Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS

Katedra informatiky a kvantitativních metod

Kvantový počítač

Bakalářská práce

Autor: **Petr Faja**

Informační technologie a management

Vedoucí práce: **Ing. Vladimír Beneš, Ph.D.**

Praha **2019**

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a v seznamu uvedl veškerou použitou literaturu.

Svým podpisem stvrzuji, že odevzdaná elektronická podoba práce je identická s její tištěnou verzí, a jsem seznámen se skutečností, že se práce bude archivovat v knihovně VŠ AMBIS a dále bude zpřístupněna třetím osobám prostřednictvím interní databáze elektronických vysokoškolských prací.

V Praze, dne ……. Petr Faja

Poděkování

Rád bych touto cestou poděkoval vedoucímu své bakalářské práce Ing. Vladimíru Benešovi, Ph.D. za odborné vedení, jeho cenné rady, připomínky a názory při tvorbě bakalářské práce.

Osobní poděkování patří mé rodině, přátelům a přítelkyni za jejich podporu po celou dobu studia.

Anotace

Cílem této bakalářské práce je seznámit čtenáře s problematikou kvantové teorie a její aplikace na kvantový počítač. V první kapitole bude popsán historický vývoj kvantového počítače. Následně v dalších kapitolách budou probrány jeho funkce a využití. Třetí kapitola nás provede klasickou a kvantovou kryptografií. V poslední kapitole bude srovnán klasický a kvantový počítač.

Klíčová slova: kvantová teorie, kvantový počítač, kryptografie, klasický počítač

Annotation

The main goal of the bachelor's thesis is to introduce quantum theory and show its application to quantum computers. In the first chapter, history progress of quantum computers is shown. In the following chapters, the thesis deals with main properties and functions of quantum computing. Cryptography is the main topic of the third chapter. Comparison between classical and quantum computer is completed at the end of the thesis.

Key words: quantum theory, quantum computer, cryptography, classical computer

Obsah

Úvod

V první části této práce se budeme zabývat samotným základem kvantové mechaniky a informatiky. Bude zde naznačen historický vývoj, počínaje Turingovo teorií až po samotný kvantový počítač. Podrobně se zde seznámíme s důležitostí času a prostoru (resp. paměťové kapacity).

Ve druhé části budou zavedeny pojmy *qubit* a *qubitová* brána. Pomocí lineární algebry a kvantové mechaniky se bude práce dále věnovat kvantovým algoritmům a qubitovým operacím. S využitím těchto znalostí zde bude vysvětlen princip fungování kvantových systémů, Fourierova transformace a postupný rozvoj. Následnou implementací těchto systémů se dostaneme ke konečnému využití.

Ve třetí části bude popsána kryptografie. Vysvětlí se zde tento pojem, dělení kryptografie, její principy a důležitost v historii i současnosti.

Ve čtvrté kapitole je vypsán seznam zástupců počítačů. Chronologicky jsou zde seřazeny stroje s popisem a důležitostí pro evoluci od nejstarších klasických modelů po nejmodernější kvantové počítače.

Pátá kapitola se bude zabývat klasickým počítačem a jeho srovnáním s kvantovým počítačem. Od základních jednotek *bitů* a *qubitů* přes jejich výkonnost a rychlost až po porovnání celých systémů. Tato část poukazuje na jejich výhody, nevýhody, omezení, ale i cenu.

1 Kvantová teorie

1.1 Úvod do kvantové teorie

„Svého času se v novinách objevil článek, v němž se uvádělo, že teorii relativity rozumí pouze dvanáct lidí. Nevěřím, že tomu tak kdy bylo. Možná jí rozuměl jenom jeden člověk, autor dosud nezveřejněného objevu. Ale poté, co se ostatní vědci seznámili s jeho myšlenkami, většinou tuto teorii tím nebo oním způsobem pochopili, a jistě jich bylo více než dvanáct. Na druhé straně si však myslím, že mohu klidně prohlásit, že kvantové teorii nerozumí nikdo.“
- Richard Feynman

První myšlenky o kvantové teorii se začaly objevovat na přelomu 19. a 20. století. Doposud dostačující fyzikální teorie tehdejší doby (dnes známé jako klasická fyzika) se potýkaly se stále většími problémy, které se zdály neřešitelné. Aby se krizím typu ultrafialová katastrofa[1] zabránilo, začaly se používat tzv. ad hoc hypotézy klasické fyziky. Ad hoc hypotéza je účelová hypotéza, která vzniká pro určitý případ nebo problém k výkladu skutečností, jež vyvracejí danou teorii. Toto řešení zprvu fungovalo dobře, ale s přibývajícími znalostmi o atomech a záření byly pokusy o jejich vysvětlení v klasické fyzice stále složitější a nesrozumitelnější.

S těmito poznatky se dostáváme do třicátých let 20. století, kde se oficiálně setkáváme s pojmem kvantová mechanika. Ihned se stala nepostradatelnou součástí moderní fyziky a pomohla nám lépe definovat a vysvětlit téměř všechny jevy týkající se elementárních částic v přírodě, např. strukturu DNA nebo supravodiče.

1.2 Kvantová mechanika

Pravidla kvantové mechaniky jsou jednoduchá, ale samotní experti je shledávají kontraintuitivní. Můžeme si je představit jako matematický rámec nebo soubor pravidel, která tvoří fyzikální teorii. Pro představu je uveden příklad fyzikální teorie známé jako kvantová elektrodynamika, jež popisuje s neuvěřitelnou přesností interakce mezi atomy a světlem. Kvantová elektrodynamika je vestavěna v matematickém rámci kvantové mechaniky, ale obsahuje specifické fyzikální teorie, které nejsou určeny kvantovou mechanikou. Tento vztah lze jednoduše převést na počítačový operační systém a jeho softwarovou aplikaci. Operační

[1] Ultrafialová katastrofa – absolutně černé těleso vydává záření o nekonečném výkonu

systém vytvoří základní parametry a režimy provozu, ale samotné řešení úlohy je závislé pouze na aplikaci.[15]

Nejznámější představitel kvantové fyziky, Albert Einstein, strávil poslední roky svého života nesmířen se svou vlastní teorií a až po jeho smrti se dalším generacím fyziků povedlo interpretovat jeho předpovědi tak, aby byly přijatelné pro veřejnost. Jeden z cílů Einsteinových následovníků bylo právě vyvinout prostředky pro vyostření naší intuice o kvantové mechanice a učinit její metody transparentnější pro lidskou mysl.[15]

V 70. letech 20. století projevovali fyzikové z celého světa velký zájem o kompletní kontrolu samostatného kvantového systému. Do této doby se aplikovaná kvantová mechanika zabývala hromadnými vzorky, které obsahovaly nepředstavitelné množství kvantových systémů, z nichž žádný nebyl přímo dostupný. Jako příklad lze uvést supravodič. Můžeme zkoumat pouze několik málo aspektů povahy kvantové mechaniky, ale samotné kvantové systémy nám zůstávají nepřístupné. Limitovaný přístup nám umožní pouze urychlovač částic, ale opět jen s malou kontrolou nad samotnými systémy.[15]

Do dnešní doby se lidstvu povedlo zdokonalit několik technik pro kontrolu samotného kvantové systému. Jedna z nejužitečnějších metod je tzv. „atomová past“[1], kdy se izoluje jediný atom od zbytku světa, což nám ho dovoluje zkoumat s neuvěřitelnou přesností. Pro tuto techniku byl využit řádkovací tunelový mikroskop[2], který nám umožní posun jednotlivých atomů a dle potřeby vytvoření jejich pole. S touto znalostí byla dokázána realizace elektronického zařízení v závislosti na přenosu jediného elektronu zařízením.[15]

Proč je vlastně tak důležité mít absolutní kontrolu nad samostatným kvantovým systémem? Když opomineme technologické důvody a zaměření na čistou vědu, jedná se především o „předtuchu největších mozků dané doby“ objevit něco nového. Z historie víme, že je to právě nápad, který dokázal změnit celý chod lidstva. V kvantové mechanice jsme teprve na úplném začátku a už teď sklízíme ovoce ve formě nečekaných poznatků a zjištění.[15]

1.3 Kvantové výpočty a informace

Kvantové výpočty a informace plynně navazují na teorii kvantové mechaniky. v tomto odvětví se však vědci zajímají o manipulaci kvantových soustav a jejich usměrnění pro jimi

[2] Řádkovací tunelový mikroskop – mikroskop, který zkoumá povrch vodivého vzorku pomocí změny potenciálu

požadovaný experiment, aby co nejlépe využili sílu a potenciál k aplikaci právě kvantových výpočtů a informací.

Navzdory velké snaze a úsilí vytvořit zařízení pro zpracování kvantových informací se věda prozatím nesetkala s velkým úspěchem. Malé kvantové počítače fungující na bázi několika kvantových bitů (vysvětleno v další kapitole), první prototypy kvantové kryptografie (vysvětleno ve 3. kapitole) již byly prokázány, ale nadále to zůstává velkým tajemstvím pro všechny fyziky a inženýry.

1.3.1 Klasický počítač

Než bude vysvětlen princip fungování kvantového počítače a složitost jeho algoritmů, je třeba zmínit historickou důležitost počítačové vědy.

První zmínky o vědě, která by se dala charakterizovat jako počítačová věda pochází již z 18. století před naším letopočtem. Babyloňané vytvořili sofistikovaný algoritmus, který byl vytesán do klínové tabulky. Někteří vědci se domnívají, že s prvními jednoduchými algoritmy bychom se setkali i v ranějších civilizacích.

S hliněnými tabulkami bychom to však moc daleko nedotáhli. Velkým skokem se tak dostáváme do roku 1936, kdy byl vydán uznávaným matematikem Alanem Turingem[3] převratný článek. Tento autor se zabýval abstraktním pojmem, který bychom dnes mohli nazývat programovatelný počítač. Turing psal ve své vlastní práci, že pro nás je důležitá především komplexnost výpočtu a množství zdrojů potřebných k vykonání daného úkolu. Proto je důležité vymezit si 2 velmi důležité zdroje. A to je čas a prostor. Za jeho neuvěřitelný nadhled v dané problematice je toto abstraktní zařízení pojmenováno jako *Turingův stroj*. Společně s Alonzem Churchem[4], dalším počítačovým vědcem, položil základy *Church-Turingovy teorie*. Tato teze tvrdí, že jestliže je možné provést určitou třídu algoritmů na daném fyzickém zařízení, je efektivně možné provést stejný algoritmus pomocí univerzálního Turingova stroje. Velký převrat v historii, ale nezůstal bez kritiky.[15]

Church-Turingova teorie se vůbec nezabývá efektivností řešení, a tak se začíná pracovat na určité ad hoc teorii, jak tuto tezi upravit. Tvrdíme, že řešení jednoho počítače lze efektivně provést na druhém počítači, pokud je simulace polynomiální. Jako příklad můžeme využít 3 počítače A, B a C. Počítače A a B jsou definovány polynomem 3. stupně (dále značeno jako

[3] Alan Turing – britský matematik, logik a kryptoanalytik (zakladatel moderní informatiky)
[4] Alonzo Church- americký matematik, logik, filozof a dlouholetý kolega Alana Turinga

o $(n^3))$. Pro simulaci počítače B je třeba, aby počítač A udělal 5 kroků. Z výsledku lze konstatovat, že je simulace efektivní (viz tabulka č. 1). V druhém případě budeme simulovat počítač C, počítačem A, kde počítač C využívá S jednotek času a T jednotek prostoru. Počítač A musí využít až $O(ST2^S)$ jednotek času. Pokud počítač C potřebuje $O(n^2)$ času a $O(n)$ prostoru, tak počítač A využije $O(n^3 2^n)$, aby se mu vyrovnal. Jak je patrné z výsledku, 2^n není polynom, a tak nelze zcela stoprocentně říci, že je efektivní.[15]

A simuluje B	A, B	A simuluje C
$O\ (n^3) \cdot 5$	$O\ (n^3)$	$O\ (n^3 2^n)$

Tabulka č. 1:Výsledky počítačových simulací

Proto se upouští od původního Turingova stroje a začíná se mluvit o pravděpodobnostním Turingově stroji. Tento prototyp je schopen náhodné volby v každém kroku. Lze ho jednoduše popsat jako originální Turingův stroj se zabudovaným náhodným hodem mincí (ve formě náhodné binární volby).

O pár let později, po vydání Turingova článku, byl sestrojen první počítač z elektronických komponentů, jehož teoretický model navrhl John von Neumann. Tento matematik dokázal spojit všechny potřebné komponenty, aby fungovaly na bázi Turingova stroje. Jeho přínos nalákal do vývoje počítačových komponentů spoustu velkých jmen a s klidem lze říci, že tomu je tak do dnes. Za zmínku stojí například Bardeen, Brattain a Shockley, již se zasloužili o vývoj prvního tranzistoru[4], bez kterého by se neobešel žádný počítač. Od té doby byl vývoj hardwaru „k nezastavení". Roku 1965 byl tento vývoj popsán jako *Moorův zákon*. Právě Gordon Moore prohlásil, že výkon počítače se přibližně zdvojnásobí každé dva roky při konstantní ceně. Odhadovaná platnost Moorova výroku je do 20. let 21. století. Další snaha o minimalizaci bude později velmi náročná a budeme se čím dál více potýkat s kvantovými problémy při realizaci.[15]

1.3.2 Kvantový počítač a Church-Turingova teorie

Church-Turingova hypotéza se zprvu jevila jako použitelná i pro kvantový počítač, ale postupem času se stává téměř nemožným úkolem provést simulaci efektivním způsobem. Výkon a rychlost kvantového počítače jsou velice odlišné od klasických počítačů. Jediným možným logickým řešením je najít nové výpočetní paradigma. Prvotní výzva pro Church-Turingovu hypotézu pochází z oblasti analogových výpočtů. Vědci si všimli, že mnoho analogových počítačů dokáže provést efektivní řešení tam, kde to Turingův stroj nedokáže. Naneštěstí pro analogové výpočty mizí v reálném provozu všechny jejich výhody kvůli

přítomností šumu. V tento moment přichází na scénu kvantový počítač, který je schopen tolerovat okolní šum a stále si zachovat své výpočetní výhody.[6][15]

V roce 1985 se David Deutsch pokusil navrhnout výpočetní zařízení, které by dokázalo simulovat libovolný fyzikální systém. Jelikož jsou fyzikální zákony vlastně kvantové zákony, pokusil se vše řešit pomocí kvantové mechaniky. V době, kdy David Deutsch prezentoval svůj návrh Deutschovova univerzálního kvantového počítače, sám nevěděl, jestli je dostatečně efektivní, aby simuloval libovolný fyzikální systém. Dnes již víme, že to byla první teorie, která silně konkuruje pravděpodobnostní Church-Turingově teorii a jeho konstrukce převyšuje výpočetní možnosti klasického počítače.[6][15]

