JEMNÝ ÚVOD DO KVANTOVÉHO POČÍTÁNÍ (3)

Od bitů ke qubitům

Jedním z témat nejčastěji zmiňovaných v souvislosti s kvantovými počítači je Shorův faktorizační algoritmus. U kryptologů vyvolává mírné mrazení v zádech, zároveň však zajišťuje uznání i materiální podporu vědcům, kteří se pokoušejí o praktické konstrukce kvantových počítačů.

Z hlediska metodiky provádění výpočtů na kvantových počítačích je nejdůležitější částí Shorova algoritmu jistý druh Fourierovy transformace, který umožňuje efektivně využít možností nabízených kvantovým paralelismem – i přes to, že při finálním měření výsledků lze od kvantového počítače získat jen jednu z mnoha paralelně vypočtených hodnot (viz předchozí díly). Právě této transformaci a způsobu jejího použití zde věnujeme hlavní pozornost – to nám totiž umožní pochopit, jaká síla a v jaké formě se lidstvu může dostat v podobě kvantových počítačů do rukou.

KVANTOVÁ FOURIEROVA TRANSFORMACE

Kdyby se Jean Baptiste Joseph Fourier dožil dnešní doby, asi by na sebe byl hodně pyšný. Vždyť nějaký druh zobecněné Fourierovy transformace nalezneme v současné fyzice takřka na každém kroku. Proto ani příliš nepřekvapí, že to, co z matematického hlediska představuje „jen" další z mnoha analytických transformací, stojí i za možností účelného využití kvantového paralelismu.

Jak již víme, neposkytne nám fenomén kvantového paralelismu oproti klasickému počítači (s generátorem náhodných čísel) v zásadě nic nového, pokud nedokážeme využít toho, že kvantový počítač poctivě prochází všechny paralelní cesty výpočtu. Kolaps kvantového systému při měření nám ovšem staví do cesty jasnou hranici, za kterou již výhodu kvantového paralelismu zřejmě využít nelze. Musíme se o to tedy pokusit dříve, než provedeme finální operaci měření (dodejme, že určitá dílčí měření jsou možná, a někdy dokonce i žádoucí už během výpočtu).

Povšimneme-li si přitom dobře způsobu zápisu stavového vektoru kvantového systému v Hilbertově prostoru, přímo se nám nabídne možnost využít jevu známého ve fyzice jako *interference*. Z matematického hlediska se jeví interferenční chování například jako součet komplexních čísel s různou hodnotou fázového posuvu (argumentem). Mějme dvě komplexní čísla c_1 a c_2, kde $c_1 = |c_1|*e^{i\alpha}$ a $c_2 = |c_2|*e^{i\beta}$, a položme $c_3 = c_1+c_2$. O absolutní hodnotě $|c_3|$ víme, že maximální ($= |c_1|+|c_2|$) bude pro $\alpha = 2k\pi+\beta$, kde $k \in \boldsymbol{Z}$, zatímco minima ($= ||c_1|-|c_2||$) bude nabývat pro $\alpha = (2k+1)*\pi+\beta$.

To jistě nevypadá, přinejmenším pro středoškoláky, jako žádný zázrak, přitom však je toto triviální pravidlo základem většiny algoritmů pro kvantové počítače. Připomeňme ještě, že druhá mocnina absolutní hodnoty komplexních koeficientů v superpozici vlastních stavů kvantového systému určuje rozdělení výsledků získaných případným měřením takového stavu. S využitím vlivu fázového posuvu tak můžeme nechat několik výsledků získaných paralelním výpočtem vzájemně interferovat a tím ovlivnit rozdělení finálně naměřených hodnot. Zde si ukážeme konkrétní postup využívající určitého druhu Fourierovy transformace.

