# Kvantové technologie a komunikace

Připraveno pro Ministerstvo průmyslu a obchodu

**[červen 2025]**

# Obsah


**Seznam zkratek a vysvětlivek** ..... **4**

**Manažerské shrnutí** ..... **7**

**Management summary** ..... **9**

**1 Základy kvantových technologií** ..... **11**

1.1 Úvod ..... 11

1.2 Základní pojmy kvantové teorie ..... 11

1.3 Kvantová senzorika ..... 13

1.4 Kvantové počítače ..... 13

*1.4.1 K čemu jsou (resp. budou) kvantové počítače* ..... *13*

*1.4.2 Princip kvantového počítače* ..... *14*

*1.4.3 Kvantová oprava chyb* ..... *15*

*1.4.4 Základní stavební prvky kvantových počítačů* ..... *16*

*1.4.5 Druhy fyzických qubitů* ..... *16*

*1.4.6 Fungování kvantových počítačů* ..... *17*

*1.4.7 Výroba kvantových komponentů* ..... *18*

*1.4.8 Stav vývoje kvantových technologií a komunikace* ..... *20*

*1.4.9 Vybrané kvantové algoritmy* ..... *23*

1.5 Kvantová komunikace ..... 26

*1.5.1 Kvantová distribuce klíčů (QKD)* ..... *26*

*1.5.2 Stav vývoje kvantové komunikace* ..... *29*

**2 Architektura 5G a její kryptografická ochrana** ..... **30**

2.1 Bezpečnostní architektura 5G ..... 30

*2.1.1 Autentizační protokoly* ..... *30*

*2.1.2 Šifrování a ochrana dat* ..... *30*

2.2 Rizikové body napadení ..... 31

**3 Kryptografie** ..... **32**

3.1 Úvod do kryptografie ..... 32

3.2 Postkvantová kryptografie (PQC) ..... 33

*3.2.1 Výhody PQC* ..... *34*

*3.2.2 Nevýhody PQC* ..... *34*

3.3 Využitelnost kvantové distribuce klíčů (QKD) ..... 34

*3.3.1 Výhody QKD* ..... *35*

*3.3.2 Nevýhody QKD* ..... *35*

**4 Historie vývoje** ..... **36**

**5 Hrozby kvantového computingu pro 5G ..... 37**
5.1 Prolomení asymetrické kryptografie ..... 37
5.2 Dopady na symetrickou kryptografii ..... 37
5.3 Quantum decryption ..... 38
*5.3.1 "Harvest now, decrypt later" (HNDL) ..... 38*
*5.3.2 Quantum-Impersonation Attack ..... 38*
*5.3.3 Quantum Man-in-the-Middle (QMITM) ..... 39*
*5.3.4 Side-Channel Attacks ..... 39*
*5.3.5 Efficient Key Recovery Attacks ..... 39*
5.4 Posílení odolnosti kryptografie vůči kvantovým útokům ..... 40

**6 Regulace a standardizace ..... 41**
6.1 Mezinárodní iniciativy ..... 41
*6.1.1 NIST (Národní institut pro standardy a technologie USA) ..... 41*
*6.1.2 ETSI (Evropský institut pro telekomunikační normy) ..... 41*
*6.1.3 ITU-T (Mezinárodní telekomunikační unie, sektor standardizace) ..... 41*
*6.1.4 GSMA ..... 41*

**7 Kvantové aktivity EU a ČR ..... 43**
7.1 Kvantové výpočetní technologie EU a jejich náklady ..... 43
7.2 Kvantové aktivity ČR ..... 44

**8 Závěr ..... 47**

# Seznam zkratek a vysvětlivek

| Zkratka | Vysvětlivka |
|---|---|
| 3GPP | Partnerský projekt třetí generace, anglicky The 3rd Generation Partnership Project |
| 4G/5G | Čtvrtá/pátá generace mobilních sítí |
| AES | Standard pokročilého šifrování, anglicky Advanced Encryption Standard |
| AI | Umělá inteligence, anglicky Artificial Inteligence |
| AKA | Primární autentizace a dohody o klíči |
| AMF | Funkce pro řízení přístupu a mobility, anglicky Access and Mobility Management Function |
| APDs | Lavinový fotodiodový detektor, anglicky Avalanche photodiode |
| AQT | Alpine Quantum Technologies |
| ATIS | Standardizační organizace, Alliance for Telecommunications Industry Solutions |
| AV ČR | Akademie věd České republiky |
| BSC-CNS | Španělské supercomputingové centrum, Barcelona Supercomputing Center-Centro Nacional de Supercomputación |
| CMOS | Komplementární metal-oxid-polovodič, anglicky Complementary Metal-Oxide-Semiconductor |
| CRQC | Kvantový počítač schopný prolomit současné šifry, anglicky Cryptographically Relevant Quantum Computer |
| CSP | Poskytovatelé komunikačních služeb, anglicky Communications Service Provider |
| CZQCI | Projekt na dodání páteřní sítě fyzické infrastruktury EuroQCI v ČR, anglicky Czech National Quantum Communication Infrastructure |
| ČR | Česká republika |
| ČVUT | České vysoké učení technické |
| DoS | Typ útoku na internetové služby, anglicky Denial-of-service |
| DSA | Algoritmus digitálního podpisu, anglicky Digital Signature Algorithm |
| DTLS | Protokol poskytující zabezpečení pro nestavové datagramové protokoly, anglicky Datagram Transport Layer Security |
| EAP | Autentizační rámec používany nejčastěji v bezdrátových sítích a point-to-point systémech, anglicky Extensible Authentication Protocol |
| ECC | Kryptografický algoritmus založený na šifrování eliptickou křivkou, anglicky Elliptic Curve Cryptography |
| ECDH | Diffieho–Hellmanův protokol s využitím eliptických křivek, anglicky Elliptic-curve Diffie–Hellman |
| ECDSA | Algoritmus asymetrické kryptografie pro elektronický podpis, anglicky Elliptic Curve Digital Signature Algorithm |
| ECIES | Hybridní šifrovací schéma postavené nad eliptickými křivkami, anglicky Elliptic Curve Integrated Encryption Scheme |
| EPS | Paketový systém používaný v sítích LTE, anglicky Evolved Packet Systém |
| ETSI | Evropský ústav pro telekomunikační normy, anglicky European Telecommunications Standards Institute |
| EU | Evropská unie |
| EUR | Euro |
| EuroQCI | Iniciativa Evropské kvantové komunikační infrastruktury, anglicky Quantum communication infrastructure |