V následujících letech se jeho teorií inspirovaly desítky vědců, některým z nich se dokonce povedlo jeho teorii vylepšit. V roce 1994 demonstroval Peter Shor dva velké problémy, které se dají efektivně řešit kvantovými počítači – *prvočíselný rozklad celých čísel* a tzv. „*diskrétní logaritmus*“. Následujícím roku se Lov Grover úspěšně zabýval prohledáváním nestrukturovaných prostor, které by se daly značně urychlit užitím kvantového počítače. Ve stejné době se mnoho dalších vědců inspirovalo Feynmanovou teorií z roku 1982 – proč řešit kvantovou mechaniku na klasickém počítači, když ji mohu řešit na kvantovém počítači a předejít všem složitostem, které s sebou přináší klasický počítač. Pomineme-li předpoklad konstrukce plně funkčního kvantového počítače, přichází ta složitější část celého procesu – algoritmus. Již na začátku bylo zmíněno, že je kvantová mechanika kontraintuitivní. K vytvoření fungujícího kvantového algoritmu se musíme odpoutat od klasického myšlení a je nutné využít pouze kvantových efektů. Druhý neméně důležitý úkol je vymyslet algoritmus, který složitostí převyšuje algoritmy klasického počítače. Kdybychom nepotřebovali řešit složitější a složitější úkoly, tak bychom mohli zůstat u klasického počítače.[11][15]

1.3.3 Komunikace a informace

Kvantový počítač nebyl jediný pokrok v 20. století. Paralelně s ním se samozřejmě vyvíjela i komunikace, tj. kvantová komunikace. Roku 1948 se Claude Shannon, který vydal několik článků týkajících se právě moderní komunikace, snažil matematicky podchytit koncept informace, ačkoliv to nebyl jeho prvotní záměr. Ze Shannonovy práce je vidět, že při přenosu informace se musíme zabývat dvěma základními parametry. Jedním z nich jsou zdroje potřebné k přenosu informace. Kolik dat je potřeba přenést daným systém, ať už je to přenos telefonním kabelem nebo z modernější doby internetový přenos a jak spolehlivý je informační tok. V druhé

řadě se zabýval právě přenosem signálu, je-li možné ho ochránit před šumem v komunikačním kanále.[18]

Shannon sám přišel s dvěma základními teoriemi pro přenos informace. První je teorie bez šumového kanálového kódování, která kvantifikuje fyzikální zdroje potřebné k uložení výstupu ze zdroje informací. Druhá fundamentální teorie je zvaná šumová kanálová kódovací teorie a jejím úkolem je určit množství informací, které je možno spolehlivě přenést při kanálovém šumu. Protože teorie informačního přenosu při šumu byla nedokonalá, navrhl Shannon tzv. opravující kódy, které mají ochránit datový tok, ale až jeho následovníkům se povedlo vymyslet takové kódy, jež se velmi přibližují jeho teorii.

Teorie kolem kvantové informace prodělaly podobný vývoj. O jeho první rozvoj se zasloužil Ben Schumacher v roce 1995. Byla to analogie k Shannonově teorii bez šumového přenosu a při té příležitosti to byl Schumacher, kdo definoval nový pojem kvantový bit. Bohužel se zatím nikomu nepovedlo vymyslet analogickou teorii pro přenos při šumu. Nicméně z předchozí kapitoly víme, že kvantový přenos efektivně překonává šum a umožňuje přenos i v šumových kvantových kanálech.[18]

V roce následujícím se na opravujících kódech podíleli tři vědci, Robert Calderbank, Peter Shor a Andrew Steane, kteří podle iniciál svých příjmení, pojmenovali nový kvantový opravující kód CSS, ten pomohl k dalšímu vývoji stabilizačních a opravujících kódů, které umožnily lépe pochopit kvantové procesy.[18]

Nedílnou součástí je i kryptografie, tj. kvantová kryptografie, ale ta bude podrobně probrána ve třetí kapitole.

2 Princip kvantového počítače

2.1 Fundamentální koncepty kvantové teorie

Aplikovaná kvantová informační teorie jako součást kvantové teorie, je definována několika důležitými aspekty. Většina těchto aspektů je plně vázaná na kvantovou teorii, některá vychází z klasické fyzikální teorie.

První pojem, který stojí za zmínku je neurčitost. Pro praktickou představu se budeme inspirovat Newtonovými zákony. V reálném světě nikdy nemůžeme přesně určit polohy a rychlosti všech objektů ve fyzikálním systému. Můžeme jen s velkou jistotou určit trajektorii a pravděpodobnost chování daných objektů. Neurčitost není unikátní vlastností kvantového systému, ale je kritická pro její popis. Obecně tedy můžeme říci, že nikdy nedosáhneme kompletní znalosti všech informací v systému, ale dokážeme s velkou přesností předpovídat nadcházející události.[10]

Rušení je další fundamentální koncept kvantové teorie a je interpretováno podobně jako jakékoliv vlnění v klasické fyzice. Při konstruktivním rušení dochází k zesílení vln, naopak při destruktivním rušení dochází k jejich zrušení. K vytvoření vlny v klasické fyzice je třeba mnoho částic, které se navzájem koherentně vytlačují. Typickým příkladem je vlna na moři, zvuková tlaková vlna nebo také vlny magnetického či elektromagnetického pole. V kvantové fyzice na rozdíl od té klasické je zapotřebí pouze jedna částice pro vytvoření vlny, tudíž samotný elektron může vykazovat vlastnosti podobné vlnám. Mluvíme zde o tzv. dualitě, kde se jakýkoliv komponent chová jako částice i jako vlna.[10]

Třetí na řadě je nejistota. V tomto případě je nejistota v kvantové teorii značně odlišná oproti klasické fyzikální teorii a zabýváme se pouze jedinou částicí v systému. Zaměříme se na dvě důležité vlastnosti – *pozice a hybnost*. S jistotou budeme znát vždy jen jednu z daných vlastností dle Heisenbergova principu neurčitosti[5], tj. pokud budeme znát přesnou polohu částice, nebudeme znát její hybnost a naopak. Stejné principy fungují i v kvantové informatice při distribuci kryptografického klíče v komunikačních kanálech. Jedná se o zakódování informace do dvou proměnných, aby se zabránilo odposlechu z třetí strany.[10]

[5] Heisenbergův princip neurčitosti – tato teorie tvrdí: pokud máme dvě konjugované veličiny, tak čím přesněji určíme jednu z veličin, tím méně přesná bude druhá veličina (uvedl příklad na hybnosti a poloze částice)

Čtvrtým fundamentálním konceptem je superpozice, jež definuje kvantovou částici v lineárním stavu nebo ve stavu superpozice. Částice se může vyskytovat v jakémkoliv z těchto dvou stavů. Tento princip vychází z linearity kvantové teorie. Z lineární Schrödingerovy rovnice je kombinace $\alpha\psi + \beta\varphi$ řešením, pokud ψ a φ jsou také řešením rovnice. Z toho vyplývá, že daná rovnice je koherentní superpozicí dvou řešení. Jednoduše řečeno, superpozice znamená, že se částice může vyskytovat v jedné i v druhé lokaci zároveň.[10]

Poslední koncept, který se zde bude rozebírat, je propletení. Propletení je unikátní vlastnost kvantových systémů, které se jen těžko popisují v klasické fyzice. Jedná se o silnou kvantovou korelaci dvou nebo více částic najednou. Schrödinger se zabýval propletením kvantových částic od roku 1935, jako první použil termín *entaglement* (*propletení*) a vypozoroval některé jejich zvláštní vlastnosti. Einstein, Podolsky a Rosen se zabývali stejnou problematikou a zavedli tzv. *zdánlivý paradox*, který způsobil určité pochybnosti o kvantové teorii. Nicméně tvrdili, že by zde mohla existovat nějaká lokální proměnná, která by zdánlivý paradox mohla popsat. Trvalo téměř 30 let, než se tento paradox povedlo vysvětlit. Zasloužil se o to John Bell svou teorií zvanou *Bellova nerovnost*[6]. Poté poukázal na dva propletené kvantové systémy, které narušily tuto nerovnost. Z nich je jasné, že nemá žádné řešení v klasické korelaci a jedná se unikátně o kvantový fenomén.[10]

2.2 Diracova rovnice a Hilbertův prostor

Před tím, než se tato práce bude zabývat kvantovým počítačem, je třeba si ujasnit určitou terminologii, která nás bude provázet celou prací.

První, velmi důležitým pojmem je *Diracova rovnice*. Vektorové veličiny se od skalárních (v textu) odlišují „psaním čárky nebo šipky nad danou veličinou“ (a – skalár, $\vec{a}$ – vektor). Paul Dirac přišel s novým značením. Symbol identifikující vektor se píše uvnitř „ket“ a vypadá takto $|a\rangle$. Pokud určujeme duální vektor pro a, píše se uvnitř tzv. „bra“ a zapisuje se takto $\langle a|$. Produkty uvnitř „bra-kets“ budou značeny $\langle a|b\rangle$.[11]

Vektorový prostor, kterým se zabýváme, se rozkládá v oboru komplexních čísel s konečným počtem dimenzí. Tato znalost nám značně usnadňuje potřebnou matematiku. Nic podstatného není doposud určeno touto definicí, jen je důležité to zmínit, protože každá literatura o kvantové mechanice pracuje s komplexním vektorovým prostorem v konečném

[6] Bellova nerovnost- J.S. Bell popisuje neslučitelnost lokálního realismu s kvantovou teorií

počtu dimenzí (značeném Hʊ). Takový vektorový prostor, který je součást třídy vektorových prostorů, se nazývá *Hilbertův prostor*.[11]

Jelikož má Hilbertův prostor konečný počet prvků (konečná dimenze), můžeme si vybrat bázi, která reprezentuje konečný sloupec vektorů a zastupuje operátory s konečnou maticí. Pro nás důležitý Hilbertův prostor je typicky 2^n dimenzionální pro kladné číslo *n*. Používá se, protože se bude konstruovat větší prostor spojováním řetězců menších prostorů, obvykle o velikosti dva. Je potřeba vybrat vhodný základ, kterému budeme přezdívat *výpočetní báze*. v této bázi budeme označovat 2^n vektory z Diracovy rovnice užitím binárního řetězce o délce *n*.

$$|00\cdots00\rangle, |00\cdots01\rangle, \cdots |11\cdots10\rangle, |11\cdots11\rangle \tag{2.1}$$

V rovnici níže vidíme porovnání zápisů Diracovy rovnice a klasického sloupcového, vektorového zápisu.

$$|00\cdots00\rangle \leftrightarrow \begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix};\ |11\cdots11\rangle \leftrightarrow \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix} \tag{2.2}$$

Hlavní účel Diracova zápisu je jednoduchost a přehlednost. Pokud máme 2-qubitový stav, tak se 2^n-dimenzionální vektor skládá ze 4 komponent. Diracův i sloupcový zápis by vypadal jednoduše. Kdybychom se však začali zabývat složitějšími stavy, sloupcový zápis by byl velmi složitý. Např. 16-qubitový stav by v 2^n-dimenzionálním vektoru měl 65536 komponent.

2.3 Kvantový bit

Bit je základní pojem v klasickém programování a v klasické informatice. Analogický koncept pro kvantový počítač je kvantový bit, zkráceně qubit. Jde o základní jednotku informace podléhající kvantové logice.

Pokud se budeme zabývat klasickým bitem, ten může nabývat hodnot od 0 do 1. Avšak qubit může také nabývat hodnot od 0 do 1. V čem tedy spočívá rozdíl? Z minulé kapitoly víme o tzv. Diracovu zápisu. Dva možné stavy kvantového bitu se tedy zapíší jako $|0\rangle$ a $|1\rangle$.

Znamená to, že se můžou vyskytovat ve stavech 0 a 1, ale díky principu superpozice je známo, že se mohou vyskytovat i ve stavech jiných. Isaac L. Chuang ve své práci popisuje kvantový bit jako fyzický objekt a zároveň jako matematický abstraktní objekt. Tvrdí, že krása práce s qubitem jako abstraktním objektem nám dává volnost interpretovat obecnou kvantovou teorii, která nám umožní jeho realizaci bez větších omezení.[11]

Obecný zápis superpozice kvantového bitu pomocí lineární kombinace je

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.3}$$

kde koeficienty α a β jsou komplexní čísla (pro představu neuškodí je považovat ani za reálná čísla). Nejsme však schopní přesně určit kvantový stav, který tyto koeficienty reprezentují. Pokud se pokusíme změřit kvantový bit, víme z předchozích kapitol, že naše možnosti jsou velmi omezené. Necháme se tedy inspirovat geometrií a pro měření použijeme zápis

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.4}$$

Měříme-li kvantový bit, dosáhneme buď výsledku 0 (pravděpodobně hodnota $|\alpha|^2$) nebo 1 (pravděpodobně hodnota $|\beta|^2$). Pochopitelně pak platí výsledek z rovnice (2.3). Jak již bylo zmíněno, z geometrie je kvantový stav normalizován na délku 1, tudíž je možné ho charakterizovat ve dvoudimenzionálním komplexním vektorovém prostoru.[11]

Druhé mocniny absolutních hodnot α a β v době měření nabývají hodnot 0 a 1, jelikož jsme schopni je měřit pouze ve stavu výpočetní báze. Nicméně, během provozu kvantových bitů je jasné, že nabývají hodnot i jiných v mezích od 0 do 1. Teoreticky mohou koeficienty α a β nabývat hodnot ve stavu

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \tag{2.5}$$

Z tohoto stavu vyplývá, že hodnota 0 i 1 nastane v 50 procentech případů. Tento stav se značí $|+\rangle$ a často se používá jako referenční hodnota pro superpozici v qubitu.[11]

2.3.1 Blochovo schéma

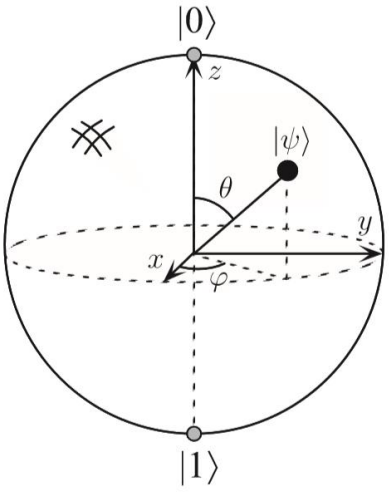
Blochovo schéma slouží k vizualizaci kvantového bitu v trojrozměrném prostoru. Pro matematickou představu je potřeba rozepsat rovnici (2.3) odhadem partikulárního řešení

$$|\psi\rangle = e^{i\gamma}(cos\frac{\theta}{2}|0\rangle + e^{i\gamma}sin\frac{\theta}{2}|1\rangle). \quad (2.6)$$

