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)

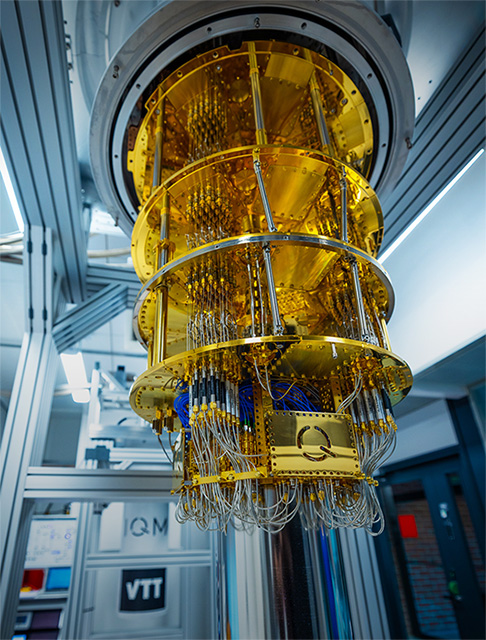
[9. Perspektívy a výzvy 6](#_Toc158566562)

[10. Záverečné myšlienky 6](#_Toc158566563)

[11. Zdroje 6](#_Toc158566564)

# 1. Úvod do kvantových počítačov

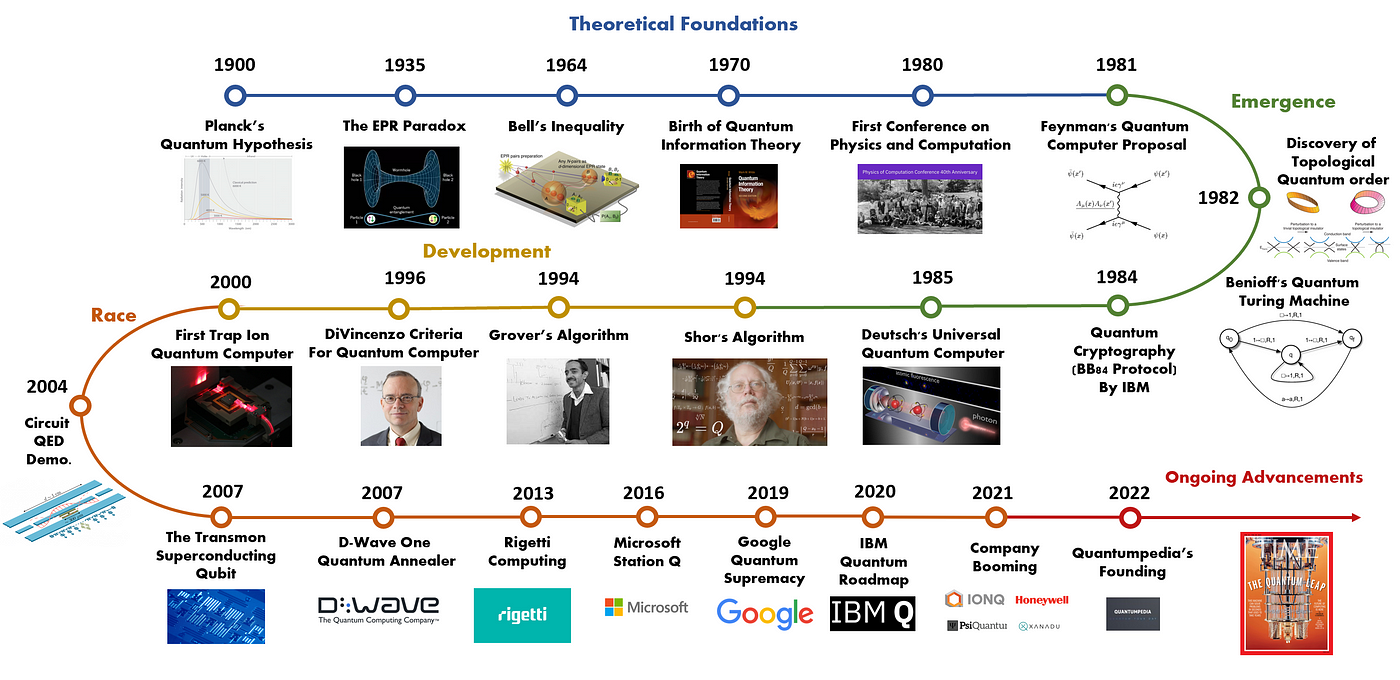
Kvantové počítače predstavujú revolučný pokrok vo svete výpočtovej technológie. Ich schopnosť vykonávať výpočty na úrovni, ktorá je neuskutočniteľná pre klasické počítače, otvára dvere k novým možnostiam v mnohých oblastiach, vrátane vedy, priemyslu a vojenských aplikácií.