| | |
|---|---|
| FT | Systém odolný proti chybám, anglicky fault-tolerant systém |
| gNB | Základnové stanice, anglicky gNodeB |
| GPU | Grafický procesor, anglicky Graphics Processing Unit |
| GSMA | Sdružení nezávislých operátorů, anglicky The Global System for Mobile Association |
| HHL | Kvantový algoritmus, Harrow-Hassidim-Lloyd algoritmus |
| HNDL | Typ kvantového útoku, anglicky Harvest Now Decrypt Later |
| HPC | Vysoce výkonné počítání, anglicky High-performance computing |
| HQC | Hybridní kódové šifrování, anglicky Hamming Quasi-Cyclic |
| HW | Hardware |
| IMSI catcher | Zařízení na odposlouchávání telefonických rozhovorů |
| IoT | Interent věcí, anglicky Internet of Things |
| IPsec | Šifrovací algoritmus chránící přenos dat mezi zařízeními šifrováním jednotlivých IP paketů a současným ověřováním zdroje těchto dat |
| ISG | Pracovní skupina pro specifikaci v rámci průmyslu organizace ETSI, anglicky Industry Specifiation Group |
| IT | Informační technologie |
| ITU-T | International Telecommunication Union Telecommunication Standardization Sector, anglicky Mezinárodní telekomunikační unie, sektor standardizace |
| KEM | Mechanismus pro zapouzdření klíče, anglicky Key encapsulation mechanism |
| LAN | Lokální síť, anglicky Local Area Network |
| LIGO | Gravitační senzor, anglicky Laser Interferometer Gravitational-Wave Observatory |
| LRZ | Německé supercomputingové centrum, německy Leibniz-Rechenzentrum |
| MAX-CUT | Úloha maximální řezu |
| mK | miliKelvin, velmi nízké teploty |
| MUNI | Masarykova univerzita |
| NCSC | Britské Národní centurm kybernetické bezpečnosti, anglicky National Cyber Security Centre |
| NFV | Virtualizace síťových funkcí, anglicky Network function virtualization |
| NISQ | Současná generace kvantových počítačů, anglicky Noisy Intermediate-Scale Quantum |
| NIST | Americký Národní institut standardů a technologie, anglicky National Institute of Standards and Technology |
| NSA | Kryptologická organizace USA, anglicky The National Security Agency |
| PKI | Infrastruktura veřejného klíče, anglicky Public Key Infrastructure |
| PQC | Postkvantová kryptografie, anglicky Post-quantum cryptography |
| QAOA | Kvantový algoritmus navržený pro řešení kombinatorických optimalizačních úloh, anglicky Quantum Approximate Optimization Algorithm |
| QC | Quantum computing |
| Qiskit SDK | Open-source sada pro vývoj softwaru pro kvantové počítače |
| QKD | Kvantová distribuce klíčů, anglicky Quantum Key Distribution |
| QMITM | Typ kvantového útoku, anglicky Quantum Man-in-the-Middle |
| QRNG | Kvantové generátory náhodných čísel, anglicky Quasirandom Number Generator |
| QSC | Kvantově odolná kryptografie, anglicky Quantum-Safe Cryptography |
| RSA | Šifra s veřejným klíčem založená na faktorizaci, Rivest-Shamir-Adleman |
| SDN | Softwarově definované sítě, anglicky Software Defined Networking |
| SIDH | Postkvantový kryptografický algoritmus, anglicky Singular Isogeny Diffie-Hellman |
| SNSPDs | Supravodivý jednofotonový detektor, anglicky superconducting nanowire single-photon detector |

| | |
|---|---|
| SUCI | Identifikátor pro ochranu uživatele, Subscription Concealed Identifier |
| SUPI | Identifikátor pro ochranu uživatele, Subscription Permanent Identifier |
| TLS | Protokol využívající šifrování veřejného klíče, ověřování pravosti informace a odhalování neodovolených manipulací s daty, anglicky Transport Layer Security |
| UE | Uživatelské zařízení, anglicky User equipment |
| UK | Univerzita Karlova |
| UPF | Síťová komponenta v 5G jádru, která zajišťuje směrování, přenos a zpracování uživatelských dat odděleně od řídící roviny, anglicky User Plane Function |
| USD | Americký dolar |
| USTC | Čínska univerzita vědy a techniky, anglicky University of Science and Technology of China |
| VQE | Hybridní algoritmus, který využívá jak klasické počítače, tak kvantové počítače k nalezení základního stavu daného fyzického systému, anglicky Variational Quantum Eigensolver |
| VŠB | Vysoká škola báňská - Technická univerzita Ostrava |
| VTT | Finské Technické výzkumné středsiko, finsky Valtion teknillinen tutkimuskeskus |
| VUT | Vysoké učení technické v Brně |
| Wi-Fi | Skupina bezdrátových síťových protokolů založených na standardech IEEE 802.11, anglicky Wireless Fidelity |
| ZUC | Streamovací šifrovací algoritmus používaný v mobilních sítích pro zabezpečení datového provozu |

# Manažerské shrnutí

**Quantum computing** (QC) je jednou z aplikací kvantové mechaniky, rozsáhlé vědecké disciplíny opřené o kvantovou teorii. Kvantová teorie poskytuje základní rámec pro pochopení chování hmoty a energie na mikroskopické úrovni a umožnila vznik celé řady nových technologií. Dnešní „druhá kvantová revoluce“ znamená, že umíme nejen pozorovat, ale i cíleně manipulovat s jednotlivými částicemi, což vede k rozvoji tří hlavních aplikačních oblastí: kvantová senzorika, kvantová komunikace, a právě kvantové počítače.

**Kvantová mechanika** pracuje s fyzikálními jevy na subatomární úrovni, které jsou zásadně odlišné od běžných fyzikálních zákonů makrosvěta. Jedná se především o superpozici stavů, kvantové provázání, pravděpodobnostní povahu měření a nemožnost kopírování kvantové informace. Tyto principy, které nejsou v klasickém světě možné, lze využít v kvantových aplikacích. V rámci informatiky, představují nový výpočetní model s potenciálem zásadně urychlit řešení určitých typů úloh (např. faktorizace, optimalizace, simulace materiálů).

**Kvantové počítače** a jejich vývoj jsou limitovány fyzikálními vlastnostmi kvantových systémů – chybovostí, dekoherencí a technologickými nároky na provoz (např. kryogenní chlazení). Základní stavební jednotkou kvantových systémů je qubit (obdoba klasického bitu), který může být realizován různými fyzikálními systémy (supravodivé obvody, iontové pasti, fotonické systémy aj.). Pro dosažení prakticky využitelných kvantových počítačů je klíčová implementace kvantové opravy chyb a škálování na stovky až tisíce logických qubitů. Největší světoví hráči (IBM, Google, Quantinuum, čínské a evropské týmy) dosahují v roce 2025 řádově stovek qubitů a postupně zvyšují kvalitu i výkon zařízení. Jde však zatím o malý počet velmi nákladných zařízení (zmíněné subjekty investují řádově stovky milionů USD ročně) a všechna jsou v hluboce experimentální fázi. Existuje celá řada různých technologických přístupů QC, které se liší dle vhodnosti pro specifické výpočetní úkoly. Je nutný další vývoj, experimentování, porovnání životaschopnosti jednotlivých různorodých metod, nalezení efektivních přístupů a následná standardizace.