Číslo $e^{i\gamma}$ nemá žádný efekt na danou rovnici (odvozeno z kvantové mechaniky), proto ho můžeme zanedbávat a budeme pracovat s upravenou rovnicí

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\gamma}sin\frac{\theta}{2}|1\rangle. \quad (2.7)$$

Rovnice (2.7) obsahuje reálná čísla $\gamma, \varphi\ a\ \theta$, kde úhel θ je v mezích $0 \leq \Theta \leq \pi$ a úhel φ v mezích $0 \leq \varphi \leq 2\pi$ a popisuje stav qubitu v závislosti na těchto úhlech.[11] (viz obr. 1)



Obrázek č. 1: Blochovo schéma qubitu[11]

2.4 Mnohonásobné kvantové bity

V kvantovém počítači není pouze jeden kvantový bit, ale je jich obvykle větší množství. Jak je známo z klasického počítače, qubity se stejně jako bity ukládají do registrů, tj. kvantových registrů. Pro představu budeme pracovat s dvěma qubity, které mají právě čtyři výpočetní báze ve tvaru $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Jelikož se jedná o kvantový bit, musíme opět zavést komplexní koeficient, který pracuje se superpozicí. Tento vektorový stav můžeme popsat následující rovnicí

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \quad (2.8)$$

Pokud bychom měli 3-qubitový systém, vypadala by rovnice obdobně, jen by čítala 8 místo 4 prvků.[11] (viz rovnice 2.9)

$$|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle. \quad (2.9)$$

Obecný zápis n-qubitového registru je tedy zapsán jako

$$|\psi\rangle = \alpha_{0\cdots0}|0\cdots0\rangle + \alpha_{0\cdots1}|0\cdots1\rangle + \cdots + \alpha_{1\cdots0}|1\cdots0\rangle + \alpha_{1\cdots1}|1\cdots1\rangle. \quad (2.10)$$

2.5 Kvantové brány

Z anglického quantum gates se překládá tento pojem do českého jazyka jako kvantové brány nebo kvantová hradla. Jedná se o brány, které mají provést určitou logickou operaci s danou informací. Z klasických počítačů víme, že je informace vedena obvodem pomocí drátů a v logických bránách jsou prováděny určité logické operace. Kvantové brány a kvantový obvod fungují na stejném principu, jen se musíme zamyslet nad tím, jestli daná operace je proveditelná i ve stavu superpozice.

2.5.1 Jednoqubitové brány

První brána, kterou popíšeme, je „NOT“. Jedná se o standardní princip negace. U klasického bitu by se změnila 0 na 1 a 1 na 0. Ve výpočtovém základu by fungoval stejný princip i pro qubit, ale ve stavu superpozice už to platit nebude. Z několikaletého výzkumu a pozorování plyne, že se NOT brána chová lineárně. Nevíme přesně proč tomu tak je, ale značně nám to usnadní realizaci. Pokud si napíšeme kvantový stav

$$\alpha|0\rangle + \beta|1\rangle, \quad (2.11)$$

tak se stav změní logickou operací NOT na

$$\alpha|1\rangle + \beta|0\rangle. \quad (2.12)$$

Linearita je typická pro celý chod kvantové mechaniky. Navíc, pokud bychom se dostali do stavu nelinearity, vedlo by to ke zdánlivým fyzikálním paradoxům typu cestování časem, porušování druhého termodynamické zákonu[7] apod. Vrátíme-li se zpět k NOT bráně, můžeme

[7] Druhý termodynamický zákon – popisuje průběh tepelných dějů a omezené možnosti tepelných energetických přeměn

ji popsat právě díky linearitě maticí X, Y a Z. Označení je dáno otáčením vektoru o úhly π radiánu po dané ose. Vše je viditelné v Blochově schématu. [11] (viz obr. 1)

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.13}$$

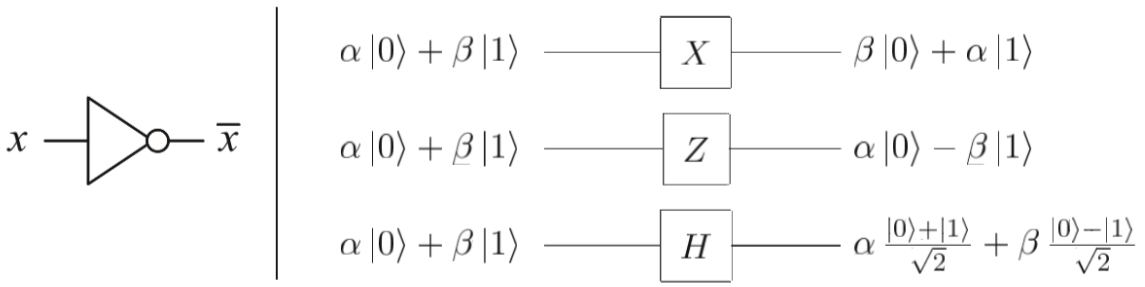
$$Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Další transformací brány NOT je *Hadamardova brána*, která je často považována za kvadratický kořen NOT brány a je definována maticí

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2.14}$$

ze které vyplývá změna $|0\rangle$ na $(|0\rangle + |1\rangle)/\sqrt{2}$ a $|1\rangle$ na $(|0\rangle - |1\rangle)/\sqrt{2}$. Obě tyto změny jsou na půl cesty mezi $|0\rangle$ a $|1\rangle$. Hadamardova brána je jedna z nejpoužívanějších bran v kvantové informatice. Princip Hadamardovy matice vychází z Blochova schématu, kde se sféra nejprve otočí o 90° v *y*-ové ose a poté o 180°v x-ové ose.[11]

Na obrázku č. 2 vidíme srovnání X, Z a H NOT bran.



Obrázek č. 2: Jednobitová brána (vlevo), Jednoqubitové brány X, Z a Hadamardova (vpravo) [15]

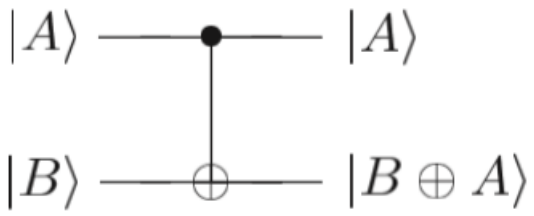
Za zmínku ještě stojí speciální brána zvaná *Phase shift gate*, která je specifická otáčením vektoru kolem osy z. Jedná se o posun úhlu Θ, který lze vyjádřit obecným zápisem

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = |1\rangle\langle 0| + e^{i\theta}|0\rangle\langle 1|, \tag{2.15}$$

kde $\theta = \frac{\pi}{4}$. Pokud by se jednalo o posuv $\theta = \frac{\pi}{2}$, mluvíme o T-gate, pokud by posuv byl $\theta = \pi$, tak se jedná o S-gate.[11][10]

2.5.2 Vícequbitové brány

První představitel vícequbitové logické brány je *controlled-NOT brána* (zkráceně CNOT). Tato brána pracuje se dvěma qubity – kontrolní qubit a cílový qubit. Obvod CNOT brány je znázorněna na obrázku č. 3 a v matici U_{CN}



Obrázek č. 3: Controlled-NOT qubitová brána[15]

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.16}$$

Horní čára symbolizuje kontrolní qubit a spodní ten cílový. Pokud kontrolní qubit nastavíme na 0, operace cílový qubit nezmění. Pokud však nastavíme kontrolní hodnotu na 1, cílový qubit převrátí svou hodnotu.[11]

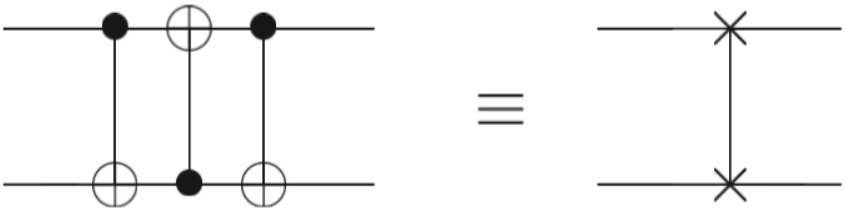
$$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle \tag{2.17}$$

CNOT (zobecněná XOR brána) je jediná z bran, kterou při inspiraci klasickým počítačem lze použít. Ostatní logické brány typu NAND nebo klasická XOR brána jsou nezvratné, a tudíž by byly při kvantových procesech nepoužitelné. Docházelo by ke ztrátě informací. Existuje spousta dalších zajímavých kvantových bran, ale za pomocí CNOT brány a jednoqubitových bran jsme schopni sestrojit jakoukoliv složitější bránu.[11]

Můžeme například zmínit *Controlled-U bránu*, *Fredkinovu bránu* nebo *Toffoliho bránu*. Všechny tyto brány jsou kombinací již zmíněných bran a užívají se ve složitějších kvantových obvodech.

2.6 Kvantové obvody

V přechozí kapitole jsme si vysvětlili, co jsou to kvantové brány. Teď je třeba vysvětlit, jakým způsobem je propojíme, abychom dostali ucelený kvantový obvod. Propojení funguje stejně jako u klasického obvodu dráty. Představa fyzického drátu napadne snad každého, ale v kvantových obvodech tomu tak být nemusí. Může ho nahradit jiný abstraktní přesun informace, např. tok času nebo fyzická částice typu foton.



Obrázek č. 4: Obvod dvou přepínacích qubitů (vlevo) a jeho ekvivalentní schématický zápis symbolů (vpravo) [15]

Na obrázku č. 4 máme obvod, ve kterém se mění stav dvou qubitů. Abychom viděli, čeho obvod dosáhne, rozepíšeme si postupně úseky změn výpočtových stavů $|ab\rangle$:

$$\begin{aligned} |a,b\rangle &\longrightarrow |a, a\oplus b\rangle \\ &\longrightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\longrightarrow |b, (a\oplus b)\oplus b\rangle = |b, a\rangle \end{aligned} \tag{2.18}$$

Máme několik pravidel, která se při tvorbě kvantových obvodů musí dodržovat. Tolik drátů, kolik do kvantové brány vchází, musí i vycházet. Nelze kopírovat qubity stejným způsobem jako bity v klasických obvodech. Kvantové obvody jsou znázorněny schématem, ve kterém horizontální čáry znázorňují dráty a všechny ostatní prvky jsou kvantové brány (viz obr. č. 4). Dalším předpokladem pro fungující kvantový obvod je vyhýbání se smyčkám. Ačkoliv to v klasickém obvodu možné je, kvantový systém musí být výhradně acyklický.[15]

Aplikací složitých kvantových obvodů bychom dokázali popsat princip fungování složitých procesů typu Bellovy báze nebo kvantové teleportace. Ve stručnosti lze konstatovat, že kvantová teleportace pojednává o přesunu kvantového stavu bez potřeby užití komunikačního kanálu.[15]

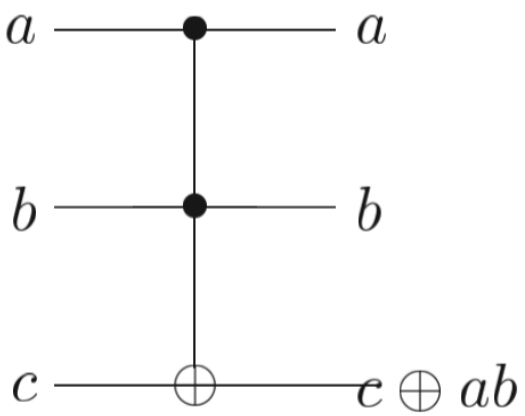
2.7 Kvantový algoritmus

Jaké výpočty mohou být provedeny užitím kvantových obvodů? Bude užití kvantových obvodů efektivnější než výpočty v klasických obvodech? Není žádným překvapením, že lze

simulovat klasický logický obvod užitím kvantového obvodu. Již několikrát jsme zmiňovali, že vše kolem nás lze vysvětlit kvantovou mechanikou, a bylo by zvláštní, kdyby to v tomto případě neplatilo.[15]

Vybereme si ekvivalentní obvod ke klasickému obvodu tak, aby obsahoval pouze vratné elementy. V tomto případě použijeme *Toffoliho bránu*, která se skládá ze dvou kontrolních bitů a jednoho cílového bitu. Jedná se o rozšířený CNOT, jenž splňuje princip vratnosti.[15]

Toffoliho brána je schopna simulovat NAND brány, ale může se použít i jako FANOUT (viz obr. č.5). S těmito dvěma vlastnostmi je možné simulovat jakékoliv elementy klasického obvodu, a tak může být libovolný klasický obvod simulován ekvivalentním vratným obvodem. Jelikož tento klasický obvod splňuje všechny podmínky kvantového obvodu, může se Toffoliho brána tvářit i jako kvantová brána.[15]



Obrázek č. 5: Obvod reprezentující Toffoliho bránu[15]

2.7.1 Kvantový paralelismus

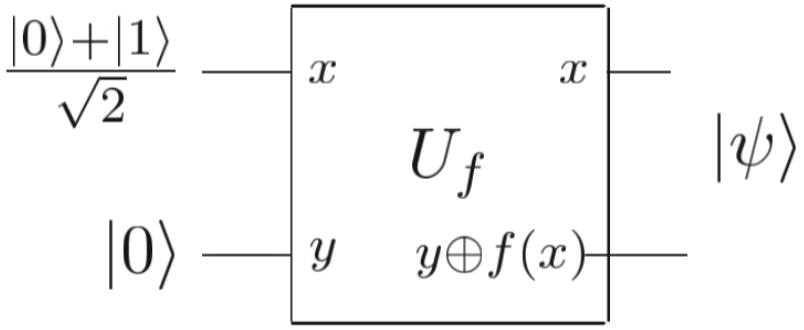
Kvantový paralelismus je fundamentální vlastnost většiny kvantových algoritmů. Umožňuje kvantovým počítačům vyhodnotit funkci *f(x)* pro více hodnot *x* zároveň. Přepokládejme, že funkce *f(x): {0,1} →{0,1}* je funkce s 1-bitovou doménou a rozsahem. Nejvhodnější cesta výpočtu bude kvantovým počítačem o dvou qubitech začínající ve stavu $|x, y\rangle$. Transformací vhodnou logickou bránou dosáhneme stavu $|x, y \oplus f(x)\rangle$. Symbol $\oplus$ znamená modulo 2. Tuto transformaci pojmenujeme U_f.[15]

Pro lepší porozumění budeme předpokládat $|y\rangle = 0$, poté hodnota $|x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, jak je patrné z obrázku č. 6. Tohoto stavu dosáhneme aplikací Hadamardovy brány ve stavu

$|0\rangle$. Ve stejném obrázku vidíme, že se nám vrátí stejná hodnota $|x\rangle$ a druhý qubit $|y\rangle$ můžeme vyjádřit rovnicí

$$|y\rangle = 0 \rightarrow \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}, \tag{2.19}$$

která obsahuje $f(0)$ i $f(1)$ po jednom spuštění brány. Tato schopnost kvantového počítače je zvaná kvantový paralelismus a proces, který by klasický počítač zpracovával několika kroky, zvládl na jeden pokus.[15]