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

# 2. Základy kvantovej mechaniky a ich aplikácia v kvantových počítačoch

Kvantové počítače, inšpirované princípmi kvantovej mechaniky, predstavujú revolúciu vo svete výpočtovej technológie. Ich jadro tvoria koncepty ako superpozícia, prepletenosť a zrážková pravdepodobnosť, ktoré nám otvárajú dvere k novým výpočtovým možnostiam. Kvantová mechanika je teória, ktorá sa zaoberá správaním veľmi malých častíc na mikroskopickej úrovni. Na rozdiel od klasických počítačov, kvantové počítače využívajú qubity namiesto bitov, ktoré môžu byť v superpozícii rôznych stavov a vzájomne prepletené. Tieto koncepty poskytujú kvantovým počítačom výnimočnú výpočtovú silu.

**Superpozícia - Rôzne možnosti stavu**

Superpozícia umožňuje qubitom existovať v kombinácii rôznych stavov s rôznymi pravdepodobnosťami, čo umožňuje paralelné vykonávanie viacerých operácií súčasne. Na rozdiel od klasických bitov, ktoré môžu byť buď 0 alebo 1, qubity môžu byť v superpozícii týchto stavov, čo poskytuje kvantovým počítačom neuveriteľnú výpočtovú flexibilitu.

**Prepletenosť - Vzájomné prepojenie**

Prepletenosť je jav, ktorý umožňuje kvantovým časticám byť vzájomne spojené tak, že ich vlastnosti nie je možné nezávisle popísať. Tento fenomén poskytuje kvantovým počítačom neuveriteľnú paralelnú výpočtovú silu a umožňuje im vykonávať komplexné operácie s vysokou efektivitou.

**Zrážková pravdepodobnosť - Pravdepodobnostné vyhodnocovanie**

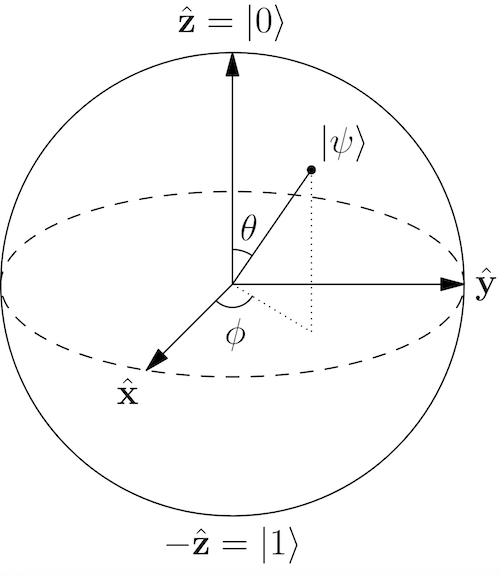
Zrážková pravdepodobnosť je kvantový jav, ktorý popisuje pravdepodobnosť, že kvantové častice sa budú správať ako vlny a prechádzať cez prekážky. Tento jav je základom experimentov, ktoré demonštrujú kvantovú povahu častíc a ich schopnosť vykazovať interferenčné vzory. ‎

**Heisenbergov princíp neurčitosti - Neurčitosť v meraniach**

Heisenbergov princíp neurčitosti hovorí, že nie je možné presne určiť súčasne polohu a hybnosť kvantovej častice. Tento princíp má dôležité dôsledky pre meranie a pozorovanie kvantových systémov, a zároveň ovplyvňuje spôsob, ako sú merané a manipulované kvantové počítače. ‎

**Aplikácia v kvantových počítačoch**

Základy kvantovej mechaniky tvoria kľúčový základ kvantových počítačov a umožňujú im vykonávať neuveriteľné výpočty a úlohy. Porozumenie týchto princípov nám pomáha lepšie chápať, ako kvantové počítače fungujú a ako môžu byť využité na riešenie komplexných problémov v rôznych odvetviach vedy a technológie.



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.