Nasazení kvantových počítačů umožní řešit složité vědecké problémy a praktické simulace (navrhování materiálů se specifickými vlastnostmi, baterií, chemických sloučenin, léků, v logistice, při učení neuronových sítí - AI, kryptografii) a současně přinese bezpečnostní riziko pro současné postupy šifrování. Zatím zjednodušeně platí, že výkony kvantových počítačů nepřevyšují standardní (legacy) systémy, avšak dokáží řešit specifické dílčí úlohy, které jsou pro standardní systémy nepřístupné – neřešitelné v představitelném čase. Tento typ kombinovaného použití standardních výpočetních systémů a QC (pro specifické podúlohy) se předpokládá i do budoucna. V současnosti je možné jen omezené komerční využití QC formou pronájmu strojového času a služeb řešitelského (vědeckého) týmu, který převede požadavky klienta do pokynů srozumitelných pro kvantová zařízení (unitární operace).

Mezi takové specifické úlohy přístupné pro QC patří šifrování a dešifrování, které je v dohledné době způsobilé prolomit současné kryptografické protokoly (zejména RSA, ECC), které jsou využívány v 5G sítích pro autentizaci a výměnu klíčů a narušit tak celkovou bezpečnost digitální komunikace. Groverův algoritmus ohrožuje i symetrické šifry, i když v menší míře. Zásadní je včasná migrace na postkvantovou kryptografii a případné využití QKD pro páteřní a kritickou infrastrukturu. Tento krok musí dostatečně předcházet vývoji samotného QC, neboť již dnes existují hrozby, které se projeví později – útočníci již nyní sbírají (odposlouchávají) a ukládají standardně zašifrovanou komunikaci s tím, že dekrypci provedou později, až k tomu získají příslušnou kvantovou technologii. Odhadovaná doba, kdy dojde k prolomení současných šifrovacích algoritmů kvantovým počítačem se odhaduje na 15 až 20 let, přičemž míra rizika se zhruba zdvojnásobuje každých 5 let.

**Postkvantová kryptografie** (PQC) reaguje na riziko představované kvantovými počítači pro současné šifrovací algoritmy. Zabývá se vývojem nových algoritmů odolných vůči útokům kvantových počítačů, aniž by přitom vyžadovala novou fyzickou infrastrukturu. NIST a ETSI tyto nové algoritmy testují a standardizují. Výhodou PQC je možnost softwarové implementace na stávajících systémech, nevýhodou jsou větší (delší) klíče, tím i větší nároky na výkon zařízení a zatím kratší historie prověření bezpečnosti.

**Kvantová komunikace**, další z aplikací kvantové mechaniky, využívá kvantových jevů (zejména provázání a nemožnosti měřit kvantový stav bez jeho ovlivnění) k bezpečnému vytvoření a distribuci šifrovacích klíčů (QKD). Tato technologie umožňuje detekovat jakýkoliv pokus o odposlech a je považována za dlouhodobě bezpečnou i vůči útokům kvantových počítačů. Hlavní limity QKD jsou v dosahu (zatím řádově desítky až stovky km bez opakovačů), nákladnosti a potřebě speciální infrastruktury. Probíhá však intenzivní výzkum integrace QKD do běžných telekomunikačních sítí a také v oblasti satelitní QKD jsou již zaznamenány první úspěchy testování technologií.

**Vývoj QC** je stále velmi složitý a nákladný proces. Investice do výzkumu QC tak vedle největších světových hráčů vynakládají samotné státy jednotlivě, nebo společně. Vývoj v EU reprezentují masivní investice do rozvoje kvantových technologií v rámci specifických programů /projektů (Quantum Flagship, EuroHPC Joint Undertaking, EuroQCI) a rozvoj QC je rovněž součástí cílů politiky Digitální Dekády. V ČR vzniká testovací národní kvantová infrastruktura (projekt CZQCI), rozvíjí se vzdělávací a výzkumné aktivity napříč univerzitami (MUNI /CS Hub) a AV ČR. Probíhá příprava národní kvantové strategie a rozvíjí se spolupráce v evropském rámci.

**Doporučené kroky** pro státní instituce a regulátory zahrnují potřebu:

- formulovat minimální (závazná) metodická pravidla pro operátory pro zajištění kybernetické bezpečnosti 5G a ostatních komunikačních sítí v souvislosti s nástupem quantum computingu,
- vytvořit referenční rejstřík PQC kompatibilních zařízení a
- stanovit minimální nároky na interoperabilitu mezi klasickou a QKD kryptografií.

# Management summary

**Quantum computing** (QC) is one of the applications of quantum mechanics, a broad scientific discipline rooted in quantum theory. Quantum theory provides the fundamental framework for understanding the behavior of matter and energy at the microscopic level and has enabled the development of numerous new technologies. Today's "second quantum revolution" signifies that we can not only observe but also deliberately manipulate individual particles, leading to advancements in three main application areas: quantum sensing, quantum communication, and quantum computing itself.

**Quantum mechanics** deals with physical phenomena at the subatomic level, which differ fundamentally from the classical laws of the macroscopic world. Key principles include superposition of states, quantum entanglement, the probabilistic nature of measurement, and the impossibility of copying quantum information. These principles, which are absent in the classical world, enable transformative applications in computing. In computer science, they introduce a new computational model with the potential to dramatically accelerate solutions to specific problems, such as factorization, optimization, and material simulations.

**Quantum computers** and their development are constrained by the physical properties of quantum systems - error rates, decoherence, and operational demands (e.g., cryogenic cooling). The basic building block of quantum systems is the qubit (analogous to the classical bit), which can be implemented through various physical systems such as superconducting circuits, ion traps, or photonic systems. Achieving practical quantum computers requires implementing quantum error correction and scaling to hundreds or thousands of logical qubits. Leading global players (IBM, Google, Quantinuum, Chinese, and European teams) are projected to reach hundreds of qubits by 2025, gradually improving device quality and performance. However, these remain expensive, experimental systems, with annual investments reaching hundreds of millions of USD. Diverse technological approaches to QC exist, each suited to specific computational tasks, necessitating further development, experimentation, viability comparisons, and eventual standardization.

Deploying quantum computers will enable solving complex scientific problems and practical simulations (e.g., designing advanced materials, batteries, chemical compounds, drugs, logistics optimization, AI training, and cryptography), while simultaneously posing security risks to current encryption methods. While quantum computers currently do not outperform classical (legacy) systems in general tasks, they excel at specific subtasks that are intractable for classical systems. A hybrid approach - combining classical and quantum systems for specialized subroutines - is expected to persist. Currently, limited commercial QC use exists via machine-time rentals and scientific team services for translating client requirements into quantum-readable instructions (unitary operations).

