrácené periody a které jednoznačně umožňují určit periodu. Pokud tyto násobky označíme λ, pak c' je nějakým násobkem λ výrazu q/r, tj. $c' = \lambda \frac{q}{r}$. Po úpravě dostaneme $c'/q = \lambda/r$, pro $\lambda \in \mathbb{Z}^+$. Odhad, jaký násobek λ byl naměřen, se provádí rozvojem c'/q do řetězcového zlomku.

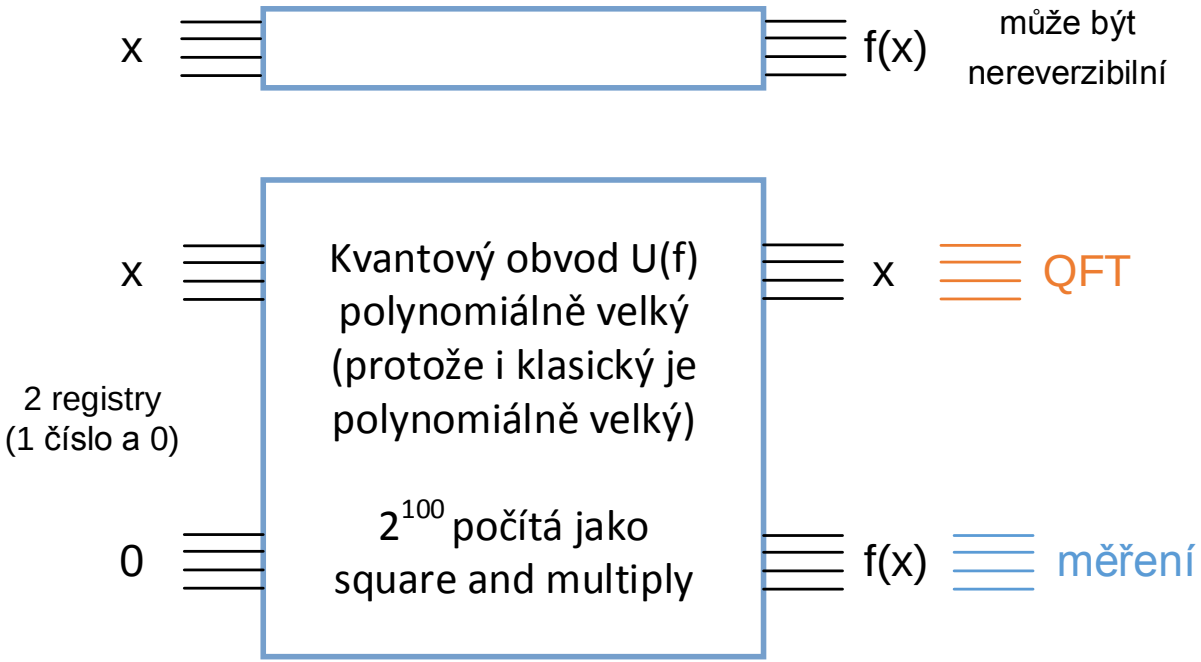
Faktorizace, Shorův algoritmus 9

- Krok 7: Když je známa hodnota r, jsou již klasicky EA vypočteny největší společné dělitele $(y^{r/2}-1, n)$ a $(y^{r/2}+1, n)$.
- Protože je tento algoritmus pravděpodobnostní povahy, není zaručeno, že na konci dostaneme dva užitečné faktory, které nás zajímají. Například špatná volba y v prvním bodě algoritmu může vést k dosažení triviálních řešení rovnice $(y^{r/2}-1)(y^{r/2}+1) \equiv 0 \bmod n$.
- Vidíme, že Shorův algoritmus je vlastně kombinací dvou metod. Jednak hledání periody funkce $f_{y,n}(a)$ na kvantovém počítači, a jednak hledání největších společných dělitelů dvou čísel na klasickém počítači. Běžící časy obou metod se asymptoticky sčítají pouze na polynomiální složitost. Je možné zhruba odhadnout, že pokud je složitost řádu L^2, pak například faktorizace 768 bitového čísla by při délce jednoho výpočetního kroku kolem 100 cyklů trvalo na 100 MHz kvantovém počítači řádově jednotky sekund. Je jasné, že pokud by se podařilo takový algoritmus použít na skutečném kvantovém počítači, dostali bychom do rukou nástroj na prolamování většiny dnes používaných kryptoschémat.

Faktorizace, Shorův algoritmus 4

- Faktorizace se dá řešit hledáním řádu prvku v grupě
- $x^2 \equiv 1 \pmod{N}$, pro $1 < x < N$ $\quad *$
  - $\leftarrow$ když to umím řešit, potom umím faktorizovat
- $x^2 - 1 = l \cdot N$
- $(x+1)(x-1) = l \cdot N$, kde $l < N$
- Alespoň jedna závorka musí sdílet faktor s N (platí $l < N$)
- $\gcd(x \pm 1, N) \rightarrow$ faktor N
- Vygenerované číslo k je buď faktor N nebo k a N jsou nesoudělná
- $k^r \equiv 1 \pmod{N}$
  - $r \rightarrow$ sudé, pravděpodobnost $p \geq 1 - \frac{1}{2^z}$, že nalezený řád je sudý
  - z je počet faktorů N
- $x = k^{\frac{r}{2}}$ dosadíme do $*$ a získáme řešení

Faktorizace, Shorův algoritmus 5



- QFT - tady se da jít vždy zpátky (pamatuje si cestu) - lineární operátor $U(f)$
- $U(f) : |x, 0\rangle \rightarrow |x, f(x)\rangle$
- $f(x) = k^x \pmod N$ je periodická funkce

Faktorizace, Shorův algoritmus 6

- V superpozici dostanu k na všechna x z nějakého rozmezí $\rightarrow$
- $\sum_{x=0}^{2^n-1} |x,0\rangle \xrightarrow{H} \sum_{x=0}^{2^n-1} |x,f(x)\rangle$
- $f(x) = k^x \pmod N$ máme teď vše, ale měřením to nemusíme dostat (stejně bychom to mohli dostat klasicky) $\Rightarrow$
- změříme jenom něco ($f(x')$) - $\sum_{x=0}^{2^n-1} |x', f(x')\rangle$,
  kde $x' \in \{x' : k^{x'} \pmod N = y\} \rightarrow$ dostáváme superpozici stavů, které to splňuji
- $|1,8\rangle + |2,6\rangle + |3,8\rangle + |4,6\rangle + \cdots$ měříme ($|2\rangle + |4\rangle \cdots |6$)
- $\sum |l + jr|y\rangle$, l je offset a jr značí $\forall$ periody ($\sum |2 + j2|6\rangle$)
- $\forall\ x'$ obsahují v sobě periodicitu
- potřebuji odstranit offset $\Rightarrow$ KFT, která "vynuluje" vše, kromě násobků periody

Kvatová Fourierova transformace - QFT

- $\sum |l + jr\rangle \quad \rightarrow \text{QFT} \rightarrow \quad \sum_{j'} |j' \frac{2^m}{r}\rangle$
- $j' \frac{2^m}{r}$ transformace přes grupu Z_{2^m}
- teď změříme j' a dostaneme $a = j'_a \frac{2^m}{r}$, ale nevíme r a j'_a
- $r = \frac{2^m}{\gcd(a, 2^{2m})}$ pro $\gcd(j'_a, r) = 1$
- j'_a nevím, pouze předpokládám a z toho dostáváme r, zbytek se dopočítá
- pokud to selže (málo pravděpodobné) tak neplatí gcd
- v případě selhání opakuji postup znovu