Študijný materiál

**Úvod do kvantových počítačov**

Ivan Polák

II.D

Ročníkový projekt

Obsah

[1. Úvod do kvantových počítačov 1](#_Toc158566539)

[Vznik a vývoj 1](#_Toc158566540)

[Základné princípy 2](#_Toc158566541)

[Výhody a výzvy 2](#_Toc158566542)

[Budúcnosť 2](#_Toc158566543)

[2. Základy kvantovej mechaniky 2](#_Toc158566544)

[Vlnová funkcia a stavový priestor 2](#_Toc158566545)

[Superpozícia 2](#_Toc158566546)

[Kvantová prepletenosť 3](#_Toc158566547)

[Zrážková pravdepodobnosť 3](#_Toc158566548)

[Heisenbergov princíp neurčitosti 3](#_Toc158566549)

[Interpretácie kvantovej mechaniky 3](#_Toc158566550)

[3. Qubyty a kvantové hradlá 3](#_Toc158566551)

[4. Kvantové algoritmy 3](#_Toc158566552)

[5. Aplikácie kvantových počítačov 3](#_Toc158566553)

[6. Bezpečnosť a kvantové počítače 4](#_Toc158566554)

[Faktorizácia veľkých čísel 4](#_Toc158566555)

[Bezpečnostné protokoly 4](#_Toc158566556)

[Post-quantum kryptografia 4](#_Toc158566557)

[Overovanie a šifrovanie 4](#_Toc158566558)

[Etické aspekty 4](#_Toc158566559)

[7. Architektúry kvantových počítačov 6](#_Toc158566560)

[8. Kvantová suprampočítačovosť 6](#_Toc158566561)

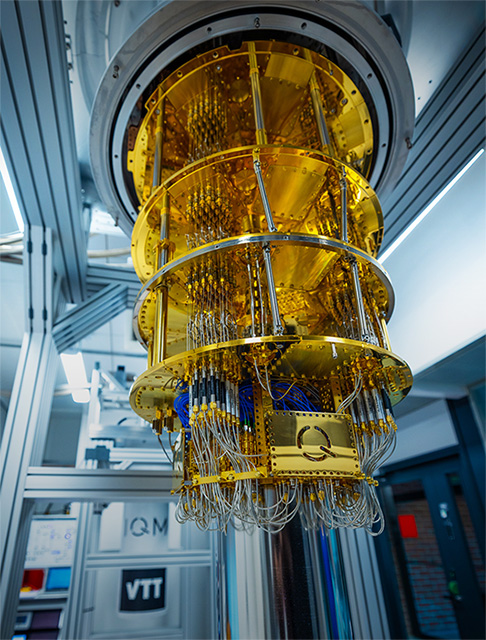
[9. Perspektívy a výzvy 6](#_Toc158566562)

[10. Záverečné myšlienky 6](#_Toc158566563)

[11. Zdroje 6](#_Toc158566564)