Key QC-accessible tasks include encryption and decryption, which could soon break current cryptographic protocols (e.g., RSA, ECC) used in 5G networks for authentication and key exchange, compromising digital communication security. Grover's algorithm also threatens symmetric ciphers, albeit less severely. Timely migration to post-quantum cryptography (PQC) and the adoption of quantum key distribution (QKD) for critical infrastructure are essential. This transition must precede QC advancements, as attackers are already harvesting (eavesdropping and storing) encrypted data for future decryption once quantum technology becomes available. The estimated timeframe for quantum computers breaking current encryption is 15 - 20 years, with risks doubling approximately every five years.

**Post-quantum cryptography** (PQC) addresses quantum computing threats by developing algorithms resistant to quantum attacks without requiring new physical infrastructure. NIST and ETSI are testing and standardizing these algorithms. While PQC allows software implementation on existing systems, drawbacks include larger keys, higher performance demands, and shorter security validation history.

**Quantum communication**, another application of quantum mechanics, leverages phenomena like entanglement and the no-cloning theorem to securely generate and distribute encryption keys (QKD). This technology detects eavesdropping attempts and remains secure against quantum attacks. Current QKD limitations include range (tens to hundreds of kilometers without repeaters), cost, and specialized infrastructure requirements. However, research into integrating QKD into standard telecom networks and satellite-based QKD is progressing.

**QC development** remains complex and costly. Beyond major global players, individual states and collaborative initiatives are investing heavily. In the EU, significant funding supports quantum technology through programs /projects like Quantum Flagship, EuroHPC Joint Undertaking, and EuroQCI, aligning with Digital Decade policy goals. In the Czech Republic, a national quantum test infrastructure (CZQCI project) is emerging, alongside educational and research activities at universities (e.g., MUNI/CS Hub) and the Academy of Sciences. A national quantum strategy is in preparation, alongside European collaboration efforts.

**The recommended steps** for state institutions and regulators include the need to:

- Formulate mandatory minimum methodological rules for operators to ensure cybersecurity of 5G and other communication networks in the context of quantum computing advancements,
- Create a reference register of PQC-compatible devices, and
- Establish minimum interoperability requirements between classical and QKD cryptography.

# 1 Základy kvantových technologií

## 1.1 Úvod

**Kvantová teorie** je obecný teoretický rámec, fyzikální teorie, která popisuje chování hmoty a energie na atomární a subatomární úrovni a zahrnuje oblasti jako jsou kvantová mechanika, kvantová elektrodynamika, kvantová pole, kvantová statistika. **Kvantová mechanika**, základní stavební kámen celé kvantové fyziky a kvantové teorie obecně, je vědní disciplína poskytující matematický aparát a přesné zákony pro popis a předpověď chování subatomárních částic (např. elektrony, fotony, kvarky). V tomto mikrosvětě platí přírodní zákony, které se zásadně liší od pravidel klasické fyziky a místo nich nastupují pravděpodobnostní jevy, dualita částic a vlnění, nebo jev okamžité korelace mezi částicemi bez ohledu na jejich vzdálenost.

Letitý výzkum v oblasti kvantových technologií, jehož výsledkem byl vznik aplikací, mezi něž se řadí např. lasery, magnetická rezonance, atomové hodiny, elektronová mikroskopie atd., dospěl do stádia, kdy dokážeme manipulovat s jednotlivými subatomárními částicemi s velikou přesností. Toto tempo pokroku pomohlo významně navýšit objem financí proudících do výzkumu a vývoje kvantových technologií, což v posledním desetiletí vedlo k vývoji dalších, zcela nových aplikací. Ty dnes můžeme rozdělit do tří hlavních oblastí:

- Kvantová senzorika
- Kvantové počítače a algoritmy
- Kvantová komunikace

## 1.2 Základní pojmy kvantové teorie

Kvantová teorie (přesněji kvantová mechanika) je rozsáhlou fyzikální teorii, která je vysoce neintuitivní. Je postavena na několika odpozorovaných základních pravidlech, ze kterých plynou veškeré důsledky vedoucí k aplikacím. Proto lze na kvantovou teorii nahlížet z dvou pohledů – první je pohled fyzikálně-filozofický, ve kterém se prozkoumávají teoretické (matematické) základy teorie, druhý pohled je praktický, čisté užití principů vedoucí k aplikacím. Druhý přístup je vhodný pro tuto studii – neslouží k pochopení samotné teorie, ale je spíše vodítkem, kdy akceptujeme některá základní pravidla (postuláty) a díváme se na jejich důsledky. Vysvětlení jevů, pokud leží v matematických základech teorie, nejsou pro svoji komplexnost předmětem této studie.

Z postulátů kvantové teorie jsou pro následující popis důležité zejména tyto principy:

1. Každý kvantový systém se nachází v nějakém **pravděpodobnostním stavu** matematicky vyjádřeném tzv. **vlnovou funkcí** nebo **stavovým vektorem** (znázorňuje se zápisem $|a\rangle$, $|b\rangle$ atd. znamenajícím vektor v Hilbertově (matematickém) prostoru), který je principiálně možné popsat, není ale možné tuto informaci z neznámého stavu získat. Kvantový stav lze rozložit do bázových stavů (dle měřených veličin, u elektronu např. poloha, energie, spin) a každý bázový stav má přiřazenou tzv. amplitudu pravděpodobnosti, která určuje, jak moc se na výsledku (celkovém stavu systému) podílí.
2. Manipulace se stavem probíhá za pomoci speciálních, teorií povolených operací, které nazýváme **unitární operace**. Unitární operace je vratná a zajišťuje že se ze systému „neztrácí pravděpodobnost“ – tedy aby součet všech možností byl pořád 100 %. Představíme-li si, že kvantový stav je jako šipka, která ukazuje určitým směrem v prostoru možností (vektor), pak unitární operace je speciální „pohyb“ nebo „otočení“ této šipky, který něco v systému změní, ale nic neztratí. Šipka se může otáčet, měnit směr, ale nikdy se nezkrátí, nezvětší ani nezmizí. Všechny možnosti zůstanou zachovány. Pokud uděláte unitární operaci a pak ji „pustíte pozpátku“, dostanete se přesně tam, kde jste začali. V kvantové fyzice je důležité, aby se při vývoji systému neztrácela pravděpodobnost a unitární operace toto zajišťuje. Samotné zadání unitární operace kvantovému systému probíhá formou fyzikálního působení na částice v systému (např. pomocí elektromagnetických polí, mikrovln, laserů nebo elektrických signálů, v závislosti na typu fyzického qubitu).
3. Jediná možnost získání klasické informace z kvantového systému je jeho **měření**. Při měření kvantového stavu zjišťujeme konkrétní hodnotu vybrané fyzikální veličiny v daném systému, například energie, spinu, hybnosti, pozice, polarizace nebo jiné vlastnosti částic. Tyto veličiny mohou v kvantovém světě nabývat pouze určitých (diskrétních) hodnot – jsou kvantovány, přičemž výsledek měření je vždy jen jeden z možných kvantovaných stavů a je dán pravděpodobnostmi podle původního

kvantového stavu. Jak již ale bylo řečeno, měření nám poskytuje jenom parciální informaci. Zároveň dochází k nenávratné změně systému, kdy je zbylá informace o kvantovém stavu ztracena.