OPERÁTOR U_{FT}

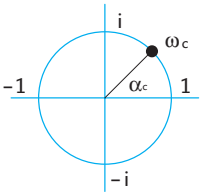
Označme $q = 2^m$. Bylo ukázáno (například v [4]), že pro tento tvar čísla q lze najít určitou kvantově schůdnou unitární transformaci, jejíž operátorovou matici budeme značit $\boldsymbol{U_{FT}}$. Tato matice operuje nad stavy m-qubitového registru (m lze volit dle potřeby), které představují prvky Hilbertova prostoru $\boldsymbol{H_q}$. Tvar matice zde pro zjednodušení uvádět nebudeme, poznamenáme pouze, že při praktické realizaci se tento operátor obvykle nezapisuje přímo, ale jako postupná aplikace několika dílčích operátorových matic ([6], [4]).

Pro náš účel jsou podstatné zejména vlastnosti této transformace s ohledem na interferenční chování kvantového systému. Mějme m-qubitový registr ve stavu $|\psi\rangle = 1/(q^{1/2})\sum_{a=0}^{q-1}|a\rangle$.

V tomto zápisu, který zde budeme často používat, chápeme hodnotu a jako celé číslo, kterým zároveň označujeme a-tý vlastní stav daného registru. Pracujeme tedy s prostorem, jehož bázové vektory značíme symbolicky jako $|a\rangle$ pro čísla $0 \le a < q$. Podívejme se nejprve, jak působí operátor $\boldsymbol{U_{FT}}$ na vybraný vlastní stav $|a\rangle$. Zde dostáváme $\boldsymbol{U_{FT}}|a\rangle = 1/(q^{1/2})\sum_{c=0}^{q-1}e^{2\pi iac/q}|c\rangle$.

Přepíšeme-li výsledek provedené transformace do základního superpozičního tvaru, jaký jsme použili v prvním dílu, dostaneme $\boldsymbol{U_{FT}}|a\rangle = \sum_{c=0}^{q-1}\omega_c|c\rangle$, kde $\omega_c = 1/(q^{1/2})\, e^{2\pi iac/q}$.

Vidíme, že jsme obdrželi vyváženou superpozici vlastních stavů (každý stav bude při měření pozorován se stejnou pravděpodobností $1/q$), jejíž koeficienty se liší právě svými fázovými posuvy. Tuto situaci ilustruje obrázek 1, který znázorňuje jeden vybraný koeficient ω_c. Takto připravený stav zde pro nás bude klíčem k využití interference mezi paralelně probíhajícími výpočty.



$\omega_c = 1/q^{1/2}\, e^{2\pi iac/q}$,
$\alpha_c = 2\pi ac/q$,
$|\omega_c| = 1/q^{1/2}$

Obr. 1. Znázornění superpozičního koeficientu pro vybraný stav $|c\rangle$

HLEDÁNÍ PERIODY FUNKCE

Mějme funkci f představující zobrazení $f: \boldsymbol{Z} \to \boldsymbol{Z}$. O této funkci řekneme, že je *periodická s periodou r*, pokud existuje $r > 0$ takové, že pro všechna $x \in \boldsymbol{Z}$ platí $f(x+r) = f(x)$. Ukážeme si, jak lze na kvantovém počítači s využitím kvantového paralelismu a interferenčního chování najít pro danou periodickou funkci její periodu r.

Označme obor hodnot funkce f jako $H(f)$. Pro jednoduchost zde budeme předpokládat, že $H(f)$ lze přímo chápat jako množinu všech binárních řetězců délky t (v opačném případě bychom ještě museli dodefinovat způsob kódování obrazů funkce f do množiny binárních řetězců délky $\lceil \log_2 |H(f)| \rceil$). Dále odhadneme q ve tvaru $q = 2^m$, tak aby $q >> r$ (například $q \sim r^2$, při dostatečně velkém očekávaném r). Pro zjednodušení zde budeme předpokládat, že se nám podařilo odhadnout q přímo jako násobek periody, takže platí $r|q$. To je sice z praktického hlediska nerealistické, pro účely výkladu však názornější.