Obrázek č. 6: Obvod reprezentující kvantový paralelismus[15]

Celý tento průběh je možné zobecnit pro libovolný počet bitů užitím Hadamardovy transformace, která jen využívá *n* Hadamardových bran paralelně na *n* qubitech. Obecný zápis této transofrmace o *n* qubitech ve stavu $|0\rangle$ je

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \tag{2.20}$$

kde suma je součet všech možných hodnot *x* a je značena $H^{\otimes n}$. Tato transformace velmi efektivně vytváří superpozice 2^n stavů použitím pouze *n* bran.[15]

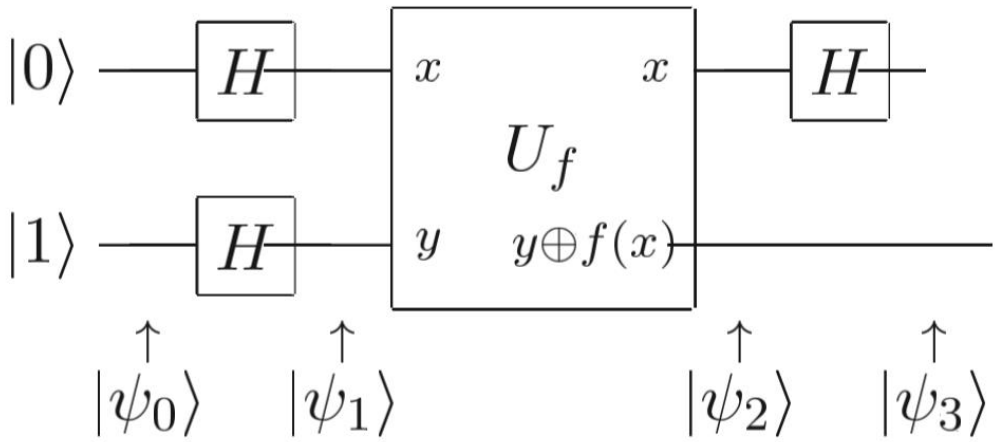
Kvantový paralelismus nám umožňuje vyhodnocovat jakékoliv možné množství funkcí *f* zároveň, nicméně není užitečný hned. Pokud si vezmeme 1-bitový systém, tak měřením získáme hodnoty $|0, f(0)\rangle$ nebo $|1, f(1)\rangle$. V podobném případě $\sum_x |x, f(x)\rangle$ dostaneme jen jeden výsledek f(x) pro hodnotu *x*. Toto by jednoduše zvládl i klasický počítač. Kvantové výpočty vyžadují více než kvantový paralelismus, aby byly užitečné.[15]

2.7.2 Deutschův algoritmus

Britský fyzik David Deutsch se jako jeden z prvních zabýval kvantovým paralelismem a za pomoci algoritmu, které nese jeho jméno, se mu povedlo modifikovat schéma (obr. č. 6)

z předchozí kapitoly. Deutschův algoritmus spojuje kvantový paralelismus a jeden z fundamentálních konceptů kvantové teorie – rušení.

Stejně jako v přechozím případě využijeme Hadamardových bran, abychom si připravili první qubit v $|0\rangle$ jako superpozici $(|0\rangle + |1\rangle)/\sqrt{2}$. Odlišná je však příprava druhého qubitu jako superpozici $(|0\rangle - |1\rangle)/\sqrt{2}$ ve stavu $|1\rangle$. Celý tento proces je znázorněn v obr. č. 7.[15]



Obrázek č. 7: Obvod znázorňující Deutschlv algoritmus[15]

Výchozí stav ve tvaru

$$|\psi_0\rangle = |01\rangle \tag{2.21}$$

prochází dvěma Hadamardovými bránami a dostáváme výsledek

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{2.22}$$

Následnou aplikací U_f do $|\psi_1\rangle$ se dostáváme do stavu $|\psi_2\rangle$, který je vyjádřen jednou ze dvou možností

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \; pro\; f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \; pro\; f(0) \neq f(1). \end{cases} \tag{2.23}$$

Poslední Hadamardovou bránou prochází pouze první qubit a je definován opět jednou ze dvou možností

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \; pro\; f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \; pro\; f(0) \neq f(1). \end{cases} \tag{2.24}$$

Pokud si uvědomíme, že $f(0) \oplus f(1)$, jestli je $f(0) = f(1)$ a naopak, můžeme výsledek $|\psi_3\rangle$ zapsat ve tvaru

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{2.25}$$

Měřením prvního qubitu jsme určili $f(0) \oplus f(1)$. Tento fakt potvrzuje funkčnost Deutschova algoritmu, protože nám kvantový obvod umožnil determinovat komplexní vlastnost $f(x)$ resp. $f(0) \oplus f(1)$ užitím pouze jednoho vyhodnocení funkce $f(x)$. Klasický počítač by k tomu potřeboval minimálně dva výpočty.[15]

Tato skutečnost opět poukazuje na rozdíl mezi kvantovým paralelismem a klasickým algoritmem. Pokud vezmeme v potaz hodnoty $f(0)$ a $f(1)$, klasický algoritmus udělí každé hodnotě pravděpodobnost 50 procent a hodnoty už se budou na vždy vylučovat. U kvantového algoritmu se bude jednat o „chytrou“ volbu, kde jedna hodnota interferuje s druhou a umožní efektivní určení informace o vhodné funkci, kterou by klasický počítač určit nedokázal. [15]

David Deutsch se podílel i na dalším, *Deutsch-Jozsovu algoritmu*, který je v podstatě jen zobecněním původního Deutschova algoritmu. Pravdou je, že řešení problému na kvantovém počítači užitím tohoto algoritmu by bylo mnohem efektivnější než na klasickém počítači. Bohužel ale nebyl navržen tak, aby se mu dostalo většího využití.[15]

Obdobný princip řešil i *Simonův algoritmus*, který se zabýval binárními vektory tvořícími mimořádné podmínky. Funkce *f* byla periodická pokud $f(x) = f(y)$ za podmínky $x = y$ nebo $x = y \oplus r$, kde *r*, popisující binární periodu, se nerovná nule. Klasický počítač by tuto úlohu řešil exponenciálním počtem dotazů. Kvantovými výpočty jsme však schopni dosáhnout výsledku s velkou pravděpodobností pouze $O(n)$ iteracemi (polynom prvního stupně).[15]

2.7.3 Kvantový algoritmus na bázi Fourierova rozvoje

Další velkou kapitolou kvantových algoritmů je Fourierova řada, resp. Fourierův rozvoj. Aniž bychom si to uvědomili, pravidla tohoto rozvoje byla ukázána již u Deutschova algoritmu. Obecnou definicí můžeme zapsat rovnicí

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i j k}{N}} x_j, \tag{2.26}$$

která popisuje transformaci N komplexních čísel $x_0, x_1, \cdots x_{N-1}$ do komplexních čísel $y_0, y_1, \cdots y_{N-1}$ zmíněnou rovnicí. Tato metoda má obrovské množství využití a její princip je převedení složitého problému do stavu snadněji řešitelného.[10]

V roce 1822 francouzský matematik a fyzik Josef Fourier, publikoval svou práci *Théorie analitique de la chaleur*. Prvotní Fourierův záměr se měl vztahovat jen na termodynamické zákony a sám autor neměl nejmenší tušení, že touto transformací změní pohled na fyziku skoro ve všech odvětvích. Mimořádný úspěch sklidila *diskrétní Fourierova transformace* (DFT), která byla diskrétně a výpočetně velmi efektivně implementována do *rychlé Fourierovy transformace* (FFT), jež je nejčastěji používaná v klasických výpočtech. Analogicky k FFT se v pozdějších letech užitím kvantových výpočtů vytváří další teorie zvaná *kvantový Fourierův výpočet* (QFT). Ta nám umožnila objevit další výhody kvantového paralelismu.[10]

V rovnici (2.26) je zapsána obecná rovnice Fourierova rozvoje, která vytváří spojení mezi dvěma vektory. V kvantových výpočtech musíme zahrnout princip superpozice, a proto využijeme Diracova zápisu, který nám umožní transformovat DFT do QFT. Začínáme ve stavu $|\varphi\rangle$ v prostoru vektorové výpočetní báze $|i\rangle$, kde $i = 0 \cdots N-1$. Pokud platí $|\psi\rangle = F(\varphi)$, pak můžeme zapsat kvantový Fourierův rozvoj jako[10]

$$|\psi\rangle \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} |k\rangle\, e^{\frac{2\pi i j k}{N}} \varphi_i. \tag{2.27}$$

Pokud tedy aplikujeme zmíněný QFT do výpočetní báze $|i\rangle$, dostáváme:

$$F|i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle. \tag{2.28}$$

Přestože je QFT exponenciálně rychlejší než jeho klasický kolega, neplní úplně stejné úkony. QFT totiž nevytváří žádný z Fourierových koeficientů. Rozdíl mezi těmito dvěma transformacemi může být vnímán jako výpočet všech pravděpodobností pravděpodobnostního rozdělení nebo vzorkování tohoto rozdělení. Tato složitá definice pravděpodobně nikomu moc

neřekne, a tak můžeme poděkovat talentovanému týmu ve složení Griffith, Niu, Cleve, Ekert, Maciavello a Mosca, který to ostatním usnadnil. Definici kvantového Fourierova rozvoje již znali, nebylo však známo, jak implementovat QFT pomocí elementárních kvantových bran. Povedlo se jim zpětně vystopovat rozklad tenzorového produktu, tím pádem dokázali asociovat jeden drát právě jedné qubitové bráně.[10][11]

Pokud bychom chtěli sestavit a popsat kvantový obvod implementováním Fourierova rozvoje, používali bychom Hadamardovy brány, elementární kvantové brány a rotační operátor R_k, který je popsán maticí

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{bmatrix}. \tag{2.29}$$

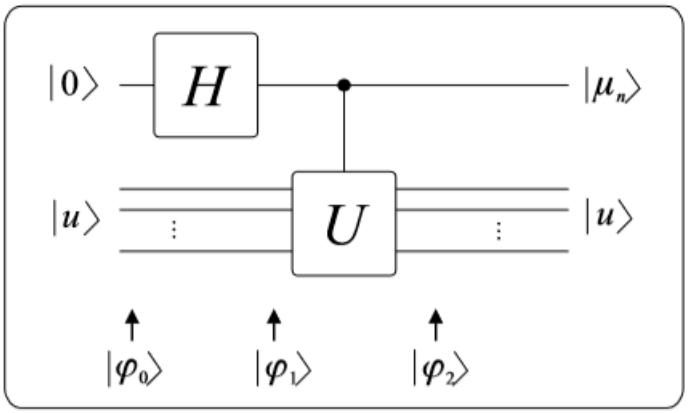
2.7.4 Kvantový fázový odhad

Fázový odhad je další stavební kámen mnoha kvantových algoritmů a umožňuje dále rozšiřovat znalosti QFT. Jednotkový operátor má vlastní hodnotu $e^{j\alpha_u}$ s reálným číslem α_u a komplexní jednotkou j a právě α_u je důležité z hlediska fáze. Snažíme se najít fázový odhad $\kappa_u \in [0,1)$: $\alpha_u = 2\pi\kappa_u$, který je ekvivalentem daného problému. Neznáme tedy přesný stav matice U, ale můžeme do ní implementovat zařízení, jež nám umožní ovládat její funkce.

Fázový odhad v ideálním stavu je popsán rovnicí

$$|\mu_l\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j2\pi 2^{n-1}\kappa_u}|1\rangle\right), \tag{2.30}$$

která se dále snaží o tenzorový rozklad produktu za účelem vytvoření vhodného kvantového obvodu. Proces je podobný Hadamardově bráně začínající v $|0\rangle$, ale musíme přenést exponenciální faktor před $|1\rangle$. Z tohoto hlediska je vhodné použít schéma inspirované Simonovým algoritmem se dvěma quregistry.[10] (obr. č. 8)



Obrázek č. 8: Obvod kvantového fázového odhadu s dvěma quregistry[10]

Horní registr obsahuje pouze jeden qubit $|0\rangle$. Spodní je však popsán vlastním vektorem $|u\rangle$ s qbitovou délkou t definován jako $|u\rangle$: $U|u\rangle = e^{j\pi\kappa_u}|u\rangle$ s počátkem ve $|\varphi_0\rangle = |0\rangle \otimes |u\rangle$. Využitím Hadamardovy brány v horním registru získáme

$$|\varphi_1\rangle = \left(H \otimes I^{\otimes t}\right)|\varphi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|u\rangle = \frac{|0\rangle|u\rangle + |1\rangle|u\rangle}{\sqrt{2}}. \tag{2.31}$$

Pokud budeme vyjadřovat dolní registr, musíme vzít v potaz neznalost operátoru U. Pro výpočet $|\varphi_2\rangle$ využijeme principu superpozice, abychom získali rovnici

$$|\varphi_2\rangle = (I \otimes I)|\varphi_1\rangle = \frac{|0\rangle + e^{j2\pi\kappa_u}|1\rangle}{\sqrt{2}} \otimes |u\rangle, \tag{2.32}$$

která se již od pohledu rovná hodnotě $|\mu_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j2\pi\kappa_u}|1\rangle\right)$ z rovnice (2.30). Jediný problém, který může nastat, je, pokud podmínku $2^0 = 1$ nahradíme jinou podmínkou 2^{n-1}. Tato překážka je snadno zdolána opakováním samotného procesu operátorů u na jednotkových vektorech $|u\rangle$.[10]

2.8 Shorův algoritmus

Shorův algoritmus je jeden z nejpoužívanějších algoritmů v kvantovém počítači. Slučuje kvantovou a klasickou část, které slouží k faktorizaci celých čísel. Autor tohoto algoritmu, Peter Shor, se snažil o nalezení všech prvočísel daného celého čísla. Mimo tuto teorii se zabýval ještě tzv. „*order-finding*“, který by se dal doslovně přeložit jako hledání pořadí. Obě uvedené teorie jsou zmíněny níže.[10]

Nejdříve shrneme společné vlastnosti obou teorií. Představme si dvě náhodná přirozená čísla, pro které platí $x < N$, že jsou prvočísla. Pořadí *x* v modulo *N* je definováno jako nejmenší přirozené číslo *r*, jež splňuje

$$x^r \ mod \ N = 1. \tag{2.33}$$

Pořadí *x* je v těsném spojení s periodou funkce $f(z) = x^z mod \ N$. Tuto vlastnost lze ověřit ze vztahu

$$f(z+r) = x^{z+r} \ mod \ N = \big((x^z mod \ N) \cdot (x^r mod \ N)\big) \ mod \ N = f(z). \tag{2.34}$$

Se znalostí této definice bychom se mohli vrhnout na praktické řešení. Nejdříve však budou vysvětleny obě teorie podrobněji pro lepší pochopení.[10]

2.8.1 Kvantové hledání pořadí

Abychom byli schopni navrhnout funkční kvantový algoritmus na hledání pořadí čísel, musíme se vrátit na úplný začátek algoritmizace. Opět využijeme kombinace kvantového paralelismu a interference. Myšlenka je v celku jednoduchá. Snažíme se vypočítat a uložit všechny možná $x^k mod \ N$ pro $0 \leq k \leq N$ v qubitu $t = (ld[N])$ kvantového registru určité velikosti v jiném qubitu jiného quregistru se stejnou velikostí a spřízněnou hodnotou *k*. V dalším kroku se budeme snažit o zvětšení pravděpodobnostní amplitudy $|x^k \ mod \ N = 1\rangle$, aby se hodnota quregistru přibližovala co nejvíce nule. Nárůst této amplitudy bude mít za výsledek vysokou pravděpodobnost návratu požadovaného pořadí *r* v druhém quregistru.[10]

Ačkoliv to vypadá srozumitelně, musíme platnost tohoto výroku ověřit na příkladu. Výpočtem lze určit stav, který je definovaný rovnicí

$$|u_s\rangle \equiv \frac{1}{\sqrt{3}} \sum_{k=0}^{r-1} exp\left[\frac{-2\pi isk}{r}\right] |x^k \ mod \ N\rangle \tag{2.35}$$

pro celá čísla $0 \leq s \leq r-1$ jako vlastní číslo *U* určené z rovnice

$$U|u_s\rangle \equiv \frac{1}{\sqrt{3}} \sum_{k=0}^{r-1} exp\left[\frac{-2\pi isk}{r}\right] |x^{k+1} \ mod \ N\rangle = exp\left[\frac{2\pi is}{r}\right] |u_s\rangle. \tag{2.36}$$

Užitím kvantového odhadu dosáhneme velmi přesného výsledku, ze kterého už snadno získáme požadovanou hodnotu pořadí r.