Tyto principy vedou k mnoha známým i méně známým projevům kvantové teorie. Některými z nich jsou:

- **Superpozice**

Princip 1 má i specifický rigorózní matematický popis, který povoluje, že systém, který může být v stavu $|a\rangle$, nebo ve stavu $|b\rangle$ (0 nebo 1), může být také ve stavu $\alpha|a\rangle+\beta|b\rangle$, tedy ve stavu, který je složen z obou možností. Tomuto pravidlu se říká superpozice. Jeho příkladem je známá Schrödingerova kočka, která je „zároveň živá a zároveň mrtvá“. Tento popis za pomoci slova „zároveň“ je ale velice nepřesný a vede k rozšířenému, ale nevhodnému popisu kvantových výpočtů jakožto paralelizovaných. Superpozice se na první pohled může jevit jako paralelizace, ale kvůli důsledkům zbylých principů je tato interpretace velice neadekvátní.

- **Pravděpodobnostní (kvantové) měření**

Rozvádí a přesněji popisuje 3. kvantový princip. Kvantové měření je schopno nám poskytnout pouze informaci o systému, jež je vybrána ze sady výsledků náležících k měření. Každé měření je specifikováno kvantovými stavy, které je schopno rozlišit (např. $|a\rangle$, $|b\rangle$, $|c\rangle$, atd.), a které jsou nám sděleny klasicky jako $a$, $b$, nebo $c$. Systém, jenž se nachází v superpozici $\alpha|a\rangle+\beta|b\rangle$ stavů $|a\rangle$ a $|b\rangle$, při daném měření dává výsledky $a$ anebo $b$ jenom s jistou pravděpodobností, přesně definovanou parametry $\alpha$ a $\beta$. Po měření je celý systém redukován na stav $|a\rangle$ anebo $|b\rangle$ dle výsledku (destruktivita měření). Pro přesnější představu o parametrech $\alpha$ a $\beta$ je proto nutné celý experiment (proces od přípravy stavu až po jeho měření) vícekrát opakovat. I přesto není možné získat celou informaci o těchto parametrech.

- **Interference**

Jeden z důsledků principu 1, který by při „paralelní představě“ nebyl možný, je tzv. interference, kdy se některé výsledky měření při změně systému mohou posílit, přičemž jiné zeslábnou. Jde o jev, kdy se vlnové funkce kvantových částic mohou navzájem „skládat“ – podobně jako vlny na vodě, a to i u jediné částice v superpozici (kdy existuje ve více stavech najednou). Pokud existuje více stavů, je třeba sečíst všechny možné amplitudy pravděpodobnosti od každého z nich. Tyto amplitudy se mohou navzájem zesilovat nebo rušit – to je právě interference. Výsledkem tohoto skládání může být zesílení pravděpodobnosti výskytu částice v některých místech (konstruktivní interference) a naopak zeslabení nebo vynulování v jiných (destruktivní interference). Interference je základem pro mnohé algoritmy, kdy za pomoci přesně definovaných operací provádíme výpočet, ve kterém se ty pro nás užitečné výsledky posilují až do bodu, kdy nám z měření vycházejí s dostatečně vysokou pravděpodobností. Komplikovanost hledání kvantových algoritmů spočívá v kombinaci omezení daných principem 2 na unitární operace a destruktivitou měření.

- **Provázání (entanglement)**

Při vyšším počtu částí systému je možné dosáhnout silné korelace mezi jednotlivými částmi. Provázaný stav lze poznat podle toho, že měření na jedné částici okamžitě určuje stav druhé. V kvantové mechanice se často používá příklad se spinem dvou elektronů. Pokud jsou elektrony provázané, změříte-li spin (kvantovou vlastnost) jednoho a zjistíte například hodnotu „nahoru“, druhý bude mít vždy „dolů“ – a to i když jsou od sebe světelné roky daleko. Výsledek měření je náhodný, ale vždy dokonale korelovaný. (Představte si, že máte dvě hrací kostky, které jsou provázané. Hodíte jednu v Praze a druhou třeba v New Yorku. Pokud vám v Praze padne šestka, v New Yorku se v tu samou chvíli objeví také šestka – ať už jsou od sebe obě kostky jakkoliv daleko. Výsledek hodu je náhodný, ale jakmile zjistíte výsledek u jedné, okamžitě víte výsledek i u druhé.) K provázání dochází typicky při společném vzniku částic (například při rozpadu částice na dvě menší), nebo uměle, pokud spolu částice interagují tak, aby se dostaly do sdíleného kvantového stavu. Kvantové korelace jsou ale silnější než ty klasické (statistické). Síla kvantové korelace je měřitelná a vede k aplikacím, které v klasickém prostředí nejsou možné. Velké využití je kupříkladu ve kvantové komunikaci, kdy je jeden z protokolů pro zabezpečení klíče založen na vytvoření právě takto provázaných stavů. Většina částic v přírodě ale provázaná není – provázání je tedy vzácný a křehký stav, který se snadno ztrácí (tzv. dekoherence).

- **Projektivní měření a slabá měření**

Měření popsaná výše jsou tzv. projektivní (také zvané silné nebo von Neumannovo měření), kdy je změnění stavu po provedeném měření absolutní. To znamená, že výsledek měření je vždy pouze jeden z možných vlastních stavů měřeného operátoru a po měření se systém zhroutí (kolabuje) do tohoto jediného stavu (žádná superpozice – odpadá pravděpodobnost jiného stavu). Silné měření silně narušuje (dekoheruje) původní kvantový stav. Známe však také měření slabá, která stav systému nemusí degradovat úplně, ale jenom částečně. Slabé měření je takové, při kterém interakce mezi měřeným systémem a měřicím přístrojem je velmi slabá a výsledkem je, že získáme jen malou (nepřesnou) informaci o systému, ale zároveň systém téměř nenarušíme. Informace takto získaná je tedy slabší než u projektivního měření. Typicky je tento typ měření prováděn tak, že se měřený systém slabě prováže s pomocným systémem. Projektivní měření na pomocném systému pak dává menší

informaci o měřeném systému, který je měřením méně zasažen. Slabá měření jsou důležitá například při kvantové opravě chyb (u kvantových počítačů).

- **No-cloning**

Specifičnost operací, které jsou kvantovou teorii povoleny (princip 2), v součinnosti s destruktivitou měření, mají za důsledek nemožnost kopírování kvantového stavu. Jakákoliv snaha o kopírování kvantového stavu vede k jeho znehodnocení. Tento princip je známý právě jako no-cloning teorém.