# 1. Úvod do kvantových počítačov

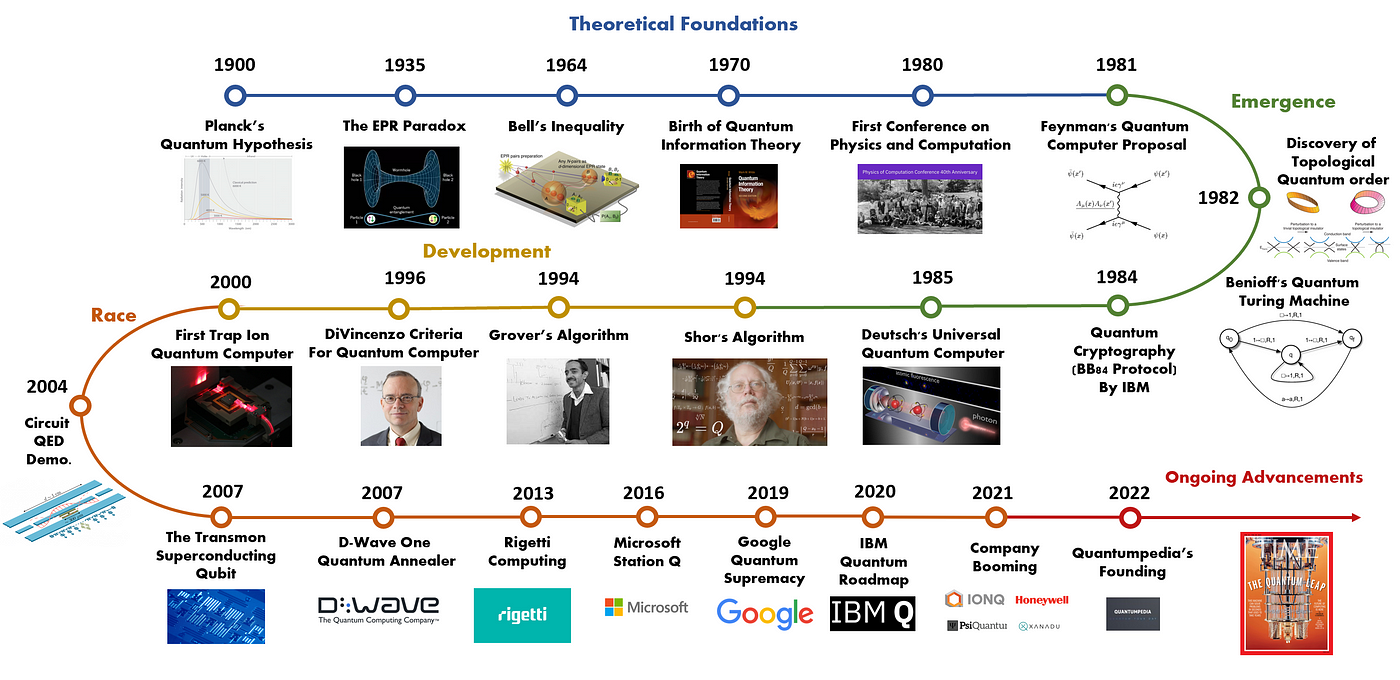
Kvantové počítače predstavujú revolučný pokrok vo svete výpočtovej technológie. Ich schopnosť vykonávať výpočty na úrovni, ktorá je neuskutočniteľná pre klasické počítače, otvára dvere k novým možnostiam v mnohých oblastiach, vrátane vedy, priemyslu a vojenských aplikácií.



Obrázok 1 - Kvantový počítač

## Vznik a vývoj

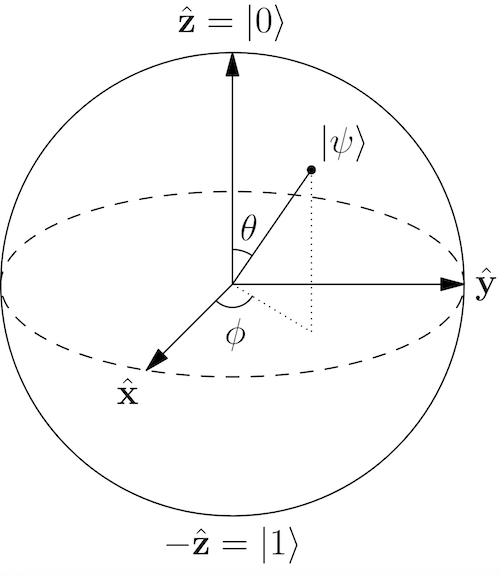
V roku 1981 Richard Feynman predstavil myšlienku vytvorenia počítačov založených na princípoch kvantovej mechaniky. Avšak prvý skutočný krok smerom k vývoju kvantových počítačov nastal v roku 1994, keď Peter Shor predstavil algoritmus na efektívne faktorizovanie veľkých čísel, čo by mohlo mať významné následky pre kryptografiu.