Pro zamýšlený výpočet budeme potřebovat kvantový počítač se dvěma kvantovými registry. Bázové vektory prostoru popisujícího stav tohoto počítače budeme zapisovat ve tvaru $|a\rangle|b\rangle$, kde a je celé číslo odpovídající vlastnímu stavu prvního registru a b je celé číslo odpovídající vlastnímu stavu druhého registru. První registr bude mít délku m qubitů, druhý délku t qubitů. Báze je tak symbolicky tvořena množinou vektorů $\{|a\rangle|b\rangle: 0 \le a < 2^m, 0 \le b < 2^t\}$.

Vidíme, že náš hypotetický kvantový počítač bude potřebovat alespoň $m+t$ qubitů. V praxi to bude patrně o něco více, konkrétní nárůst závisí mimo jiné také na tom, zda použijeme některou z metod opravy chyb (praxe ukazuje, že to bude asi nezbytné) a zda budeme od počítače vyžadovat ještě nějaké výpočty v rámci přípravy a finalizace úlohy.

Výklad omezíme pouze na úlohu hledání periody, a to za předpokladu, že kvantový počítač pracuje tak ideálně, jak si jej zde matematicky popisujeme. Stojí za zmínku, že v podobném duchu byl proveden i experiment [7], v němž autoři pro rozklad čísla 15 vystačili se sedmi qubity (tři na první registr a čtyři na druhý), a navíc v jejich úloze platí $r|q$ (nejvyšší řád v $\boldsymbol{Z}_{15}^*$ je $2^2 = 4$).

Naším prvním krokem bude připravit počítač do stavu
$|\psi_1\rangle = 1/(q^{1/2}) \sum_{a=0}^{q-1} |a\rangle|0\rangle$.

Nyní na první registr aplikujeme funkci f, jejíž periodu hledáme, a výsledek uložíme do druhého registru. Tento výpočet lze vždy udělat reverzibilně, neboť původní vstupní hodnotu si uchováváme v prvním registru. V tomto okamžiku využíváme masivního kvantového paralelismu, neboť vstupem prováděné transformace bude superpozice několika (q) vlastních stavů. Výsledkem bude stav $|\psi_2\rangle = 1/(q^{1/2}) \sum_{a=0}^{q-1} |a\rangle|f(a)\rangle$.

V této fázi některé popisy Shorova algoritmu (například [8]), jehož část si zde v mírně zobecněném pohledu předvádíme, zejména z didaktických důvodů zařazují měření na druhém registru. Tímto krokem by byla jeho hodnota determinována na nějaké $f(x)$, pro $x < r$, a v prvním registru bychom dostali superpozici pro vlastní stavy ve tvaru $|x+kr\rangle$, kde k je nějaké kladné celé číslo, $x+kr < q$. S ohledem na konzistentnost celého kvantového systému totiž musí měření na určité části počítače vyvolat zároveň projekci zbývající (dosud nedeterminované) části systému do stavu slučitelného s naměřenou hodnotou (naše dělení na registry je z hlediska vlastních stavů systému jen pomyslná konstrukce pro lepší přehlednost; pozorný čtenář jistě zaregistroval souvislost s provázanými stavy zmíněnými v prvním dílu).

Ve vlastním popisu Shorova algoritmu [6] se však měření v této fázi nepředpokládá (v první praktické realizaci [7] rovněž nebylo použito) a ani pro naše účely jej zde nebudeme zavádět. Jako následující krok hned provedeme transformaci $\boldsymbol{U}_{FT}$ na prvním registru (opět proběhne paralelně pro všechny vlastní stavy v aktuální superpozici). Tím dostaneme stav
$|\psi_3\rangle = 1/q \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle|f(a)\rangle$.