# 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aplikácia** | **Kvalita predpovede potrebného počtu qubitov** | **Príklad využitia** | **Potrebných qubitov** | **Gate Error Assumed** |
| Prelomenie kryptografie | Dobrá | Prelomenia RSA-2048 | ~ 20 miliónov | ~ 0.1% |
| Chémia | Stredná | Simulácia FeMoco | ~ 4 milióny | ~ 0.1% |
| Optimalizácia / AI | Zlá | ? | ? | ? |

# 6. Bezpečnosť a kvantové počítače

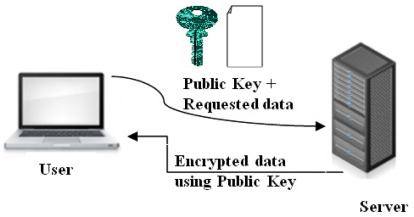
Kvantové počítače, svojou povahou a schopnosťami, zasahujú do oblasti kryptografie a zabezpečenia informácií. Zatiaľ čo môžu priniesť inovácie v mnohých smeroch, môžu aj ohroziť existujúce kryptografické systémy, ktoré sú založené na problémoch, ktoré sú pre klasické počítače ťažké na vyriešenie. Tu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

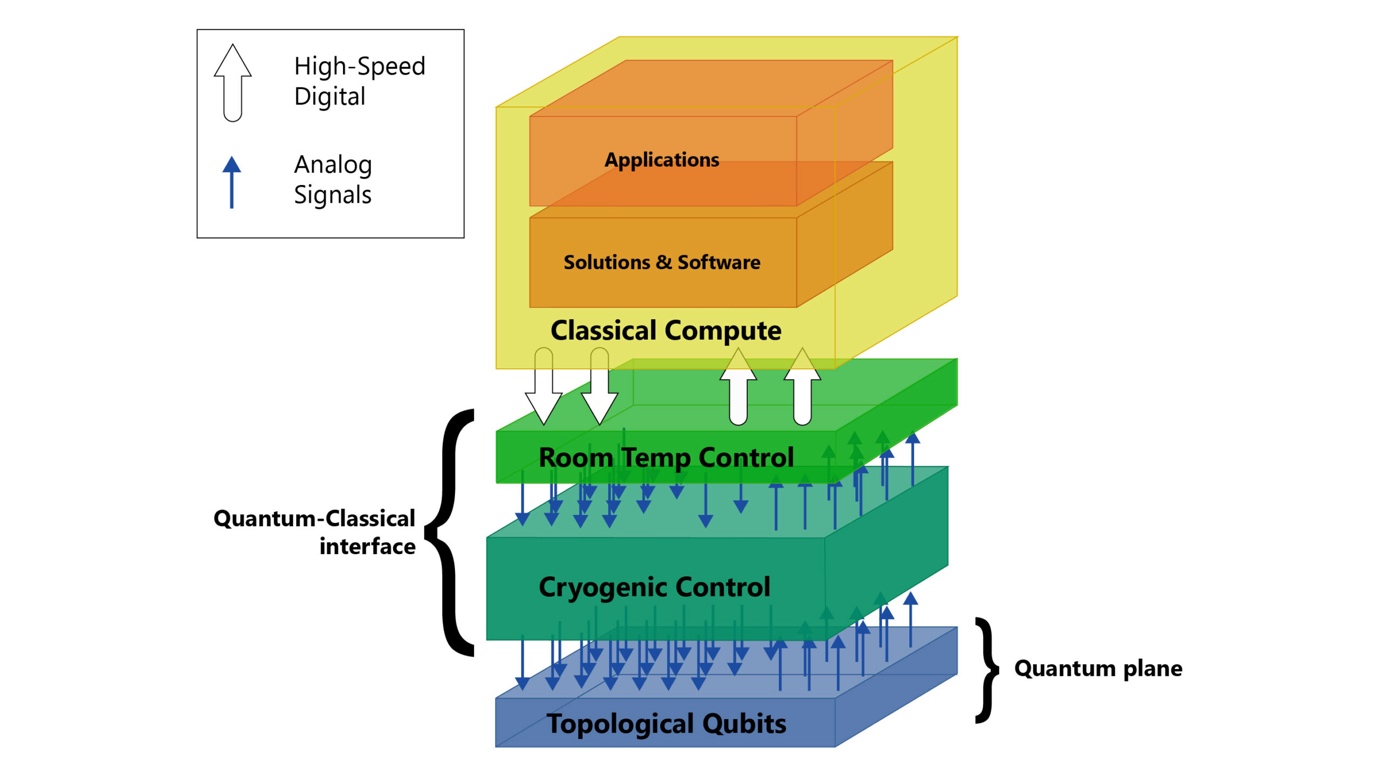
Tieto algoritmy používajú rovnaký kľúč na šifrovanie a dešifrovanie a nespoliehajú sa na faktorizáciu veľkých čísel. Používajú iné techniky, ako je substitúcia, permutácia, hashovanie atď. Kvantové počítače nemôžu použiť **Shorov algoritmus** na prelomenie týchto algoritmov.