- **Dekoherence**

Kvantové stavy jsou velice křehké, snadno interagují s okolím a jejich stav tak ztrácí informaci v něm uloženou. Můžeme si to představit jako by prostředí kontinuálně provádělo slabá měření na systému z kterého se informace tímto způsobem postupně vytrácí. Tento jev se také nazývá kvantový šum (quantum noise). Jelikož jakékoli propojení s okolím vede k dekoherenci, při navrhování kvantových zařízení musíme zaručit co nejlepší ochranu před okolím. Mnohé systémy jsou proto uloženy ve vakuu a při velmi nízkých teplotách (mK).

# 1.3 Kvantová senzorika

Kvantová senzorika přináší do různých oblastí zlepšení přesnosti měření, někdy i o několik řádů. Principy, které jsou k tomuto účelu použity jsou různé a liší se od aplikace k aplikaci. Například provázání se dá použít k dalšímu vylepšení atomových hodin, anebo k vytvoření citlivějších magnetometrů. Interference je užitá ve fotonických senzorech, mikroskopii, anebo v gravitačních senzorech (LIGO). Jiným příkladem může být vytvoření citlivějších přijímačů radiových vln, které jsou navíc energeticky úspornější[1]. Tento výčet není kompletní a jen ukazuje na rozmanitost dané problematiky.

# 1.4 Kvantové počítače

## 1.4.1 K čemu jsou (resp. budou) kvantové počítače

Kvantové počítače fungující na kvantových principech přinášejí do oblasti výpočetní techniky nové paradigma. Od jiného přístupu k výpočtům se očekává možnost urychlení některých specifických operací. I proto je jejich vývoji věnována značná pozornost. Je třeba mít na paměti, že nelze očekávat univerzální urychlení jakýchkoli výpočtů, využití lze nalézt ve velmi specifických oblastech matematických operací. Nacházení kvantových algoritmů, jenž můžou být užitečné, je složitý proces, který je ovlivněn specifickými omezeními kvantové teorie – destruktivita měření, specificita vývoje systému (limitace na unitární operace). Zajímavé pro kvantové výpočty jsou obzvláště oblasti, ve kterých je prohledáván exponenciálně velký prostor (různé optimalizace), nebo které mají nějakou relevanci ke kvantové fyzice (materiály, baterie, chemie, medicína atp.). Lze je rozdělit na tři skupiny:

1. Samotné kvantové systémy, jež jsou velice těžko simulovatelné klasicky, by mohly být simulovány na dobře kontrolovatelných kvantových systémech – simuluje se kvantové kvantovým. Do téhle skupiny spadají oblasti výzkumu jako navrhování materiálů se specifickými vlastnostmi, baterií, chemických sloučenin anebo léků.

2. Kvantové počítače můžou pomoci s řešením i nekvantových problémů s exponenciálně mnoha možnostmi, pro které nejsou k dispozici klasické efektivní algoritmy. Jedná se o různé optimalizace skrze například kvantové žíhání (koncept hledání minima a maxima v daném prostředí a hledání optimálních scénářů), např. v logistice, ale také při učení neuronových sítí (avšak i přes letitý výzkum v této oblasti ještě nejsou k dispozici spolehlivé algoritmy, u kterých by byla prokázána jejich lepší efektivita než u klasických přístupů).

3. Kvantové počítače mají jinou výpočetní složitostní hierarchii, což otevírá nové směry v teoretické informatice, výuce i hledání hranic výpočtových možností. Třetí oblast tak seskupuje různé specifické kvantové algoritmy, u nichž byla teoreticky prokázána jejich účinnost (Shorův, Groverův, nebo HHL – viz dále). Všechny tyto algoritmy využívají specifické vlastnosti kvantové teorie na řešení specifického problému a nejedná se tak o universální přístup, který by byl schopen generovat třídy algoritmů.

[1] https://ieeexplore.ieee.org/document/9492845

Jelikož ještě nejsou standardně fungující příklady aplikace kvantových počítačů (všechny jsou dosud v experimentální fázi), jedná se spíše o předpoklad, ve kterých oborech kvantové počítače nepřekonají ty klasické, podaří-li se jejich praktická implementace (odstranění šumu apod.)

Každý kvantový počítač umí simulovat klasický výpočet. V případě, že by kvantový a klasický počítač měly stejný výkon a kapacitu, byly by téměř stejně rychlé. Jelikož jsou současné kvantové počítače značně pomalejší, tohle přirovnání není zcela vhodné, ale ukazuje na to, že u výpočtů, jenž jsou efektivní na klasických počítačích není nutné využívat počítače kvantové.

Odhaduje se, že v budoucnu budou existovat specializovaná kvantová zařízení podobná grafickým výpočtovým kartám (GPU), která budou dostupná spíše jako cloudové řešení se zapojením do vysoce výkonného počítání. Lze předpokládat jistou fúzi oblasti vysoce výkonného počítání (HPC), datových analýz (HPDA), umělé inteligence (AI), quantum computingu (QC) a jejich aplikací do dalších vědeckých, průmyslových i společenských oborů. Očekávaný je nárust důležitosti kvantových algoritmů, jenž nebudou poskytovat kompletní řešení problémů, ale budou spíše subrutinami používanými na urychlení výpočtů v hybridních úlohách.

Zárodky praktické aplikace QC lze ilustrovat na následujících příkladech:

- JPMorgan Chase ve spolupráci s IBM Research zkoumali možnost použití kvantových výpočtů pro odhad ceny opcí.
- Mitsubishi Chemical v spolupráci s Keio University zkoumají možnost využití kvantových počítačů při simulaci komplexních elektrochemických reakcí.
- Společnost Phasecraft nabízí databázi materiálů, pro které umí poskytnout optimalizované algoritmy na jejich simulaci na kvantových zařízeních.

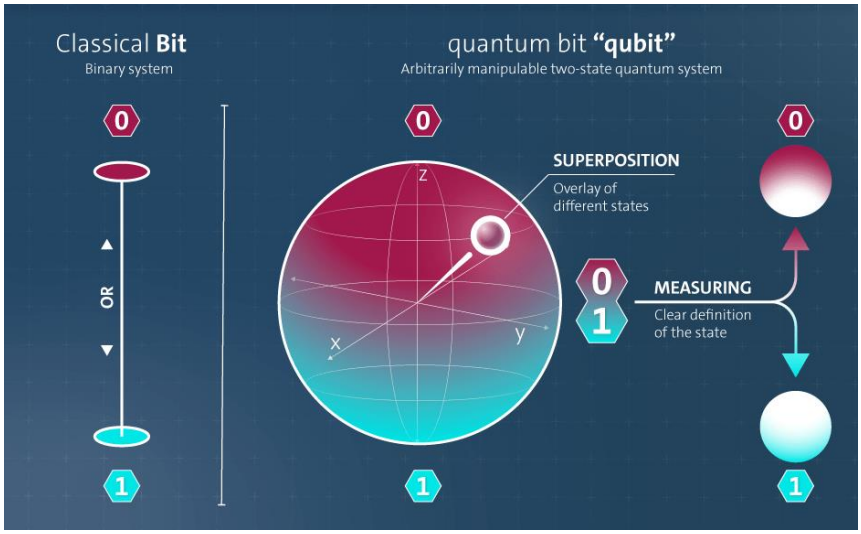
Očekává se rovněž role kvantových počítačů v procesu rozvoje AI a obráceně (v pořadí dle míry rozpracování):