Díky periodičnosti funkce f nám na koeficientech v superpozici odpovídající stavu $|\psi_3\rangle$ dochází k interferenci. Pro určitou hodnotu $|c\rangle$ v rozvoji uvedeného výrazu interferují koeficienty stavů $|c\rangle|f(a_1)\rangle$ s koeficienty stavů $|c\rangle|f(a_2)\rangle$, kde $r|(a_1-a_2)$. Položíme-li $x = a \bmod r$, můžeme psát $|c\rangle|f(a_1)\rangle = |c\rangle|f(a_2)\rangle = |c\rangle|f(x)\rangle$. Jde tedy stále o tentýž vlastní stav, který se ve výrazu pro $|\psi_3\rangle$ vyskytuje na několika místech. Fyzikální proces interference zde vnímáme jako součet komplexních koeficientů vyskytujících se u stejných vektorů vlastních stavů v rozvoji naznačeného součtu. Záleží přitom právě na vzájemném fázovém posuvu těchto koeficientů, jestli bude tato interference konstruktivní (zastoupení daného vlastního stavu ve stavu $|\psi_3\rangle$ se posílí), nebo naopak destruktivní (zastoupení se oslabí).

Zdá se, že obecný fyzikální jev interference je jedním z nejlepších nástrojů k využití síly ukryté v kvantovém paralelismu.

Pro lepší představu si napišme superpoziční koeficient $\omega_c^{[x]}$, který přísluší určitému vlastnímu stavu $|c\rangle|f(x)\rangle$. Zde můžeme odvodit
$\omega_c^{[x]} = e^{2\pi i x c/q} / q \sum_{k=0}^{v} e^{2\pi i k r c/q}$, kde $v = q/r - 1$.

Díky zvoleným vstupním podmínkám zde dostáváme učebnicové hodnoty uvedených koeficientů, a to:

- $\omega_c^{[x]} = e^{2\pi i x c/q}/r$, pro $q|rc$,
- $\omega_c^{[x]} = 0$ v ostatních případech.

Vidíme, že transformace $\boldsymbol{U}_{FT}$ nám spolu s interferencí umožnila, aby se hledaná perioda r „otiskla" do rozdělení výsledků měření na prvním registru. S využitím vypočtených hodnot $\omega_c^{[x]}$ můžeme stav kvantového počítače $|\psi_3\rangle$ přepsat jako
$|\psi_3\rangle = 1/r \sum_{x=0}^{r-1} \sum_{(c:\, q|rc)} e^{2\pi i x c/q} |c\rangle|f(x)\rangle$.

Pokud v tomto stavu provedeme měření prvního registru, potom s jistotou dostaneme hodnotu c splňující podmínku $q|rc$. Měřením jsme tedy dostali nějaké celé číslo c, které je (díky podmínce $r|q$) celočíselným násobkem podílu q/r, tedy $c = b*(q/r)$, kde $b \in \boldsymbol{Z}$. Pokud platí, že $b > 0$ a zároveň $gcd(b, r) = 1$, můžeme hodnoty b a r najít tak, že zlomek c/q jednoduše zkrátíme do základního tvaru. Stane-li se, že změříme hodnotu c pro nevyhovující b (což poznáme tak, že nalezené r nebude periodou funkce f), opakujeme postup znovu od začátku. Lze ukázat (podobným postupem jako v [6]), že v počtu opakování úměrném hodnotě $log\ log\ r$ tímto způsobem s vysokou pravděpodobností najdeme hledanou periodu r.

Snad ještě malou poznámku, jak vlastně máme použitý operátor $\boldsymbol{U}_{FT}$ nazývat. Jmenná konvence je zde bohužel nepříliš vypilovaná, avšak není pro pochopení této transformace ani příliš podstatná, takže se přesnému pojmenování vyhýbáme a uvádíme ho zde jen jako okrajovou informaci. Najdeme prameny, které volí prostý název *Fourierova transformace* (odtud FT v indexu operátorové matice), což je sice příliš obecné, ale zároveň nemůžeme šlápnout vedle (nějaký druh Fourierovy transformace to z nějakého pohledu asi bude).