Obrázok 2 - História

## Základné princípy

Kvantové počítače sa líšia od klasických počítačov v tom, že využívajú qubity (Obrázok 1) namiesto bitov na reprezentáciu informácií. Zatiaľ čo bit môže byť buď 0 alebo 1, qubit môže byť v superpozícii týchto stavov, čo znamená, že môže byť súčasne 0 a 1. Okrem toho môžu qubity byť vzájomne prepletené, čo umožňuje kvantovým počítačom vykonávať určité úlohy výrazne rýchlejšie, ako je to možné pre klasické počítače.



Obrázok 3 - Qubit

## Výhody a výzvy

Hlavnou výhodou kvantových počítačov je ich schopnosť riešiť určité problémy rýchlejšie, ako je možné pomocou klasických počítačov. To otvára dvere k novým možnostiam v oblastiach ako kryptografia, chemické a biologické simulácie, optimalizácia a umelá inteligencia. Avšak vývoj kvantových počítačov je stále v ranom štádiu a existujú mnohé technické výzvy, ktoré je potrebné prekonať, ako sú chyby v kvantovom hardvéri, nedostatok škálovateľnosti a náročné algoritmy.

## Budúcnosť

Budúcnosť kvantových počítačov je plná možností a prísľubov. Ich úplné využitie by mohlo mať významné dôsledky pre mnohé odvetvia a priniesť nové technologické inovácie, ktoré by mohli zmeniť spôsob, akým vykonávame výpočty a riešime komplexné problémy.

Toto je len začiatok cesty, ktorá nás zavedie do sveta kvantových počítačov. Čakajú nás vzrušujúce objavy, technologické pokroky a nové aplikácie, ktoré môžu zmeniť náš svet.

# 2. Základy kvantovej mechaniky

Kvantová mechanika je teória, ktorá popisuje správanie sa veľmi malých častíc, ako sú atómy, fotóny a elektróny, na mikroskopickej úrovni. Rozdiel medzi klasickou a kvantovou mechanikou spočíva v tom, že kvantová mechanika využíva koncepty ako superpozícia, kvantová prepletenosť a pravdepodobnostné interpretácie.

## Vlnová funkcia a stavový priestor

Kľúčovým pojmom v kvantovej mechanike je vlnová funkcia, ktorá popisuje pravdepodobnosť nájdenia častice v určitom stave. Stav častice je reprezentovaný v stavovom priestore, ktorý sa nazýva Hilbertov priestor. Vlnová funkcia je všeobecným popisom stavu kvantového systému.

## Superpozícia

Superpozícia je fenomén, ktorý umožňuje kvantovým časticám existovať v kombinácii rôznych stavov s rôznymi pravdepodobnosťami. To znamená, že kvantové častice môžu byť v superpozícii viacerých stavov súčasne.

## Kvantová prepletenosť

Kvantová prepletenosť je jav, ktorý umožňuje kvantovým časticám byť vzájomne spojené tak, že ich vlastnosti nie je možné nezávisle popísať. To znamená, že stav jednej častice je neoddeliteľne spojený so stavom druhej častice, bez ohľadu na vzdialenosť medzi nimi. Kvantová prepletenosť je kľúčovým pojmom v kvantovej mechanike a má dôležitý význam pri kvantových výpočtoch a komunikácii.

## Zrážková pravdepodobnosť

Zrážková pravdepodobnosť je kvantový jav, ktorý popisuje pravdepodobnosť, že kvantové častice sa budú správať ako vlny a prechádzať cez prekážky. Tento jav sa prejavuje napríklad v dvojštrbinovom experimente, kde častice môžu prejsť cez dve úzke štrbiny a vytvárať interferenčné vzory na detektore za štrbinami.

## Heisenbergov princíp neurčitosti

Heisenbergov princíp neurčitosti je základným princípom kvantovej mechaniky, ktorý hovorí, že nie je možné presne určiť súčasne polohu a hybnosť kvantovej častice. Tento princíp má dôležité dôsledky pre meranie a pozorovanie kvantových systémov.