2.8.2 Faktorizace

Faktorizace je nedílná součást kryptografie a pokud se bavíme o Shorově algoritmu, napadá nás právě toto téma. Princip je opět velmi jednoduchý. Máme kladné celé číslo N, které není prvočíslem. Která prvočísla po vynásobení mezi sebou budou mít hodnotu zvoleného čísla? Cíle dosáhneme redukcí faktorizace zpět do teorie hledání pořadí.

Peter Shor ve své práci navrhl postup pěti kroků, kterými dosáhneme cíle. Pokud je číslo sudé, vrátíme se k děliteli dva. Druhým krokem se snažíme rozhodnout, zda platí $N = a^b$ pro celá čísla $a \geq 1$ a $b \geq 2$. Pokud to číslo splňuje, vrátíme se k děliteli a. Třetím krokem náhodně vybereme číslo x v rozsahu $1 \cdots N - 1$. Pokud je $\gcd(x, N) > 1$, vrátíme se k děliteli $\gcd(x, N)$. Ve čtvrtém kroku využijeme algoritmus hledání pořadí a zjistíme pořadí r čísla x modulo N. V pátém kroku se rozhodne, zda je pořadí r sudé a zároveň $x^{r/2} \neq -1(mod\ N)$. Splněním těchto podmínek můžeme provést výpočty gcd $(x^{r/2} - 1, N)$ a gcd $(x^{r/2} + 1, N)$, kterými dosáhneme aspoň jednoho netriviálního dělitele. Pokud se ani poté tak nestane, algoritmus je chybný.[10]

Celý proces je téměř neřešitelný pro klasický počítač. Tento úkol vyžaduje $O((\log n)^3)$ operací s omezenou pravděpodobností a kvantový počítač by jej zvládl značně rychleji. Touto problematikou se opět dostáváme ke kryptografii, která bude řešena v příštích kapitolách. Kvantový počítač by byl schopný prolomit standardní kryptografický kód velmi rychle. Proto společně s vývojem kvantových počítačů a kvantové algoritmizace se věda pro zachování bezpečnosti dat musí zabývat i kvantovou kryptografií.[10]

3 Kryptografie

3.1 Úvod do kryptografie

Slovo kryptografie pochází z řeckého kryptós a gráphein, v překladu skrytý a psát. Věda, která se zabývá šiframi, se nazývá kryptologie. Kryptografie má mnoho definicí, ale nejčastěji se uvádí, že je to věda a umění zabývající se šiframi, jejich vznikem a návrhem. Naopak kryptoanalytici se pomocí kryptoanalýzy snaží kód prolomit, cizím slovem dekódovat.

Potřeba šifrovaně komunikovat je stará jako civilizace sama. Stovky let se kryptografové celého světa snaží vymyslet složitější šifru než jejich protivníci. Donedávna bylo šifrování doménou diplomacie, armády a především špionážních služeb. V dnešní moderní době se k šifrování dostane i široká veřejnost, neboť se jedná o nástroj ochrany při práci s daty. Vývoj šifer můžeme rozdělit do dvou etap. Nejstarší a nejprimitivnější dochované šifry pocházejí ze starověkého Egypta a Mezopotámie. Lidé se už v tu dobu snažili šifrovat zprávy vyrýváním symbolů na zeď nebo do hliněných destiček. Vyjmenovávat všechny typy šifer a šifrovacích strojů v dějinách lidstva by bylo nad možnosti této práce. Mezi některé z historicky zajímavých patří třeba šifra Caesarova anebo šifrovací stroj Enigma. První etapa končí přibližně v polovině 20. století. Druhá etapa kryptografie je ta dnešní. Jedná se o moderní dobu s moderními technickými vymoženostmi.

3.2 Symetrické šifrování

Symetrické šifrování, často také označováno jako konvenční šifra za užití jednoho klíče, bylo jediným typem šifrování před vyvinutím veřejného klíče v 70. letech minulého století.

Symetrický šifrovací model prochází pěti procesy. Nejdříve vytvoříme *prostý text*. Ten má reprezentovat námi vytvořená data, která mají být zakódována. Tato vstupní data projdou *šifrovacím algoritmem*. Úkol takového algoritmu je transformovat a nahradit naši zprávu. Druhou vstupní ingrediencí je nezávislý *skrytý klíč*. Algoritmus vytvoří pokaždé jiný výstupní kód v závislosti na skrytém klíči v daném čase. Ve čtvrtém kroku na výstupu vzniká *šifrovaný text*, který se jeví jako nesmyslný tok dat. Dokáže ho rozluštit jen originální vstupní skrytý klíč.[16]

Existují dvě podmínky pro správné kódování zpráv. Musíme vytvořit velmi silný šifrovací algoritmus. Minimální požadavek je, aby náš útočník nedokázal vyluštit danou problematiku, pokud by se zmocnil jedné nebo více zašifrovaných zpráv. Druhou podmínkou je, aby odesílatel

i přijímající zvolili bezpečnou cestu pro přenos tajného klíče a udrželi ho v bezpečí. Pokud by se někdo zmocnil tohoto klíče a znal by algoritmus, je pro něj zpráva čitelná. Jinými slovy, stačí udržet v tajnosti jen klíč a zprávu nikdo cizí nerozluští.[16]

Jak bylo naznačeno v příkladu, proces algoritmizace je založen na dvou principech – substituce a transportace. Substituce vyměňuje elementy prostého textu (písmena, bity nebo jejich skupiny) za elementy jiné. Transportace nebo také přesun pouze přehazuje elementy mezi sebou. Oba tyto procesy jsou samozřejmě vratné.

Název symetrické šifrování vychází z počtu klíčů, které použijeme. Pokud odesílatel a příjemce použijí stejný klíč, mluvíme o symetrickém šifrování. Pokud příjemce použije jiný klíč, pak jde o asymetrické šifrování.

Pokud bychom chtěli vyjádřit symetrickou kryptografii odborně, musíme zavést konkrétní pojmy. Hodnoty $\{f, g, M, K, C\}$ jsou symetrické, z toho vyplývají funkce $f: M \times K \rightarrow$ $\rightarrow C$ a $g: C \times M = K$, které popisují šifrování a dešifrování. K je tajný klíč.[16]

3.2.1 Caesarova šifra

Jedná se první a nejprimitivnější symetrickou šifru. Měla pouze 25 klíčů a jednalo se o posun písmena v abecedě o *k* řádů výše. Tento kód můžeme popsat jednoduchým algoritmem

$$C = E(k, p) = (p + k) mod\ 26, \tag{3.1}$$

kde *k* symbolizuje posun písmen v abecedě. Caesar ve své šifře používal posun o 3 písmena.[16]

3.2.2 Hillova šifra

V roce 1929 vymyslel Lester Hill šifru na bázi maticového výpočtu. Jeho algoritmus přidělil každému písmenu čísla od 0 do 25 ($a = 0, b = 1, \cdots, z = 25$). Algoritmus je vyjádřen rovnicí

$$(c_1 c_2 c_3) = (p_1 p_2 p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} mod\ 26, \tag{3.2}$$

ve zkráceném tvaru

$$C = PK\ mod\ 26. \tag{3.3}$$

Největší výhoda Hillova algoritmu je zamaskování opakujících se stejných písmen.

3.2.3 Vigenérova šifra

Tento algoritmus fungoval na podobné bázi jako Caesarův algoritmus, ale místo základního stavu, od kterého se posouvala písmena v abecedě, bylo jiné. Popisuje ho rovnice

$$C_i = (p_i + k_{i\ mod\ m}) mod\ 26. \tag{3.4}$$

3.2.4 Block cipher (bloková šifra)

S blokovou šifrou je jednáno jako s celkem. Obvykle má velikost od 64 do 128 bitů. Prostý text je překládán jako blok a jako blok vychází i na výstupu. Tato šifra se již od začátku jevila jako velmi užitečná a používá se i dnes v mnohem větším měřítku než šifra proudová.[16]

Bloková šifra operuje na exponenciální bázi 2^n. Pokud je celý blok o 128 bitech zaplněn, bude velmi těžké ho dešifrovat. Nevýhoda vzniká, pokud použijeme počet bitů $n = 4$ nebo i menší. Blok je pak ekvivalentní ke klasické substituované šifře.[16]

Další patrnou nevýhodou je používání stále stejného klíče. Jeden klíč lze použít na více bloků nebo i na celý text. Počítačoví experti se však na tuto slabinu zaměřili a před spuštěním algoritmu přidávají ještě jeden vstup, který má za úkol snížit pravděpodobnost opakujících se prvků v bloku.

Nejznámějším zástupcem blokové šifry je *Data Encryption Standard* (DES), který byl aplikován v roce 1977. Využíval 64bitové bloky, ze kterých bylo klíčových 56 a zbylých 8 pouze kontrolních. Jeho nástupce se objevil v roce 2002 pod názvem *Advanced Encryption Standard* (AES). Velikost jednoho bloku je standardně 128 bitů a všechny jeho operace jsou prováděny v 8bitových bytech. S touto šifrou se můžeme setkat i v běžném životě, jejím typickým příkladem je WPA2 pro zabezpečení wifi sítě.[16]

3.2.5 Stream cipher (proudová šifra)

Proudová šifra funguje na podobném principu jako bloková, jen používá velmi malé bloky dat. Často zpracovává i hodnoty jednoho bitu a pracuje pouze s 1 blokem v daném čase. Typickým představitelem proudové šifry je Vigenérova šifra. Každá operace má svůj klíč, a tak se zde často setkáváme s logistickým problémem, jak poskytnout přenos velkého množství klíčů rychle a bezpečně. Výsledný tok dat je ovlivněn transformací šifrovacího klíče a šifrovacího algoritmu, ze kterého vzniká rozdílný šifrovací kód jednoho textu v různém časovém úseku.[16]

3.3 Pseudonáhodný generátor čísel

Než se budeme zabývat další problematikou veřejného klíče a asymetrické kryptografie, musíme definovat důležitost pseudonáhodné generace čísel. Náhodná čísla hrají v mnoha bezpečnostních aplikacích a celkově v šifrování velmi důležitou roli.

Prvním pojmem, nad kterým se musíme zamyslet, je náhodnost. Je velmi těžké vytvořit systém, který by striktně dodržoval onu náhodu. Obvykle se soustava řídí nějakým algoritmem a můžeme aspoň předpovídat výsledky nebo najít poměr ve výsledných hodnotách. Rozdělení bitů v sekvenci by tedy mělo být jednotné a poměr jedniček a nul přibližně stejný, abychom nebyli schopni najít vzor, dle kterého algoritmus pracuje. Druhou podmínkou, která by měla být dodržována generátorem náhodných čísel, je nezávislost. Žádná sekvence by neměla být možná určit jinou sekvencí.[3]

Pokud N značí soubor přirozených čísel a $\{f, K\}$ symbolizují pseudonáhodnost, tak můžeme zapsat pseudonáhodnou funkci $f: K \times N \rightarrow \{0,1\}^*$. K představuje klíčový prostor.

3.4 Jednosměrná hashovací funkce

Jednosměrná hashovací funkce je velmi snadno vypočitatelná, ale už mnohem hůře převratitelná. Důvod tohoto problému je velké množství potenciálních výsledků pro vstupní hodnoty. Velmi důležitá hashovací vlastnost je, že x v doméně $f(x)$ nesmí být ve tvaru polynomu, který by nabýval hodnot menších než x. Typickým příkladem hashovací kryptografické aplikace je MD5 a SHA.[3]

Pokud bychom chtěli spočítat hodnotu h (hashe) pro jakékoliv x v doméně, užijeme rovnici $f(x) = h$, kde x je předobrazem h. Účel hashovací funkce je získat takovou hodnotu h, se kterou bude jednáno jako s unikátně spojenou s předobrazem x pro praktické využití. Využitím kladných celých čísel Z^+a $\{f, D, R, l\}$ můžeme definovat hashovací funkci $f: D \times Z^+ \rightarrow R$, kde D je doména funkce, R je rozsah funkce a l je délka hashové hodnoty $l = |f\{x, l\}|$.[3]

3.5 Funkce padacích dveří a kryptografie veřejných klíčů

Funkce padacích dveří je další příklad jednosměrné funkce a je velmi důležitá pro kryptografii používající veřejný klíč. V tomto případě nám informace padacích dveří umožní vypočítat vratnost funkce. Tato vlastnost je charakterizována právě veřejným klíčem.

Při vytváření šifry se používají 2 klíče – šifrovací a dešifrovací. Každý uživatel umístí veřejně k dispozici kódovací klíč, ale dešifrovací si nechá pro sebe. Znamená to, že každý může použít algoritmus k zašifrování zprávy, ale jen majitel dešifrovacího klíče ho může přečíst.