Smělejší autoři používají název FFT, tedy *rychlá Fourierova transformace*. Z pohledu superpozice získané aplikací na vybraný vlastní stav to opravdu intuitivně připomíná vzorec pro numerický výpočet FFT. Výsledek ovšem dostáváme jako celkový kvantový stav systému, což je oproti klasické FFT poněkud náročnější na představivost, takže někteří jedinci sahají při ústupovém manévru k označení QFT – *kvantová Fourierova transformace*.

Patrně největší odvážlivci se na celou věc dívají z pohledu na charakter výsledku, který získáme měřením na transformovaném registru. Zde nám situace připadá, jako bychom si vybírali hodnoty z klasické FFT počítané „pozpátku" (tedy od harmonických koeficientů k funkčním hodnotám). Na základě tohoto náhledu pak tito bijci (mezi nimi například i autoři proslulého experimentu [7]) sahají k označení *inverzní QFT*. Fyzici sami jsou v těchto otázkách silně pragmatičtí a do sáhodlouhého rozboru jmenné konvence se příliš nehrnou. Zatím tedy nezbývá, než si vybírat z nabídnutého spektra podle vlastního gusta.

Starý trik v novém aranžmá

Takto bychom mohli nazvat Shorův algoritmus z pohledu teorie čísel. Jeho hlavní přínos totiž spočívá jen v efektivním využití schopností kvantových počítačů k nalezení

periody diskrétní funkce, což na klasických počítačích není dnes (pro velké periody) schůdná úloha. Vše ostatní již jede ve starých kolejích.

Mějme celé číslo n, $n = \prod_{j=1}^{k} p_j^{dj}$, kde $\{p_j\}$ jsou jeho hledané prvočíselné faktory. Definujme $f(x) = g^x \bmod n$, kde $g \in \mathbf{Z}_n^*$, jako periodickou funkci f s periodou r rovnou řádu prvku g v multiplikativní grupě $\mathbf{Z}_n^*$. Hlavním krokem Shorova algoritmu je využití výše popsaného postupu k nalezení neznámé periody r. Tím jsme získali řád prvku g a můžeme psát $g^r \equiv 1 \pmod n$. Jestliže jsme získali sudé r, můžeme položit $y = g^{r/2} \bmod n$ a psát $y^2 - 1 \equiv 0 \pmod n$. Odtud plyne $n|(y-1)(y+1)$.

Pokud se nám podařilo získat $y \neq n-1$, můžeme najít jeden z netriviálních faktorů n (ne nutně prvočíselný pro n složené z více prvočísel) jako $gcd(n, (y-1))$. Je-li n složeno právě ze dvou prvočísel, máme hotovo. V opačném případě pokračujeme v rozkladu získaných faktorů tak dlouho, dokud nedojdeme k prvočíselným hodnotám (lze použít klasické pravděpodobnostní algoritmy pro test prvočíselnosti). Všechny uvedené výpočty vyjma hledání periody probíhají již na klasickém počítači.

Lze odvodit (viz [6]), že pravděpodobnost, že nalezená perioda povede k získání netriviálního faktoru čísla n, je $1-1/2^{k-1}$, kde k je počet prvočíselných faktorů. Pro praxi z toho plyne jednak poznatek, že tímto postupem nelze faktorizovat čísla tvořená mocninou jediného prvočísla (s takovými tvary si ovšem hravě poradí algoritmy pro klasický počítač), jednak to, že pro běžný modul RSA (kvůli kterému celý algoritmus vlastně vznikl) budeme s padesátiprocentní pravděpodobností úspěšní. Pokud výpočet v tomto bodě neuspěje, je třeba provést novou volbu prvku g a hledání periody opakovat.

Po chvilce zamyšlení asi zjistíme, že se zde opět opakuje myšlenka využití netriviálních kořenů kvadratické kongruence. Na stejném principu je založena také klasická metoda NFS (viz popis v [2]), liší se pouze způsob, jakým tyto kořeny hledáme. Dodejme ještě, že tak pracoval i předchůdce NFS, metoda QS, a že stejnou metodu nalezneme také u optického zařízení Twinkle (které však kvantovou mechaniku k výpočtu přímo nepoužívá), což je v podstatě specializovaný akcelerátor metod QS a NFS (viz [2]). „Starý trik" se tedy stále osvědčuje.