## Interpretácie kvantovej mechaniky

Existuje niekoľko rôznych interpretácií kvantovej mechaniky, ktoré sa pokúšajú vysvetliť význam a interpretáciu kvantových javov. Niektoré z najznámejších interpretácií zahŕňajú Kodaňskú interpretáciu, mnoho-svetostranný prístup a de Broglie-Bohmovu interpretáciu.

Kvantová mechanika je základnou teóriou, ktorá leží v základoch kvantových počítačov. Porozumenie základných princípov kvantovej mechaniky je kľúčové pre pochopenie toho, ako kvantové počítače fungujú a aké sú ich možnosti a obmedzenia.

# 3. Qubyty a kvantové hradlá

Qubity sú základné jednotky kvantových počítačov, ktoré môžu byť v superpozícii alebo prepletené. Kvantové hradlá sú kvantové verzie klasických logických hradiel, ktoré umožňujú manipulovať s qubitmi a vykonávať výpočtové operácie.

# 4. Kvantové algoritmy

Existuje niekoľko kvantových algoritmov, ktoré umožňujú riešiť určité problémy rýchlejšie, ako je možné pomocou klasických algoritmov. Medzi najznámejšie kvantové algoritmy patria Shorov algoritmus na faktorizáciu veľkých čísel a Groverov algoritmus na vyhľadávanie v nezoradených databázach.

# 5. Aplikácie kvantových počítačov

Kvantové počítače majú potenciál revolučne ovplyvniť rôzne odvetvia, vrátane kryptografie, farmaceutického výskumu, umelého učenia a optimalizácie. Ich výkonnosť by mohla viesť k vytváraniu nových liekov, optimalizácii logistických procesov a vytváraniu nových kryptografických štandardov.

# 6. Bezpečnosť a kvantové počítače

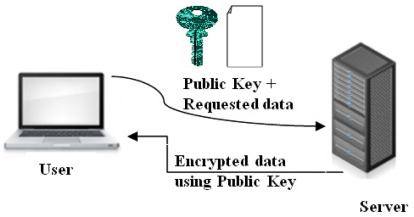
Kvantové počítače, svojou povahou a schopnosťami, zasahujú do oblasti kryptografie a zabezpečenia informácií. Zatiaľ čo môžu priniesť inovácie v mnohých smeroch, môžu aj ohroziť existujúce kryptografické systémy, ktoré sú založené na problémoch, ktoré sú pre klasické počítače ťažké na vyriešenie. Tu je pohľad na niektoré dôležité aspekty bezpečnosti a kvantových počítačov:

## Faktorizácia veľkých čísel

Jedným z najznámejších algoritmov v oblasti bezpečnosti týkajúcej sa kvantových počítačov je Shorov algoritmus, ktorý má schopnosť faktorizovať veľmi veľké čísla v čase, ktorý je exponenciálne menší ako je tomu v prípade klasických algoritmov. Faktorizácia veľkých čísel je základom mnohých kryptografických protokolov, ako napríklad RSA (Rivest-Shamir-Adleman) a ECC (Elliptic Curve Cryptography). Ak by kvantové počítače dokázali efektívne faktorizovať veľké čísla, tak by mohli ohroziť bezpečnosť týchto systémov.

## Bezpečnostné protokoly

V súčasnosti prebieha veľa výskumu v oblasti kvantových bezpečnostných protokolov. Jedným z príkladov je kvantová distribúcia kľúčov (QKD), ktorá využíva kvantové princípy na vytvorenie nevyhnutného kľúča pre kryptografické účely. Tieto protokoly sú navrhnuté tak, aby boli odolné voči útokom založeným na kvantových algoritmoch.