Matematické definice použitím $\{f, g, M, C, K_p[f, g]\}$ prvků veřejného klíče bude vypadat takto $f: M \times K_f \rightarrow C$ a $g: C \times K_g \rightarrow M$ pro popis šifrující a dešifrující funkce.[3]

3.5.1 Diffie-Hellmanova výměna klíčů

Jako první navrhli práci s veřejným klíčem spolupracovníci Diffie a Hellman. Ve své práci popsali kryptografii s veřejným klíčem. Prvotním cílem byla realizace bezpečného předání klíče, který slouží k zašifrování dokumentu, mezi dvěma uživateli.[3]

3.5.2 RSA algoritmus

Vědci z MIT reagovali velmi rychle na Diffie-Hellmanovu práci a v roce 1978 byl vytvořen nový šifrující algoritmus RSA, jež v názvu nese iniciály svých tvůrců – Rivest, Shamir, Adleman. Toto kryptovací schéma je dodnes nejrozšířeněji používáno v rámci metod kryptografie veřejného klíče. S typickou velikostí 1024bitů RSA funguje na exponenciální bázi 2^n, kde n je právě počet bitů. Tento algoritmus je velmi složitým shlukem funkci, ale pro názornost ho můžeme matematicky popsat

$$C = M^e mod\ n \tag{3.5}$$

$$M = C^d mod\ n = (M^e)^d mod\ n = M^{ed} mod\ n, \tag{3.6}$$

kde M symbolizuje prostý text a C šifrovaný text. Pro všechny musí být známa hodnota n. Příjemce zná ještě hodnotu d a odesílatel hodnotu e. Z toho vyplývá, že veřejný klíč obsahuje hodnoty $PU = \{e, n\}$ a privátní klíč $PR = \{d, n\}$.[3]

3.6 Digitální podpis

Digitální podpis má nahradit klasický podpis ve formě potvrzení, že dotyčná osoba viděla dokument, který jí přišel, a je si jej vědoma. Každý takový podpis musí být spojen s danou osobou a daným dokumentem. Za pomoci vlastního privátního klíče je uživatel schopen potvrdit svoji identitu, protože je jediný, kdo dokáže vygenerovat podpis spojením s veřejným klíčem. Celý tento proces je závislý na kryptografii s veřejným klíčem.

Digitální podpis lze matematicky popsat užitím $\{f, g, M, S, K_p[f, g]\}$ prvků, kterými získáme ověřující a podepisující funkce $f: M \times S \times K_g \rightarrow \{TRUE, FALSE\}$ a $g: M \times K_f \rightarrow S$. v tomto příkladu M označuje zprávu a S značí podpis.[3]

3.7 Kvantová kryptografie

Kvantové počítače mohou pravděpodobně nabídnout kryptografii mnohem více než klasické počítače. Je to však stále jedna velká neznámá. Věda je v tomto smyslu pořád na začátku a aplikace těchto teorií bude velmi drahá a náročná. Nicméně už teď je fyzikálně potvrzená správnost kvantových teorií a jejich reálné výsledky v kryptografii a komunikaci mohou být ohromující.[4]

3.7.1 Teorie složitosti

Než popíšeme problematiku kvantové kryptografie, seznámíme se s používanou terminologií. Teorie složitosti se zabývá obtížností výpočetních problémů. Nejvýznamnějším měřítkem je asymptotický čas nebo prostor potřebný k realizaci algoritmu. Časová závislost může být definována několika způsoby. Od konstantního času $O(1)$, přes lineární a polynomiální čas $O(n)$ a $O(n^k)$ až po exponenciální čas $O(2^{n^k})$, kde k je časová konstanta.[3]

Třída složitosti P je problém řešitelný deterministickým Turingovým strojem v polynomiálním čase. Typickým představitelem takového stroje je digitální počítač. Názorným příkladem problému P je určení, zda je číslo prvočíslo nebo ne. Další třídou složitosti je PN, vycházející z nedeterministického Turingova stroje, který dokáže během výpočtu provádět odhad. Pokud tedy provede takový odhad, vykoná cestu k oběma výsledkům.[3]

Další třídou složitosti je BPP, která vychází z omezeného pravděpodobnostního Turingova stroje. Ten již byl popsán v kapitole č. 1 a jeho princip spočívá v implementovaném náhodném jevu. Pracuje na stejném principu jako předchozí Turingův stroj, jen se principem náhody může dostat k řešení rychleji.[3][5]

Jednoznačný Turingův stroj je vázaný na jednosměrné funkce. Používá právě jednu informaci na každém možném vstupním vláknu. Značení této třídy složitosti je UP a probíhá opět v polynomiálním čase.[3][5]

Další třída složitosti je zvaná *PSPACE*, je specifikována polynomiálním prostorem, ale není specifikována časem. Všechny zmíněné složitosti jsou podmnožinou *PSPACE*, ale není známo, v jakém přesně pořadí.[3][5]

3.7.2 Teorie složitosti ve vztahu ke kvantovým počítačům

V tomto případě jde o kvantový Turingův stroj, který je schopen operací z kvantové mechaniky. Značení třídy složitosti je BQP a funguje analogicky k BPP v klasických strojích. BQP probíhá v polynomiálním čase jako předchozí zástupci.

I mezi teoriemi klasického počítače lze velmi těžko najít souvislosti, v kvantových počítačích je to ještě složitější. V následujících kapitolách budou popsány vztahy, které jsou známé.

3.7.3 Známé vztahy klasických a kvantových složitostí

V roce 1977 představil John Gill svou práci, ve které popisuje závislost mezi složitostmi

$$P \subseteq BPP \subseteq PSPACE.$$

Jelikož platí vztah $P \subseteq NP \subseteq PSPACE$, není známo, jestli BPP je podmnožinou NP nebo naopak. Bernstein a Vazirani demonstrovali skutečnost závislostí mezi klasickým BPP a PSPACE s kvantovým BQT ve vztahu

$$BPP \subseteq BQP \subseteq PSPACE$$

Dle autora knihy *Handbook of Theoretical Computer Science* Davida S. Johnsona můžeme dále definovat známý vztah

$$P \subseteq UP \subseteq NP.$$

Grollmann a Selman dokázali ve své práci o kryptosystémech s veřejným klíčem, že jednosměrná funkce existuje pouze za předpokladu $P \neq UP$. Ačkoliv tento výrok nedává úplně smysl v případě hashovací funkce, jeho přínos byl značný. Vědci jsou přesvědčeni, že vztahy z této kapitoly jsou pravdivé a vše tomu nasvědčuje. Teoreticky je stále možné, aby dané vztahy typu $P \neq UP$ nebo $P = PSPACE$ neplatily.[3][5]

3.7.4 Implikace BPP = BQP ⊂ NP

Případ, kde $BQP = BPP$ a oba jsou podmnožinou NP nám nepřináší nic nového do kryptografie, protože vše důležité je již obsaženo v BPP. Nicméně se musíme aspoň zamyslet nad alternativou Shorova algoritmu u klasického BPP.[3][5]

3.7.5 Implikace BPP ⊂ BQP

V tomto případě připouštíme, že BPP je podmnožinou BQP. Nejpravděpodobnější problém v tomto vztahu bude faktorizace a diskrétní logaritmus, které jsou základem bezpečnosti pro většinu veřejných klíčů a digitálních podpisů v dnešní době. Nemáme důvod si myslet, že by digitální podpisy a veřejné klíče byly v tomto případě nemožné. Avšak konstrukcí kvantového počítače by určitě došlo k zániku alespoň některých kryptosystémů založených na faktorizaci a diskrétním logaritmu.[3][5]

3.7.6 Implikace UP ⊆ BQP

Výskyt této implikace je velice blízký vztahu $UP \subseteq P$. Pokud však platí $UP \subseteq P$, nemůže existovat žádná jednosměrná funkce. Na druhou stranu, vezmeme-li v potaz Grollmannovu a Selmanovu teorii a definujeme nerovnost $UP \neq P$, tak bude existovat jednosměrné řešení. Tato varianta je zatím ze všech nejméně reálná.[3][5]

3.7.7 Implikace NP ⊆ BQP

Tato implikace je momentálně nereálná, ale pokud by se dokázala její pravdivost, mělo by to obrovský dopad na současnou kryptografii. Principem této varianty je připuštění existence Turingova „zázračného stroje“[8].[3][5]

[8]Zázračný stroj – jedná se o abstraktní stroj, který je schopen řešit operaci jedním krokem (Turingův stroj s černou skříňkou)

4 Modely počítačů

4.1 Úvod do výpočetní techniky

Vývoj techniky kráčí mílovými kroky a každým rokem přibývá mnoho nových vynálezů a technologií. V dalších kapitolách si stručně popíšeme technologický vývoj od nejprimitivnějších vynálezů po moderní počítače a budeme se věnovat problematice kvantového počítače.

Tato bakalářská práce byla inspirována knihou *The Computer Book* od Simson L. Garfinkela a Rachel H. Grunspanové. Je velmi složité udělat komplexní souhrn všech důležitých vynálezů, a právě názory přispěly ke členění období a výběru zástupců.

4.2 Předchůdci počítačů

První vynálezy, které předcházejí dnešním pokročilým počítačům, se objevily již tisíce let před naším letopočtem. Byly založeny čistě na mechanických procesech a většina z nich byla poháněna lidskou silou. Toto období sahá až do počátku 20. století, kdy světlo světa spatřil první elektromechanický počítač.

4.2.1 Abakus

V Mezopotámii, v roce 2200 před naším letopočtem byl vyvinut první matematický nástroj zvaný Abakus. Doposud nebyl problém ve výpočtech, ale řešila se spíš problematika uchování informací. V ten moment přichází na scénu Abakus. Je to zařízení, připomínající dnešní dětská počítadla, schopné vykonávat základní matematické úkony jako sčítání, odečítání a za pomoci jednoduchých algoritmů i násobení a dělení. První sumerský abakus měl podobu hliněné ploché destičky, na které se prováděly výpočty a znázorňovaly se paralelními čárami a oblázkovými kamínky.

4.2.2 Antikythérský mechanismus

Z roku 150 před naším letopočtem pochází další mechanické zařízení důležité pro vývoj počítače. Jedná se o zařízení skládající se až z 30 zámkových bronzových kol, které sloužilo řeckém námořnictvu k orientaci na moři a k předpovědi astronomických jevů. Tento výtvor byl nalezen ve vraku lodi blízko řeckého ostrova Antikythera, podle kterého nese název. Posuvem manuální páky se mechanická kola dala do pohybu a zapříčinila pohyb několika prstenců

a čísel, které měly určovat polohu Slunce, Měsíce a planet. Mechanismus byl tak vyspělý, že dokázal předpovědět i fáze Měsíce, jeho zatmění a jiné kalendářní cykly.

4.2.3 Programovatelný robot

Heron z Alexandrie vymyslel zařízení schopné pohybu ve všech směrech a později byl označen Noelem Sharkeyem za tvůrce prvního programovatelného robota. Tento stroj o třech kolech byl zabudován do panenek nebo figurín a za pomocí provazů a závaží se pohyboval na tehdejších divadelních jevištích. Je to přímým důkazem, že Řekové a Římané byli schopni prvního principu programování již v prvním století našeho letopočtu.

4.2.4 Šifrovací disk

Šifrovací disk byl vytvořen v roce 1470 a sloužil jako první mechanické zařízení k záměně písmen. Jednalo se o 2 měděné kotouče. Vnější kotouč byl napevno připevněný a vytvářel šifru, vnitřní kotouč byl otočný a reprezentoval tvorbu reálného textu. Právě tento vynález byl předlohou pro vynález Blaise de Vigenéra, jehož šifra byla prolomena až v 19. století.

4.2.5 Mechanický Turek

V Rakousku, roku 1770 se Wolfgang von Kempelen ujal úkolu vytvořit zařízení, které by předčilo iluzionistické vystoupení v paláci Schönbrunn. Snažil se ohromit císařovnu Marii Terezii Rakouskou a povedlo se mu vytvořit „myslící“ stroj, který porazí kohokoliv v šachách. Mechanický Turek, jak byl tento stroj přezdíván, opravdu porazil téměř každého a na jeho listě poražených se objevila jména jako Benjamin Franklin, Edgar Allan Poe nebo Napoleon Bonaparte.

4.2.6 Diferenciální motor

Diferenciální motor byl výtvor Johanna Helfricha von Müllera a Charlese Babbage. Roku 1822 se těmto matematikům podařilo vytvořit automatizovaný stroj pro tabulkování a výpočet polynomiálních funkcí, který nahradil lidské, velmi často chybné, výsledky. Diferenciální stroj dokázal tisknout výsledky do děrných štítků, zvládal používat mezivýsledky a fungoval s přesností na 16 desetinných míst. Proto není divu, že byl předlohou vzniku některých dalších vynálezů typu ENIAC.[14]

4.2.7 Diferenciální analyzér

V roce 1931 byl sestrojen první analogický stroj poháněný elektrickou energií. Na jeho plánech a realizaci se podíleli Vannevar Bush a Harold Locke Hazen, kteří se snažili vytvořit stroj schopný samostatně počítat diferenciální rovnice. Díky tomuto mechanickému stroji, obsahujícímu desítky automatizovaných pák a ozubených kol, bylo porozuměno tuctům složitých fyzikálních teorií z oblastí seismologie, elektrických sítí nebo balistických výpočtů. Zdánlivě perfektní stroj měl jednu velkou vadu. Stále ho tvořily mechanické součásti a postupem času celý stroj chátral a způsoboval nepřesnosti ve výpočtech.[14]

4.3 Nultá generace

Mechanický stroj byl na vrcholu svého vývoje a jeho degradace v čase byla nepřekonatelnou překážkou. Mnoho vědců se snažilo přijít s novým principem pro efektivní řešení výpočtů. Naštěstí roku 1936 publikoval svou teorii Alan Turing a společně s Alonzem Churchem se postarali o teoretický popis abstraktního Turingova stroje. Jednalo se o zařízení schopné pracovat dle jakéhokoliv algoritmu a provést všechny výpočty. Jeho principy a vývoj byly již popsány v první kapitole.

4.3.1 Z1, Z2 a Z3

Německý inženýr Konrad Zeus se po získání svého vysokoškolského titulu ihned vrhl na vývoj svého prvního počítače. Pracovní název Z1 představoval mechanický kalkulátor ovládaný děrnými páskami. Přímo pro tento prototyp používal jako děrnou pásku kinofilm, což fungovalo na bázi 22-bitových číslech s plovoucí desetinnou čárkou, podporující Booleanovu algebru.

V roce 1939 bylo jeho zařízení leteckým náletem zničeno. Ve stejném roce byl však naverbován do německé armády, kde se pustil do vývoje druhého prototypu Z2. Vymyslel mnohem propracovanější design a celé toto zařízení fungovalo na principu telefonních relé pro aritmetickou a řídící logiku.