Shorův algoritmus

Vlastní Shorův algoritmus tak, jak je popsán v práci [6] (tento zápis lze ještě optimalizovat), vidíte na obrázku 2. Všechny funkčně důležité části jsme již představili, takže se omezíme pouze na hlavní odlišnosti od našich „školních" příkladů. Asi hlavní rozdíl spočívá v tom, že nejsme schopni přesně volit q tak, aby $r|q$. Proto nám po interferenci nevyjdou superpoziční koeficienty tak ostře jako v našem příkladu výše. Pro q splňující podmínku $n^2 \leq q < 2n^2$ lze však ukázat, že při polynomiálním počtu opakování celého postupu získáme měřením prvního registru s vysokou pravděpodobností hodnotu c vyhovující vztahu $|c/q - b/r| \leq (2q)^{-1}$, kde b a r jsou celá čísla (r je hledaná perioda) a $gcd(b, r) = 1$. Odtud pak najdeme racionální číslo b/r, $r < n$, jako řetězový zlomek, kterým budeme aproximovat podíl c/q. Tento výpočet opět probíhá na klasickém počítači a má nejvýše polynomiální složitost.

Z pohledu teorie čísel je základ Shorova algoritmu postaven na stejné myšlence, jakou nalezneme u zatím nejlepších klasických metod.

Vstup: složené číslo n
Výstup: netriviální faktor p, $p|n$
Postup:
1. Příprava
- zvolme celé číslo q, $n^2 \leq q < 2n^2$, $q = 2^m$, $m \in \mathbf{Z}$
- zvolme celé číslo g, $g < n$, $gcd(g, n) = 1$
- definujme $f(x) =^{def} g^x \bmod n$

2. Výpočet na kvantovém počítači
- $\mathbf{start} \rightarrow |\psi_1\rangle = 1/(q^{1/2}) \sum_{a=0}^{q-1} |a\rangle|0\rangle$
- $|\psi_1\rangle \rightarrow |\psi_2\rangle = 1/(q^{1/2}) \sum_{a=0}^{q-1} |a\rangle|f(a)\rangle$
- $|\psi_2\rangle \rightarrow |\psi_3\rangle = 1/q \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i ac/q} |c\rangle|f(a)\rangle$ (odpovídá aplikaci $\mathbf{U_{FT}}$ na první registr)
- změřme hodnotu prvního registru a výsledek označme c

3. Výpočet na klasickém počítači
- aproximujme podíl c/q jako řetězový zlomek b/r, kde $r < n$
- ověřme, že r je hledaná perioda, pokud není, proveďme znovu výpočet od bodu 2 (případně od bodu 1)
- pokud je r liché, opakujme výpočet od bodu 1
- položme $y = g^{r/2} \bmod n$
- pokud $y = n-1$, opakujme výpočet od bodu 1
- vypočtěme $p = gcd(n, (y-1))$
- vraťme hodnotu p

Obr. 2. Hlavní kroky Shorova algoritmu

Celkově lze složitost Shorova algoritmu asymptoticky vyjádřit jako $O((\log n)^2(\log\log n)(\log\log\log n))$ kroků na kvantovém počítači a $O(P(\log n))$ kroků na klasickém počítači ([6]) , kde $P(x)$ je nějaký polynom. Pokud bychom tedy měli k dispozici dostatečně robustní kvantový počítač, stala by se úloha faktorizace nejspíš docela triviálním problémem. Pod pojmem robustnosti kvantového počítače zde máme na mysli jeho výbavu potřebným množstvím qubitů (lze odhadovat, že například pro modul RSA o délce 1024 bitů jich budou potřeba řádově tisíce) a schopnost pracovat koherentně v počtu kroků asymptoticky vyjádřeném výše.