Obrázok 4 - RSA Šifrovanie

## Post-quantum kryptografia

Vzhľadom na potenciálnu hrozbu, ktorú kvantové počítače predstavujú pre existujúce kryptografické systémy, sa vyvíja koncept post-kvantovej kryptografie. Tieto systémy sú navrhnuté tak, aby boli odolné voči útokom zo strany kvantových počítačov, a teda by mali zostať bezpečné aj v prípade, že by sa takéto počítače stali realitou.

## Overovanie a šifrovanie

V oblasti bezpečnosti je kritické, aby sme si boli istí bezpečnosťou overovacích procesov a šifrovaných komunikácií. Kvôli možnému vplyvu kvantových počítačov na tieto procesy je dôležité vyvíjať a implementovať nové technológie a protokoly, ktoré sú odolné voči takýmto hrozbám.

## Etické aspekty

Okrem technických otázok je dôležité zvážiť aj etické a spoločenské dôsledky kvantových počítačov v oblasti bezpečnosti. Rýchly rozvoj kvantových technológií si vyžaduje zodpovedný prístup k vývoju a nasadeniu, aby sme zabezpečili, že tieto technológie budú používané v prospech ľudstva a budú slúžiť k zlepšeniu našej bezpečnosti a súkromia.

Kvantové počítače prinášajú nové výzvy a príležitosti v oblasti bezpečnosti. Je dôležité monitorovať ich vývoj a prijať opatrenia na zabezpečenie, že naše kryptografické systémy zostanú odolné voči budúcim hrozbám a útokom.

Schor's Algorythm

V tejto oblasti su kvantové počítače veľkým prelomom. Pretože dokážu vynásobiť číslo v polynomiálnom čase, zatiaľ čo klasické počítače potrebujú exponenciálny čas.

Grover's algorithm

V tejto oblasti sa síce podľa grafu môže zdať, že sú kvantové počítače obrovským prelomom, ale v skutočnosti iba zmenšujú obrovské číslo na polovicu.

256 bitové šifrovanie je väčsinou založené na algoritmoch **symetrických kľúčov**, ako sú AES alebo SHA-256.