- Využití klasických neuronových sítí na optimalizaci anebo řešení různých kvantových problémů
- Využití kvantových počítačů na urychlení některých procesů při strojovém učení
- Plně kvantová neuronová síť – ukládání informací do qubitů (nejméně rozvinuta oblast)

## 1.4.2 Princip kvantového počítače

Základní jednotkou informace klasických počítačů je jeden bit – může mít hodnotu 0 nebo 1. Z bitů jsou sestaveny registry, nad kterými provádíme různé operace, které stav registru mění. Základní jednotka informace u kvantových počítačů je kvantový bit neboli qubit, který na rozdíl od bitu, může být i ve stavu superpozice $|0\rangle$ a $|1\rangle$. Spojením více qubitů do registru můžeme sestrojit zařízení analogické ke klasickým počítačům. Kvantový výpočet na takovém zařízení probíhá za pomoci aplikace unitárních operací. Výpočet je pak zakončen měřením alespoň části kvantového registru, jehož cílem je předat informaci o jeho stavu uživateli. Kvantový algoritmus musí být navržen tak, aby zaručil, že parciální informace o stavu registru při kvantovém měření má co nejvyšší informační hodnotu. To je však zásadní komplikace plynoucí z teorie, která vede k tomu, že kvantových algoritmů je málo a jsou vhodné jenom na specifické úlohy.

*Obrázek 1: Vizualizace klasického bitu a kvantového bitu (Qubitu)*



Z technologického hlediska je jedním z důležitých faktorů chybovost neboli nepřesnost veškeré manipulace s kvantovými systémy. Je relativně jednoduché mít více qubitů, avšak s počtem qubitů je obtížné držet jejich chybovost na hodnotách dosažitelných při malém počtu qubitů. Chybovost narůstá obzvláště u dvouqubitových operací. Také stávající technologie nejsou fyzicky schopné obsluhovat velké množství qubitů. Většina funkčních kvantových počítačů má proto jenom několik desítek, nebo stovek qubitů.

Z pohledu praktického je dalším zásadním problémem dekoherence. Ta kvantovou informaci uloženou v registrech (qubitů) postupně degraduje. Kvantové výpočty na zařízeních s vyšší úrovní kvantového šumu jsou poté časově omezeny a v současnosti mají daleko k užitečnosti. Snaha o snížení dekoherence je ale v přímém rozporu s naším požadavkem na schopnost systém ovládat (příprava stavů, výpočet a měření). I proto je vývoj kvantových počítačů technologicky náročný. Požadavky na kvantové počítače byly v roce 1996 zformalizovány v Německu působícím americkým teoretickým fyzikem Davidem P. DiVincenzem:

- Škálovatelný systém s dobře definovaným qubitem;
- Schopnost inicializovat qubit do jednoduchého a dobře definovaného stavu;
- Dlouhé koherenční časy;
- Schopnost provádět univerzální (libovolné) výpočty;
- Schopnost měření jednotlivých qubitů.

Když zařízení splňuje tyto požadavky, říkáme, že jde o kvantový počítač. Ne všechna kvantová výpočtová zařízení splňují všechny tyto požadavky. Obzvláště když není dodržen bod 4, je zařízení redukováno na systém nazývající se kvantový simulátor, který dokáže provádět jenom specifické výpočty. Příkladem je např. systém společnosti D-Wave Systems.

Dosažení splnění všech pěti požadavků, obzvláště omezení šumu (dekoherenci) je věnováno značné úsilí. Dnešní stádium vývoje se nazývá NISQ éra (noisy intermediate-scale quantum), kdy jsme omezeni nejen šumem, ale také technologickými schopnostmi výroby jednotlivých komponent a podpůrné techniky, které kladou omezení na velikost a kvalitu zařízení.

V potlačování šumu se využívají různé přístupy:

- Mitigace (zmenšování) šumu a navrhování algoritmů tak aby fungovaly i přes přetrvávající šum – snaha dosažení tzv. quantum utility (kvantové užitečnosti), kdy hlavním cílem je užitečnost algoritmu, a ne jeho škálovatelnost (možnost aplikace na větší zadání).
- Hardwarové přístupy, jako např. cat qubity (Alice & Bob), topologické qubity (Microsoft). U těchto přístupů se výrobci snaží „zakódovat“ kvantovou informaci do té části (komplikovanějšího) kvantového systému, která je méně zasažena vlivem okolí. Okolí tak převážně interaguje s tou částí stavu, která výpočetní kvantovou informaci nedisponuje, a tak ji nedegraduje.
- Kvantová oprava chyb vedoucí k fault-tolerant (FT) výpočtům (popsaná v následující samostatné kapitole).

### 1.4.3 Kvantová oprava chyb

V klasických počítačích také dochází k pozvolné degradaci informace, která se však dá zpomalit za pomoci opravy chyb natolik, že klasické počítače provádějí výpočty prakticky bez chyb. Základním principem opravy chyb je znásobení bitů, které, za využití specifického kódování, danou informaci uchovávají a při případné chybě je možné ji opravit na základě získání informace z části systému. Klasická oprava chyb tak spoléhá na možnost znásobení informace (kopírování), což je v kvantové teorii nepřípustné, protože měření v kvantové teorii nezvratně mění stav měřeného systému.

Snaha o vytvoření kvantového analogu klasické opravy chyb tak naráží na omezení kladené kvantovou teorii. Algoritmy pro kvantovou opravu chyb jsou tudíž výrazně odlišné od klasických přístupů. Podobnost spočívá v tom, že qubity dané technologie (fyzické qubity) jsou seskupeny a kódovány do větších celků, kterým říkáme logické qubity (definice a dělení druhů qubitů je dále rozvedeno v následující kapitole). Základním cílem je, aby chybovost a dekoherence na logickém qubitu byla menší než na fyzických qubitech.

Princip fungování protokolů kvantových oprav chyb spočívá ve schopnosti kódování kvantové informace do jedné části systému (fyzických qubitů), přičemž musí zaručit schopnost za pomoci slabých měření odhalit k jaké chybě došlo a opravit ji. To vyžaduje, aby chyby na fyzických qubitech byly dostatečně malé a nekumulovaly se při implementaci protokolu. Existuje proto hraniční velikost chyb, kterou musí samotná technologie dosáhnout, aby bylo možné na ni opravu chyb aplikovat.