Nejen faktorizace

Ačkoliv se o Shorově algoritmu hovoří zejména v souvislosti s úlohou faktorizace (z čehož se vyvozuje hrozba pro kryptografické systémy, kde je tento problém nějak využit – typicky RSA), lze obdobným způsobem využít sílu kvantových počítačů i pro řešení úlohy diskrétního logaritmu. Zde je situace sice již poněkud komplikovanější, nicméně teoretický postup existuje, má polynomiální časovou složitost a Shor jej přímo uvádí ve své práci společně s faktorizačním algoritmem (viz [6]). Navíc byl tento postup zobecněn v [3] tak, že je aplikovatelný na libovolnou cyklickou grupu. Kvantové počítače se tak stávají hrozbou i pro systémy založené na *problému diskrétního logaritmu* (DLP), a to v jeho libovolné variantě, včetně kryptosystémů na bázi eliptických křivek (založeny na problému ECDLP). Odtud plyne, že potenciální existence kvantového počítače ohrožuje téměř všechny asymetrické algoritmy. Snažit se před touto hrozbou „kličkovat" například přechodem od RSA na jiná schémata (například na bázi ECDLP) tedy nemá v dlouhodobé perspektivě valný smysl.

Groverův algoritmus

V krátkosti zmiňme ještě *Groverův vyhledávací algoritmus* ([5]), který k ovládnutí síly kvantového paralelismu rovněž využívá interferenční chování i obdobnou transformaci, jakou jsme zde představili. Cílem tohoto algoritmu je najít v netříděném seznamu určitou položku splňující zadané kritérium. Na klasickém počítači to zvládneme se složitostí $O(N)$, kde N je délka seznamu. Groverův algoritmus je schopen hledaný prvek nalézt se složitostí $O(N^{1/2})$. Zároveň bylo ukázáno, že rychlejší algoritmus pro tuto úlohu již pro kvantový počítač sestavit nelze. To mimo jiné ukazuje, že tímto způsobem (metodou zkoušení všech výsledků) nelze kvantový počítač použít k řešení všech NP úloh v kvantovém polynomiálním čase

(což by šlo, pokud bychom měli uvedený druh algoritmu se složitostí $O(\log N)$).

Přesto však tento algoritmus představuje pro některé kryptografické mechanismy obdobnou hrozbu jako Shorův algoritmus. Jde o ta schémata, jejichž luštění lze převést na útok hrubou silou (metodou zkoušení všech možností – například klíče). Každá šifra s délkou klíče (u asymetrického případu se jedná o délku privátního klíče) k bitů může být rozbita na kvantovém počítači hrubou silou se složitostí $O(2^{k/2})$ počtu zkoušek (ověření platnosti klíče musí být realizováno na kvantovém počítači). Na klasickém počítači bychom k tomu potřebovali ve střední hodnotě 2^{k-1} zkoušek.

Z tohoto pohledu můžeme říci, že Groverův algoritmus nám „půlí" efektivní délku klíče. Na rozdíl od Shorova algoritmu sice zachovává původní exponenciální složitost problému, avšak posunuje hranici bezpečné délky klíče. Například symetrická šifra s délkou klíče 80 bitů, kterou dnes považujeme s ohledem na klasické počítače za dostatečnou, už neobstojí (vzato přes asymptotickou složitost) při existenci kvantových počítačů. Standard AES je přitom se svou nejnižší podporovanou délkou klíče 128 bitů jakž takž „na hraně". Zdůrazněme však, že se jedná o teoretické odhady za předpokladu ideální výsledné složitosti luštění, která se od asymptotického odhadu může nakonec lišit o podstatný multiplikativní koeficient.

Co bude dál?

Ukázali jsme si, jak lze pomocí jisté Fourierovy transformace obejít zdánlivě nepřekročitelnou překážku v podobě kolapsu kvantového systému při měření a využít tak ohromné výpočetní síly kvantového paralelismu. Peteru W. Shorovi se navíc tímto způsobem podařilo efektivní vyřešení problému faktorizace, čímž se zasloužil o bleskový nárůst zájmu o oblast kvantových počítačů. Koncem minulého roku byly jeho teoretické závěry potvrzeny i experimentálně ([7]).