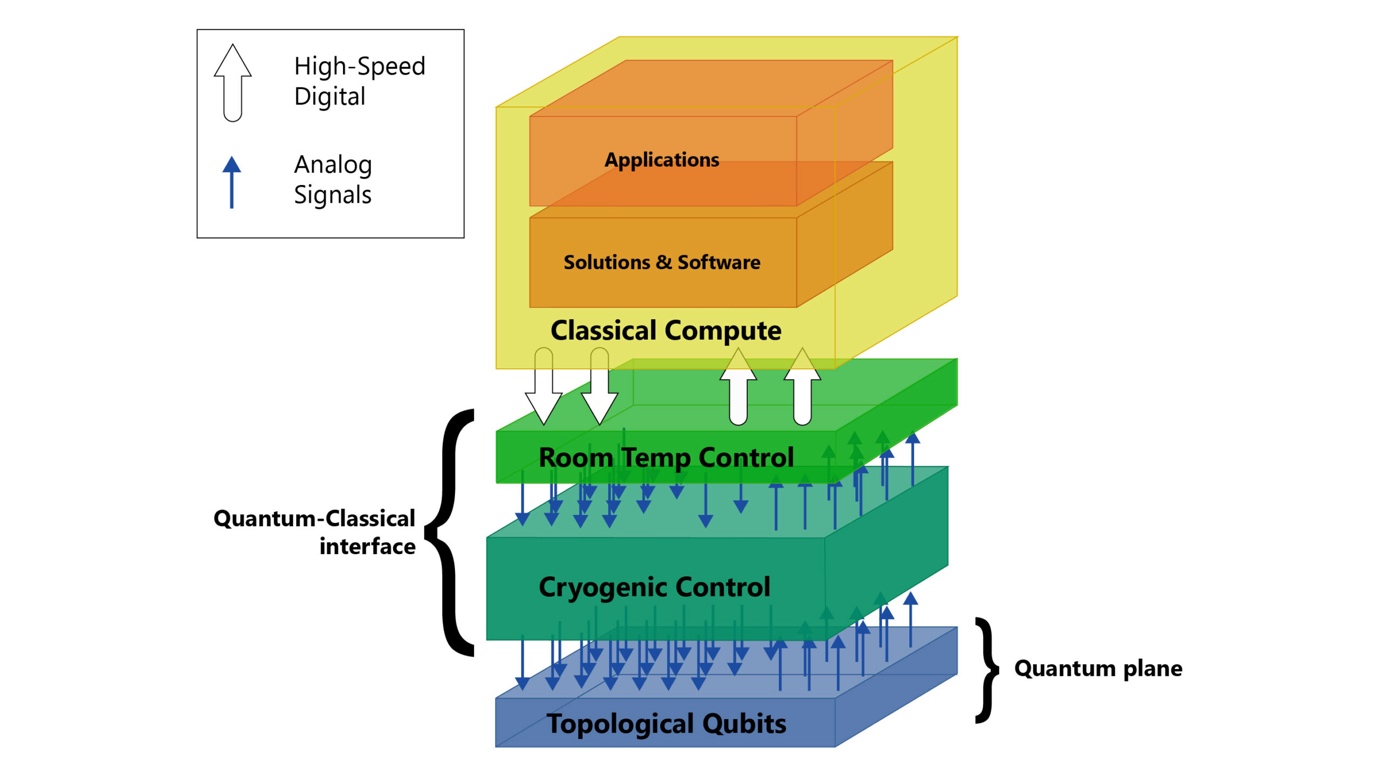
Tieto algoritmy používajú rovnaký kľúč na šifrovanie a dešifrovanie a nespoliehajú sa na faktorizáciu veľkých čísel. Používajú iné techniky, ako je substitúcia, permutácia, hashovanie atď. Kvantové počítače nemôžu použiť **Shorov algoritmus** na prelomenie týchto algoritmov.

Musia použiť iný algoritmus nazývaný **Groverov algoritmus**. Ten vyhľadať kľúč vo veľkom priestore v odmocnine času, zatiaľ čo klasické počítače potrebujú lineárny čas.

To znamená, že kvantový počítač dokáže prelomiť 256-bitové šifrovanie rýchlejšie ako klasický počítač, ale nie o veľa. Ak klasický počítač potrebuje 2^256 operácií na dešifrovanie 256-bitového kľúča, kvantový počítač by potreboval **2^128 operácií**.

# 7. Architektúry kvantových počítačov

Existujú rôzne prístupy k vytváraniu kvantových počítačov, vrátane kryogénnych superpočítačov, optických počítačov a iontových pascí. Každá architektúra má svoje výhody a nevýhody a je predmetom aktívneho výskumu.



Obrázok 5 - Architektúra kvantového počítača

# 8. Kvantová suprampočítačovosť

Kvantová suprampočítačovosť je fenomén, pri ktorom kvantové počítače dosahujú výkon nad rámec možností klasických počítačov. Tento koncept je stále predmetom výskumu a jeho realizácia by mohla mať široké dôsledky pre počítačovú vedeckú oblasť.

# 9. Perspektívy a výzvy

Aj keď kvantové počítače majú veľký potenciál, existujú aj výzvy, ktoré je potrebné prekonať, ako sú technické obmedzenia, chyby v kvantovom hardvéri a náročné algoritmy na korekciu chýb.

# 10. Záverečné myšlienky

Kvantové počítače predstavujú fascinujúci nový smer vo výpočtovej vede. Ich rozvoj a úspech sú kľúčové pre riešenie komplexných problémov, ktoré sú pre klasické počítače nepraktické.

# 11. Zdroje

Pre ďalšie informácie o kvantových počítačoch odporúčame nasledujúce zdroje:

* Quantum Computing Report (quantumcomputingreport.com)