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

Pohľad do budúcnosti je fascinujúci, no zároveň aj plný výziev a otázok, ktoré nám prináša éra kvantových počítačov. S ich príchodom sa otvárajú dvere do novej dimenzie technológie, ktorá môže transformovať náš svet a spôsob, akým chápeme výpočtovú silu.

Kvantové počítače nás nútia premýšľať o budúcnosti s nádejou, no zároveň aj s určitou mierou opatrnosti. Ich možnosti sú nepochybne ohromujúce - sľubujú rýchlejšie výpočty, zlepšené metódy kryptografie a nové inovácie, ktoré môžu zmeniť naše životy. Môžu nám pomôcť objavovať nové lieky, optimalizovať procesy výroby a riešiť zložité problémy, ktoré dnes predstavujú neprístupnú prekážku.

Avšak s týmito novými možnosťami prichádzajú aj nové výzvy a riziká. Kvantové počítače by mohli ohroziť bezpečnosť dnešných kryptografických systémov, a tak nás nútia hľadať nové spôsoby ochrany našich údajov. Okrem toho si vyžadujú značné úsilie a investície do výskumu a vývoja, aby sme ich mohli účinne využiť a integrovať do našej spoločnosti. Preto je naliehavé, aby sme sa už teraz začali pripravovať na príchod kvantových počítačov. Potrebujeme investovať nielen do technologických inovácií, ale aj do vzdelávania a osvety, aby sme zabezpečili, že budeme pripravení na výzvy, ktoré nám táto nová éra prinesie. Musíme budovať odolné kryptografické systémy, rozvíjať nové algoritmy a aplikácie a zároveň sledovať etické a sociálne dôsledky týchto technologických zmien.

Sme na prahu doby, ktorá nám prinesie nové príležitosti, ale aj nové záväzky. Ako spoločnosť máme moc ovplyvniť, akým spôsobom sa tieto nové technológie budú používať. S primeraným úsilím, inováciou a spoluprácou môžeme zabezpečiť, že éra kvantových počítačov bude pre nás všetkých prínosom, ktorý povedie k ďalšiemu kroku v našej technologickej a ľudskej evolúcii.

# 11. Zdroje

Pre ďalšie informácie o kvantových počítačoch odporúčame nasledujúce zdroje:

1. Quantum Computing Report. [online] [cit. 2024-04-12] Dostupné na: [https://quantumcomputingreport.com](https://quantumcomputingreport.com/)
2. PATHEON SPACE ACADEMY - Quantum Computing Explained for Beginners: The Science, Technology, and Impact, ISBN-13 979-8892387200
3. Dr. MICHELE MOSCA - "A quantum threat timeline report 2023". [online] [cit. 2024-04-24] Dostupné na: <https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2023.pdf>
4. NOUREDINE ZETTILI – Quantum Mechanics: Concepts and Applications, ISBN-10 0470026790, ISBN-13 978-0470026793
5. ZBIGNIEW FICEK - Quantum Physics for Beginners, ISBN-10 9814669385, ISBN-13 978-9814669382

## Ďaľšie zdroje použité pri tvorbe učebného materiálu:

1. A Brief History of Quantum Computing. [online] [cit. 2024-04-12] Dostupné na: <https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0>
2. The promise of quantum money. [online] [cit. 2024-04-17] Dostupné na:  
   <https://www.hpcwire.com/2014/01/07/promise-quantum-money/>
3. "IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation". [online] [cit. 2016-05-04] Pôvodne dostupné na: <https://www-03.ibm.com/press/us/en/pressrelease/49661.wss> Dostupné na <https://web.archive.org/web/20160505160937/https://www-03.ibm.com/press/us/en/pressrelease/49661.wss>
4. "IBM Quantum Experience Update". [online] [cit. 2017-04-06] Pôvodne dostupné na: <https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c> Dostupné na: <https://web.archive.org/web/20190129182024/https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c>
5. "Quantum computing gets an API and SDK". [online] [cit. 2017-03-06] Dostupné na: <https://developer.ibm.com/dwblog/2017/quantum-computing-api-sdk-david-lubensky/>
6. "What Is Quantum Computing?". [online] [cit. 2024-04-24] Dostupné na: <https://blogs.nvidia.com/blog/what-is-quantum-computing>
7. "The professional’s guide to Quantum Technology". [online] [cit. 2024-04-24] Dostupné na: <https://www.quantum.amsterdam/part-5-when-can-we-expect-a-useful-quantum-computer-a-closer-look-at-timelines>