Skoro by se tedy zdálo, že klasickou asymetrickou kryptografii můžeme rovnou odepsat (a to je tu ještě další hrozba v podobě Groverova algoritmu). Jednou snad, ale dnes na to doba ještě zralá není. To, že hysterie není na místě, však neznamená, že nemá význam celou problematiku sledovat. Naopak je docela možné, že se brzo objeví další algoritmy tohoto druhu, které zájem o celou oblast ještě zvýší.

Kromě toho bude vhodné věnovat pozornost také problematice *kvantových kryptografických mechanismů* (na ty se možná časem také podíváme), které se zdají slibnou protizbraní pro okamžik, kdy kvantové počítače definitivně pohřbí některá klasická kryptoschémata. Je důležité poznamenat, že kvantová kryptografie je založena na elementárních principech kvantové mechaniky a kvantové počítače ke svému nasazení nepotřebuje. Proto se jí můžeme věnovat s předstihem už teď a být tak na příchod prvních robustních kvantových počítačů řádně připraveni.

To však stále hovoříme o poměrně vzdálené budoucnosti. Z pohledu návrhu aktuálních kryptografických systémů postačí v souvislosti s uvedenou potenciální hrozbou dodržovat dvě celkem jednoduchá pravidla. První doporučuje stavět systémy tak, aby byly co nejméně závislé na konkrétních algoritmech. To znamená zavést pro přístup ke kryptografickým mechanismům co možná nejobecnější rozhraní, která v případě potřeby umožní jejich snadnou výměnu (třeba i za schéma z oblasti kvantové kryptografie). Druhé doporučení říká, že bychom měli stále myslet na to, že každý použitý mechanismus může být (alespoň teoreticky) prolomen ze dne na den.

Tomu by také měl odpovídat krizový scénář umožňující rychlý přechod na jiné algoritmy, s pokud možno co nejmenšími ztrátami na kvalitě zabezpečení dat z předešlého období. Budeme-li tyto zásady dodržovat, pak se můžeme bez obav kochat výsledky dosaženými v oblasti kvantového počítání a fandit vědcům pracujícím v této oblasti, aniž bychom se museli třást hrůzou, že se jim to třeba jednou skutečně povede...

Kvantová mechanika nepředstavuje pro kryptografii jenom hrozbu. V podobě kvantové kryptografie nabízí i obranu.

Na úplný závěr poznamenejme, že na tento spíše matematicky pojatý seriál naváže ještě příspěvek přímo z pera kvantových fyziků, kteří vás seznámí s konkrétními fyzikálními aspekty této problematiky.

Tomáš Rosa, *autor@chip.cz*

Literatura:

[1] Archiv vědeckých článků arXiv, *http://arxiv.org/*
[2] Archiv českých článků o kryptologii, *http://www.decros.cz/bezpecnost/_kryptografie.html*
[3] Boneh, D. and Lipton, R.-J.: Quantum Cryptanalysis of Hidden Linear Functions (Extended Abstract), in Proc. of CRYPTO '95, pp. 424-437, 1995
[4] Coppersmith, D.: An Approximate Fourier Transform Useful in Quantum Factoring, IBM Research Report RC 19642, 1994
[5] Grover, L.-K.: A Fast Quantum Mechanical Algorithm for Database Search, in Proc. of STOC 1996, pp. 212-219, 1996
[6] Shor, P.-W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, extended article, 25 Jan 96, arXiv: quant-ph/9508027 v2
[7] Vandersypen, L., M., K., Steffen, M., Breyta, G., Yannoni, C.-S., Sherwood, M.-H. and Chuang, I.-L.: Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, Vol. 414, 20/27 December 2001
[8] Williams, C.-P. and Clearwater, S.-H.: Explorations in Quantum Computing, Springer-Verlag, 1998