Německý výzkumný institut byl nadšen jeho výtvory, a tak zafinancoval celý jeho projekt a roku 1941 byl sestrojen třetí prototyp Z3. Tento model pracoval s 32-bitovou matematikou s podmíněnými skoky. Německo bohužel nikdy nevyužilo potenciál těchto zařízení.

4.3.2 ABC

Ani Spojené státy Americké nezůstaly pozadu a v roce 1942 přišel profesor John Atanasoff a jeho student Clifford Berry s novým modelem digitálního počítače. Předpokladem vzniku modelu ABC bylo řešení lineárních rovnic o maximální hodnotě 29 neznámých. Ačkoliv toto zařízení, vážící přes 300 kg, počítalo řešení několik hodin, jeho vzor byl velmi důležitý pro vývoj modernějších počítačů.

4.3.3 Colossus

Dalším představitelem počítačů nulté generace byl Colossus. Britské zařízení, používající přes 765 000 elektromechanických součástek, bylo schopno dešifrovat německé šifrovací zařízení Enigma. Tento kolos s pracovním názvem Mark I poháněl motor o příkonu téměř 4 kW.

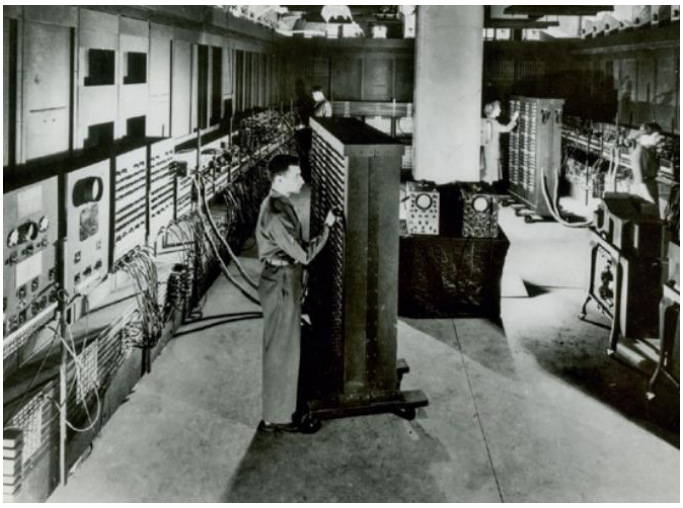
Howard Hathaway Aiken, spoluautor modelu Mark I, se následně pustil do realizace modelu Mark II. Počítač přešel z elektromechanických součástek na relé (resp. 13000 relé) a byl schopen provést operace jako sčítání a násobení v řádech desetin sekund. Velký zájem o tento počítač projevila armáda a ten se stal její nedílnou součástí.

4.4 První generace

V tomto krátkém časovém úseku, přibližně od roku 1945 do roku 1950, se vývoj počítače zaměřil na vakuové elektronky, které měly plně nahradit relé. Bohužel ještě neexistovaly operační systémy, a tak realizace a obsluha počítačů na principu elektronek byla velmi náročná.

4.4.1 ENIAC

ENIAC bylo první elektrické zařízení, které můžeme pojmenovat počítač. Relé plně nahradily elektronky a celý tento stroj vážil 300 tun, měřil přes 30 m a sahal do výšky 2,5 metru. Obsahoval 17 468 elektronek, čtecí děrovou kartu na vstupu a další děrovou kartu na výstupu. Samotný počítač nedokázal ukládat informace, a proto se používaly počítačové akumulátory, které byly schopny uložil číslo o deseti cifrách a provést základní matematické operace. Prvotní záměr ENIACu byl výpočet balistických střel pro americkou armádu. John von Neumann, vědec podílející se na projektu Manhattan, se však o počítači dozvěděl a využil ho pro výpočty a vývoj první vodíkové bomby. Neumannem upravená verze ENAICu nesla název MANIAC.



Obrázek č. 9: První elektronický počítač ENIAC[7]

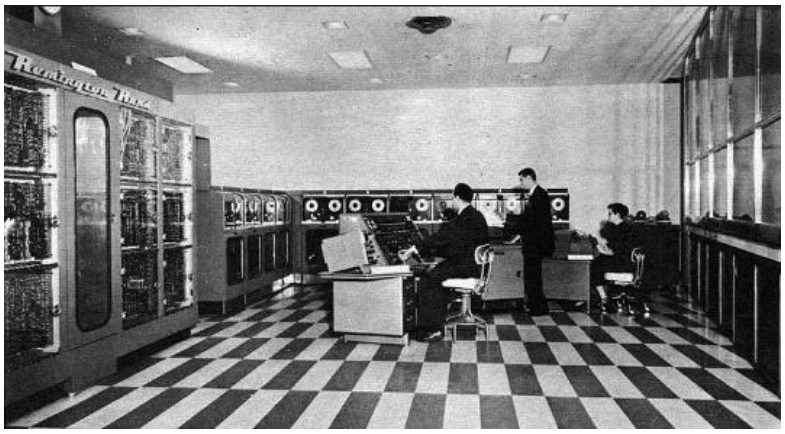
4.5 Druhá generace

Ve druhé generaci vývoje počítačů se setkáváme s pojmem *tranzistor*. Jedná se o polovodičovou součástku, která je schopna zesilovat proud nebo napětí, a i malá změna na vstupu dokáže způsobit velké rozdíly na výstupu. Toto období řadíme do 60. a na počátek 70. let.

Setkáváme se zde také s magnetickými páskami, které nahrazují dosavadní děrné pásky a štítky. Vyvíjí se i první operační systémy pro samostatnou obsluhu počítače.

4.5.1 UNIVAC

Nejznámějším zástupcem této generace je počítač UNIVAC. Jednalo se o stroj používající magnetické kovové pásky pro ukládání dat a byl to první komerčně vyráběný počítač na světě. Skládal se z 5000 elektronek a na jeho realizaci se podílel i John von Neumann. Nehledě na programovací jazyk základní jednotkou UNIVACu bylo slovo. Každé slovo se skládalo z 12 znaků a k dispozici jich měl 63. Magnetická páska umožňovala počítači uložit až 1000 slov a zobrazoval je v tzv. „boxech“ pro lepší chápání.[31]



Obrázek č. 10: Obecný pohled na počítač UNIVAC[31]

4.5.2 ANITA

V roce 1961 byla představena první komerčně prodávaná kalkulačka. Obsahovala 10 tlačítek pro každou desetinnou pozici a prodávala se za cenu 1000 dolarů nebo 355 liber.

4.6 Třetí generace

Společnost IBM přišla s novou teorií, jak počítač efektivně zmenšit, zrychlit a zlevnit. Firma se snažila o tvorbu integrovaných obvodů, ve kterých by se nacházelo, co nejvíce integrovaných tranzistorů. V závislosti na vývoji integrovaných obvodů se začíná objevovat pojem multitasking. Na konci 70. let se také objevují první koncepty minipočítačů a mikropočítačů.

Mimo klasické počítače se v této době objevila spousta dalších vynálezů spjatých s počítači a důležitých periferních zařízení pro snazší ovládání počítačů. Můžeme jmenovat vývoj LCD displejů, prvního dotykového displeje nebo prvního bankomatu. Nemůžeme opomenout ani první počítačovou myš (zdaleka ne takovou jakou známe dnes), první médium na přenos informací (disketu) nebo laserovou tiskárnu.

4.6.1 IBM System 360

Typickým představitelem třetí generace počítačů je počítač System 360 od společnosti IBM. Jejich úmyslem bylo vytvořit samostatnou počítačovou architekturu, která by umožňovala softwaru spravovat všechny systémy IBM počítačů. Počítač neobsahoval žádné elektronky a fungoval pouze na bázi integrovaných obvodů. Postupem času se vyrobilo několik verzí tohoto počítače a všechny byly zpětně kompatibilní. Obsah paměti se pohyboval v rozsahu 8 tisíc až 8 milionů znaků a jednalo se o jeden z největších průlomů moderní historie.

Společnost IBM investovala více než 5 miliard dolarů do vývoje počítače a konstrukce továren na jeho realizaci. Jen za první rok prodeje těchto modelů se firmě vrátila miliarda dolarů zpět. Fred Brooks, projektový manažer, byl v roce 1999 oceněn A. M. Turingovým oceněním za práci na počítačové architektuře, operačním systému a vývoji softwaru.

4.7 Čtvrtá generace

Čtvrtá generace počítačů započala kolem roku 1970 a trvá do dnes. Hlavním indikátorem této doby je vznik mikroprocesorů a výroba osobních počítačů pro soukromé využívání. Společnost INTEL se stala známou v roce 1971, když představila prototyp svého mikroprocesorového čipu s pamětí o kapacitě 1024 bitů. Stejného roku vydali model 4004, který byl základem prvního klasického počítače. Mikroprocesor obsahoval 2300 tranzistorů v jednom integrovaném obvodu. Tato verze měla velikost pouze 4 bity a hodila se jen do kalkulaček. Jeho nástupce, 8008, byla 8bitová kopie původní verze. Na trh vešla o pár měsíců později a měla paměťovou kapacitu až 16 384 bytů. Všechny mikroprocesory používají stejný kód, který byl později používán u Intel Pentium procesorů. Kód zůstal principově neměnný i u dnešních Intel Core procesorů.

4.7.1 Altair 8800

Do roku 1974 nebylo možné koupit vlastní počítač. Jedinou možnost, jak jej získat, bylo vyrobit si ho z dostupných částí. S nápadem pro vlastní podnikání se toho zhostil Henry Edward Roberts a začal skládat počítačové modely. Tyto počítače obsahovaly mikroprocesory Intel 8080 a neměly žádný monitor ani klávesnici. Z výstupů byly značeny výsledky světly a uživatel si musel vymyslet vlastní program pro jeho obsluhu. V roce 1975 se jeho počítač, Altair 8800, dostal po prodeji pěti tisíc kusů do novinového článku. Tohoto výtisku si všiml Bill Gates a Paul Allen a krátce na to přišli s programovacím jazykem Altair BASICS.

4.7.2 Apple II

V roce 1977 přišel na trh nový osobní počítač. Pracovali na něm Steve Wozniak, hlavní designér, a Randy Wigginton, programátor. Společně s promotérem Stevem Jobsem se jejich produkt, Apple II, stal velmi úspěšným sériově vyráběným počítačem. Jako první přišli s barevným textem na monitoru a také byli autory pěti a čtvrt palcové diskety, která plnila funkci inovace softwaru počítače.

4.7.3 IBM PC

Atari oslovila společnost IBM, jestli by se nepodílela na dalším vývoji počítačů s nimi. William Love, ředitel IBM, však smetl nabídku ze stolu a začal vyvíjet nový vlastní počítač.

V roce 1981 firma přišla s modelem IBM Personal Computer 5150, jehož 16-bitový procesor poskytoval 16kibibytovou paměť, rozšířitelnou až na 256 kibibytů. S počítačem byla dodána profesionální klávesnice a byly na výběr dva typy monitorů – monochromatický nebo barevný grafický. Po úspěšných testech byl prototyp poslán do společnosti Microsoft, která se věnovala dalšímu vývoji. Během prvního roku, co byl model uveden do prodeje, bylo prodáno přes 750 000 kusů.

Obrázek č. 11: IBM PC[7]

4.8 Kvantový počítač

Dnešní mobilní telefony by strčily do kapsy kterýkoliv ze zmíněných počítačů. Mikroprocesory jsou stále menší, paměťová kapacita je stále větší a všechny tyto systémy jsou stále dostupnější. Předpokládaná platnost Moorova zákona byla do roku 2020. Ačkoliv vývoj procesorů pokračuje stále vpřed, je na čase přijít s nějakým novým technologickým přístupem.

Albert Einstein tvrdil, že není možné přenést informaci rychleji než rychlostí světa. Tuto teorii pojmenoval „strašidelná akce na dálku“. Význam tohoto tvrzení si vysvětlíme na následujícím příkladu. Představme si, že jsme v New Yorku a vyžádáme si webovou stránku z Londýna. Latence nebude menší než 0,01 sekundy, protože vzdálenost Londýn – New York

(cca 5 585 kilometrů) bude trvat světlu 0,0186 sekundy, aby ji překonalo. Pokud se však podíváme na Einsteinovu speciální teorii relativity do kvantového světa, je tomu stále tak?

V posledních několika letech se vědci zabývali vyvrácením mnoha teorií užitím kvantové mechaniky A právě jedna z nich je nahrazení částice světla kvantovým propletením. Tyto teorie jsou stále v zárodku a nikdo přesně neví, co můžeme očekávat.

Kvantové počítače jsou stále ve vývoji a dodnes neexistuje zařízení, které by přesně plnilo představy kvantového počítače.

4.8.1 D-Wave

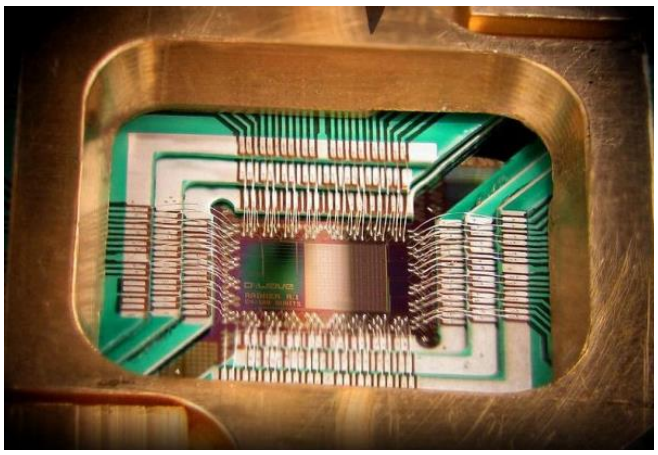
Nejnovější model *D-Wave 2000Q* byl představen roku 2017. Celý tento systém operuje v extrémních podmínkách – téměř absolutní nula (0,015 K). Důvodem těchto teplot je materiál, ze kterého je vyroben QPU (kvantová obdoba CPU). Kvantový mikroprocesor je vyroben z niobia, které je při teplotách pod 9,2 K supravodivé a vykazuje efekty kvantové mechaniky. Kvantový čip obsahuje 128 000 Josephonových tunelových přechodů[9], jež jsou tvořeny 2000 qubity a 5600 supravodivými spojkami. Při dodaném výkonu 25 kW je kvantový počítač 10 000x výkonnější než klasický superpočítač. D-Wave typy počítačů jsou určené pro tzv. *annealing*[10] a nejsou schopné práce se Shorovým algoritmem. Odhadovaná cena tohoto modelu je 15 milionu dolarů.[23][28]

Obrázek č. 12: Nejnovější model kvantového počítače D-Wave 2000Q[23]

[9] Quantum annealing – proces nalezení globálního minima dané funkce nad danou sadou kandidátních řešení
[10] Josephonův tunelový přechod – vznik elektrického proudu mezi dvěma supravodiči oddělenými tenkou vrstvou izolantu (Josephonův jev)

4.8.2 IBM Q System One

V lednu roku 2019 byl představen nový komerčně prodávaný model kvantového počítače *IBM Q Systém One*. Jeho kvantový mikroprocesor obsahuje 20 qubitů. Není to málo ani moc, jeho stabilita a dostatečná schopnost výpočtů je však důvodem realizace tohoto počítače.[29]



Obrázek č. 13: 128-bitový kvantový procesor[23]

5 Porovnání klasického a kvantového počítače

5.1 Základní jednotka bit/qubit

Pokud porovnáme klasický počítač a kvantový počítač, je potřeba začít od nejmenší jednotky bit/qubit.

V momentě měření se obě tyto jednotky jeví jako totožné. Mají výstup 0 nebo 1 a žádný jiný stav nepřipadá v úvahu. Pokud proces bude probíhat v kvantovém prostředí a jestliže připustíme kvantový jev, základní jednotkou je qubit. Z důvodu superpozice pravděpodobnostního stavu se kvantový bit může vyskytovat kdekoliv v rozmezí od 0 do 1. Matematické označení pro logické stavy qubitu jsou z Diracovy teorie symboly $|0\rangle$ a $|1\rangle$.

5.2 Mikroprocesory a realizace

Mikroprocesory jsou součástí všech složitějších elektronických zařízení. Jedná se o programovatelnou procesní jednotku, která slouží ke zpracování dat, jejich uložení a následné interpretaci.

CPU, *central process unit,* je základní procesní jednotka klasického počítače. Jedná se o integrovaný obvod, který může obsahovat 1-16 jader a během jedné operace může čip přenést až 128 bitů. QPU, *quantum process unit*, je základní jednotkou kvantového počítače. Nejběžnější typ, který využívá i kvantový počítač D-Wave, je 128qubitová verze procesoru Rainer. V plánu už jsou i 256qubitové nebo 1024qubitové procesory.

Opět se dostáváme k rozdílu bit/qubit. Kvantový procesor dokáže oproti klasickému pracovat se všemi qubity současně a navyšováním stavu qubitů v QPU budeme brzy schopni zpracovávat více úloh efektivněji a rychleji.

Výhoda CPU oproti QPU spočívá v jednoduchosti provozu. CPU je integrovaný obvod na křemíkové destičce. Právě křemíková destička slouží jako polovodič a může zastávat roli izolantu i vodiče (dle potřeby). Klasický mikroprocesor obsahuje milióny tranzistorů, které jsou propojeny hliníkovými nebo měděnými drátky. Dohromady tento systém zpracovává data a provádí důležité logické funkce a výpočty, které od procesoru vyžadujeme. Chlazení obstarává větráček a univerzální teplo vodivá pasta. Kvantový procesor funguje na podobném principu. Je však velmi složité dosáhnout podmínek, ve kterých platí kvantové jevy. QPU musí být ve vakuu a ke spuštění kvantových jevů je potřeba dosáhnout co nejnižší teploty. Kvantový

počítač D-Wave používá materiál niobium a pomocí chlazeného helia je dosažena teplota 9,2K, která je postačující k funkci kvantového čipu.

5.3 Kryptografie

Kryptografie je z hlediska kvantové teorie velkou neznámou. Jsme na počátku vývoje prvních kvantových počítačů a už teď máme poměrně dobrou představu rychlosti a potenciálu těchto strojů.

Ve svém článku *Nejasná budoucnost kryptografie?* uvádí Vladimír Beneš velmi zajímavý příklad. K prolomení 128-bitového hesla by současné počítače potřebovaly přes 10 triliónů let. Takové číslo si člověk reálně nedokáže ani představit a s předpokladem, že cena informace každým dnem ztrácí na hodnotě, je tento případ absurdní. Kvantovému počítači by však stačil k prolomení této šifry čas v řádech hodin, dní nebo týdnů.

Pokud by byl sestrojen kvantový počítač, který by byl schopen prolomit vojenské šifrování během několika sekund, co potom? Jednou z možností, jak dešifrování zabránit, by mohla být kvantová teleportace. Tato teorie pojednává o vzájemné provázanosti dvou částic. Akce na jednom prvku vyvolá okamžitou změnu na částici druhé, která může být vzdálena tisíce kilometrů od první částice. Tato teorie je bohužel zatím nejasná a její realizace je v nedohlednu. Kvantová kryptografie je druhé možné řešení, jak zabránit dešifrování. Na pochopení této problematiky si však budeme muset ještě pár let počkat. Informace z této oblasti drží nadnárodní společnosti v tajnosti.

5.4 Ekonomická stránka

Momentální cena kvantových počítačů se pohybuje kolem 15 miliónu dolarů. Pro běžného člověka je to obrovská suma. Pokud se však podíváme do historie, tehdejší předchůdci klasických počítačů měly cenu podobnou. Už teď se předpovídá, že velikost a cena kvantových počítačů bude značně klesat a že budou mít podobný ekonomický vývoj jako počítače klasické.

Pokud řešíme ekonomičnost, nezmiňujeme pouze cenu výrobku. Důležitá je i náročnost na výrobu, materiály a spotřeba energie. Vědci se snaží nahradit drahé materiály v kvantových počítačích a první pokusy o náhradu niobia křemíkem se právě realizují. Modely D-Wave se pyšní spotřebou energie 25 kW. Výhoda kvantové počítače je neměnná náročnost výkonu při maximálním využití. Superpočítače oproti tomu dosahují spotřeby až několika tisíc kW.

Závěr

Tato práce se věnovala popisu kvantových počítačů a jejich srovnání s počítačem klasickým. Byl zde popsán vývoj od antických mechanických zařízení až po moderní klasické a kvantové počítače. Dále byl vysvětlen princip kvantové teorie, jeho aplikace na kvantové počítače a algoritmy je obhospodařující. Součástí této práce je i kryptografie a její vývoj s příchodem kvantových systémů.

Ačkoliv je možné říct, že vývoj kvantových počítačů je velmi rychlý, stále nejsme schopni využít naše znalosti k realizaci takového stroje, jaký bychom si představovali. Používání prvních modelů typu D-Wave nebo IBM je velmi složité. Tato zařízení jsou schopna plnit pouze testovací úkoly a s navyšujícími se nároky vzniká stále více chyb a problémů. Vznik univerzálního kvantového počítače schopného Shorova algoritmu je v nedohlednu, a nemusíme se tedy obávat prolomení asymetrických šifer s veřejným klíčem. Podle odhadů by měl první takový počítač vzniknout do dvaceti až třiceti let.

V blízké době nebude kvantový počítač dostupný pro běžného člověka. Jeho funkce je vázána na extrémní podmínky z hlediska teplot (až -273 °C), vakua či prostoru. Materiál niob, ze kterého jsou vyrobeny kvantové čipy, je také poměrně vzácný, neboť jeho obsah v zemské kůře je pouze 15 mg na kg. I kdybychom byli schopni vytvořit pro kvantový počítač vhodné prostředí, dalším faktorem jeho nedostupnosti je cena, která se momentálně pohybuje v řádech desítek milionů dolarů.

Shrneme-li si všechny poznatky, budoucnost kvantového počítače je velmi slibná. Realizace takového stroje by změnila chod lidstva a kryptologové celého světa se snaží vymyslet šifru, která by odolala i kvantovému počítači. Prozatím si však musíme vystačit s počítači bez užití kvantových jevů a můžeme jen odhadovat, co nám přinese technologie příštích let.

Seznam použité literatury

[1] AARONSON, Scott Joel. *Limits on Efficient Computation in the Physical World*. Berkeley, 2004. Disertace. University of Carolina.

[2] ARNDT, Markus a Anton ZEILINGER. Hledáme hranice kvantového světa I. *Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie Aldebaran*. 2009, **7**(33). ISSN 1214-1674.

[3] BARRENO, Marco A. *The Future of Cryptography Under Quantum Computers*. 2002. Senio Honors. Dartmouth College.

[4] BENEŠ, Vladimír. *NEJASNÁ BUDOUCNOST KRYPTOGRAFIE?*. Praha, 2018. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS, a.s.

[5] BENJAMIN, Eric, Kenny HUANG, Amir KAMIL a Jimmy KITTIYACHAVALIT. *Quantum Computability and Complexity and the Limits of Quantum Computation*. Berkeley, 2003. University of Carolina.

[6] DEUTSCH, David. *Quantum theory, the Church-Turing principle and the universal quantum computer*. Oxford, 1999.

[7] GARFINKEL, Simson L. a Rachel H. GRUNSPAN. *The Computer Book*. New York: STERLING, 2018. ISBN 978-1-4549-2622-1.

[8] HÁLA, Vojtěch a Anton ZEILINGER. Kvantová teleportace. *Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie Aldebaran*. 2004, **2**(31). ISSN 1214-1674.

[9] HÁLA, Vojtěch. Kvantová kryptografie. *Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie Aldebaran*. 2008, **1**(14). ISSN 1214-1674.

[10] IMRE, Sandór a Ferenc BALÁZS. *Quantum Computing and Communications*. West Sussex: John Wiley & Sons, 2005. ISBN 0-470-86902-X.

[11] KAYE, Philip, Raymond LAFLAMME a Michele MOSCA. *An Introduction to Quantum Computing*. New York: Oxford University Press, 2007.

[12] KULHÁNEK, Petr a Anton ZEILINGER. Kvantové počítače. *Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie Aldebaran*. 2004, **1**(21). ISSN 1214-1674.

[13] KULHÁNEK, Petr a Anton ZEILINGER. Kvantové počítače – principy. *Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie Aldebaran*. 2009, **15**(37). ISSN 1214-1674.

[14] MUSÍLEK, Michal. *Kapitoly z dějin informatiky 1: Od starověku do 19. století*. Hradec Králové, 2010. Pedagogická fakulta UHK.

[15] NIELSEN, Michael A. a Isaac L. CHUANG. *Quantum Computation and Quantum Information*. New York: Cambridge University Press, 2010. ISBN 978-1-107-00217-3.

[16] STALLINGS, William. *Cryptography and Network Security*. 6th. New Jersey: Pearson, 2014. ISBN 978-0-13-335469-0.

[17] TALELE, Nikhil, Ajinkya SHUKLA a Sumant BHAT. Can Quantum Computers Replace the Classical Computer?. *International Journal of Engineering and Advanced Technology*. 2002, , 4. ISSN 2249 – 8958.

[18] WILDE, Mark M. *From Classical to Quantum Shannon Theory*. 2nd. Cambridge University Press, 2019.

Internetové zdroje

[19] BLAIN, Rebecca. The Evolution of Technology - The History of Computers. *Www.streetdictionary.com* [online]. [cit. 2019-08-02]. Dostupné z: https://www.streetdirectory.com/travel_guide/2123/computers_and_the_internet/the_evolution_of_technology___the_history_of_computers.html

[20] CUMMINGS, Tucker. Short summary of the History of Computers. *Www.techwalla.com* [online]. [cit. 2019-08-02]. Dostupné z: https://www.techwalla.com/articles/history-evolution-of-computers

[21] DAVIDOVÁ, Andrea. Někdejší výpočetní pomůcky. *Www.fi.muni.cz* [online]. [cit. 2019-08-02]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/xdavidov.html

[22] Dějiny počítačů. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-08-02]. Dostupné z: https://cs.wikipedia.org/wiki/D%C4%9Bjiny_po%C4%8D%C3%ADta%C4%8D%C5%AF

[23] The D-Wave 2000Q™ System. *Www.dwavesys.com* [online]. [cit. 2019-08-02]. Dostupné z: https://www.dwavesys.com/d-wave-two-system

[24] *History of computers* [online]. 2019 [cit. 2019-08-02]. Dostupné z: https://history-computer.com/

[25] HOUSER, Pavel. Kvantové počítače: kde zůstává zdravý rozum stát. *Www.scienceworld.cz* [online]. [cit. 2019-08-02]. Dostupné z: https://www.scienceworld.cz/neziva-priroda/kvantove-pocitace-kde-zustava-zdravy-rozum-stat-4435/

[26] HUI, Jonathan. QC — The strength and the weakness of Qubits in Quantum Computing. *Www.medium.com* [online]. [cit. 2019-08-02]. Dostupné z: https://medium.com/@jonathan_hui/qc-the-strength-and-the-weakness-of-qubits-in-quantum-computing-dc54c442fcb3

[27] HUI, Jonathan. QC — What are Qubits in Quantum computing?. *Www.medium.com* [online]. [cit. 2019-08-02]. Dostupné z: https://medium.com/@jonathan_hui/qc-what-are-qubits-in-quantum-computing-cdb3cb566595

[28] JAVŮREK, Karel. D-Wave 2000Q: nový model kvantového počítače je až tisíckrát výkonnější než předchozí generace. *Www.connect.zive.cz*[online]. 2017 [cit. 2019-08-02]. Dostupné z: https://connect.zive.cz/clanky/d-wave-2000q-novy-model-kvantoveho-pocitace-je-az-tisickrat-vykonnejsi-nez-predchozi-generace/sc-320-a-185826/default.aspx

[29] MIHULKA, Stanislav. Společnost IBM představila světu kvantový počítač Q System One. *Www.osel.cz* [online]. 2019 [cit. 2019-08-02]. Dostupné z: http://www.osel.cz/10304-spolecnost-ibm-predstavila-svetu-kvantovy-pocitac-q-system-one.html

[30] ROWLAND, Todd. Church-Turing Thesis. *Www.mathworld.wolfram.com* [online]. [cit. 2019-08-02]. Dostupné z: http://mathworld.wolfram.com/Church-TuringThesis.html

[31] UNIVAC. *Www.museo.inf.upv.es* [online]. [cit. 2019-08-02]. Dostupné z: http://museo.inf.upv.es/en/univac/

[32] VOJÁČEK, Antonín. Kvantový počítač – princip, funkce, možné použit. *Www.vyvoj.hw.cz* [online]. 2012 [cit. 2019-08-02]. Dostupné z: https://vyvoj.hw.cz/teorie-a-praxe/trendy/kvantovy-pocitac-princip-funkce-mozne-pouziti.html

Seznam obrázků

Seznam zkratek

AES – Advanced Encryption Standard (standard pokročilého šifrování)

CNOT – Controlled-NOT brána

CPU – Central Processing Unit (centrální procesorová jednotka)

DES – Data Encryption Standard (standard pro šifrování dat)

DFT – Diskrétní Fourierova Transformace

FFT – Rychlá Fourierova Transformace

MD5 – Message-Digest Algorithm (jednosměrná matematická funkce)

QFT – Kvantová Fourierova Transformace

QPU – Quantum Processing Unit (kvantová procesorová jednotka)

RSA – šifra s veřejným klíčem (Rivest, Shamir, Adleman)

SHA – Secure Hash Algorithm (bezpečná hashovací funkce)

WPA2 – Wi-Fi Protected Access (šifrovací algoritmus pro bezdrátové sítě)

Seznam tabulek