## 1.4.4 Základní stavební prvky kvantových počítačů

- **Fyzický qubit**

Tyto qubity jsou základními kameny kvantových počítačů. Jsou to skutečné fyzické systémy, které se používají k ukládání kvantových informací a manipulace s nimi. Každý fyzický qubit může existovat v superpozici 0 a 1 a může být provázán s jinými qubity, což umožňuje kvantovým počítačům provádět složité operace.

Fyzické qubity jsou však velmi křehké a náchylné k chybám způsobeným vnějším šumem, nedokonalou kontrolou a interakcemi s okolím (dekoherence). Kvůli těmto nestabilitám jsou operace s fyzickými qubity náchylné k chybám, což omezuje spolehlivost a škálovatelnost současných kvantových počítačů.

Pro vývoj kvantových počítačů jsou však fyzické qubity nezbytné. Používají se v dnešních NISQ (Noisy Intermediate-Scale Quantum) zařízeních jako je procesor IBM Eagle, nebo čip Google Sycamore.

- **Logický qubit**

V kvantové výpočetní technice jsou logické qubity konceptem vyšší úrovně. Tyto qubity již nejsou jednou fyzickou entitou, spíše se dají popsat jako zakódovaný stav rozložený mezi mnoho fyzických qubitů.

Hlavním účelem těchto qubitů je dosáhnutí korekce chyb, čehož dosahují za pomocí kvantových kódů pro korekce chyb. Tento systém funguje na základě rozložení informace mezi více fyzických qubitů takovým způsobem, že i když některé fyzické qubity dosáhnou chybovosti, celkový logický qubit zůstane stabilní a neporušený.

Logické qubity mohou detekovat a opravovat chyby bez narušení uložené kvantové informace, což je činí odolnými vůči šumu a dekoherenci. Sestavení a provoz logických qubitů je rozhodujícím krokem k vytvoření kvantových počítačů odolných proti chybám, které jsou schopny spolehlivě provádět dlouhé a složité výpočty.

Vzhledem k metodám korekce chyb a požadované úrovni chybovosti jsou k vytvoření jednoho logického qubitu zapotřebí stovky nebo i tisíce fyzických qubitů.

## 1.4.5 Druhy fyzických qubitů

Způsob fungování kvantového počítač, určuje druh použitého fyzického qubitu. Technologie dosud není ustálená a existuje více navzájem soupeřících principů, z nichž každý má svoje výhody a nevýhody, neboť v praxi nejsou všechny qubity stejné povahy. V reálných kvantových procesorech jsou známé:

- **Supravodivé qubity**
  - Princip: Qubity tvoří supravodivé smyčky (např. Josephsonovy kontakty), ve kterých proudí proud bez odporu. Stav qubitu je určen kvantovými stavy proudu nebo fáze.
  - Výhody: Dobře škálovatelné litografickými technikami (CMOS-kompatibilní), rychlé brány (~ns).
  - Nevýhody: Nutnost extrémního chlazení (~10 mK, kryostat), koherence ~100 μs (omezená), vysoké nároky na přesnost.
  - Výzvy pro FT: Velké množství qubitů kvůli chybovosti, potřeba vysoké fidelity (přesnosti) brán a efektivního korekčního kódu.
  - Výrobci: IBM, Google, Rigetti, IQM (Finsko),

- **Ion trap (iontové pasti)**
  - Princip: Jednotlivé ionty jsou zachyceny v elektromagnetické pasti a manipulovány pomocí laserů. Qubitem je elektronický/spinový stav iontu.
  - Výhody: Dlouhá koherence (v řádu sekund až minut), vysoká fidelita dvouqubitových operací.
  - Nevýhody: Pomalejší operace (ms), obtížnější škálování (potřeba přesné optiky, chladicí systémy).
  - Výzvy pro FT: Lepší integrace optiky a rychlejší brány, modulární škálování (např. propojení více pastí).
  - Výrobci: IonQ, Honeywell/Quantinuum, Alpine Quantum Technologies (Rakousko)

- **Neutrální atomy**
  - Princip: Neutrální atomy jsou zachyceny ve světelných pastích (optické pinzety) a excitovány do Rydbergových stavů, kde se silně ovlivňují.
  - Výhody: Přirozeně vysoká konektivita (každý s každým), dlouhá koherence
  - Nevýhody: Potřeba extrémně precizní optiky a laserů, složitá kontrola více částic.
  - Výzvy pro FT: Zlepšení fidelit brán a stabilita optických mřížek.
  - Výrobci: QuEra, Pasqal (Francie)

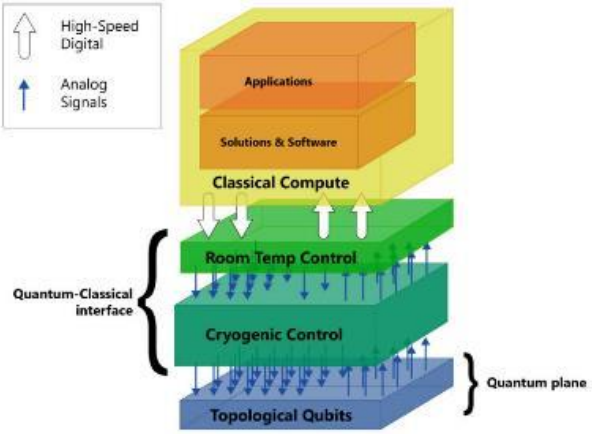
- **Fotonické kvantové počítače**
  - Princip: Qubity tvoří fotony v různých módech (polarizace, dráha). Výpočty se provádějí pomocí interferencí a měření.
  - Výhody: Pracují při pokojové teplotě, snadná distribuce (optická vlákna).
  - Nevýhody: Obtížná deterministická realizace kvantových bran, nízká pravděpodobnost interakce mezi fotony.
  - Výzvy pro FT: Zajištění deterministických brán a kvalitní zdroje jedno-fotonových stavů.
  - Výrobci: PsiQuantum, Xanadu, Quandela

- **Spinové qubity (kvantové tečky)**
  - Princip: Využívá spin elektronu nebo díry v kvantové tečce. Manipulace pomocí magnetického pole nebo mikrovln.
  - Výhody: Možná integrace s běžnými čipy, nízká spotřeba energie.
  - Nevýhody: Velmi malé rozměry, náročné na kontrolu a čtení.
  - Výzvy pro FT: Potřeba precizní výroby kvantových teček, zlepšení koherence a čitelnosti spinových stavů.
  - Výrobci: Intel, Universal Quantum (UK)

## 1.4.6 Fungování kvantových počítačů

Kvantové výpočty jsou prováděny na kvantových čipech, které mohou být založeny na různých technologiích. Tyto čipy jsou propojeny na klasická rozhraní, která zadávají výpočet, řídí výpočet a sbírají a interpretují výsledky. Vzhledem k technologické složitosti nutné k správnému fungování kvantových čipů (velmi nízké teploty, vakuum) je však technologicky značně náročné vytvoření funkčního propojení klasické technologie s tou kvantovou.

*Obrázek 2: Propojení kvantové a klasické vrstvy technologie kvantového čipu*

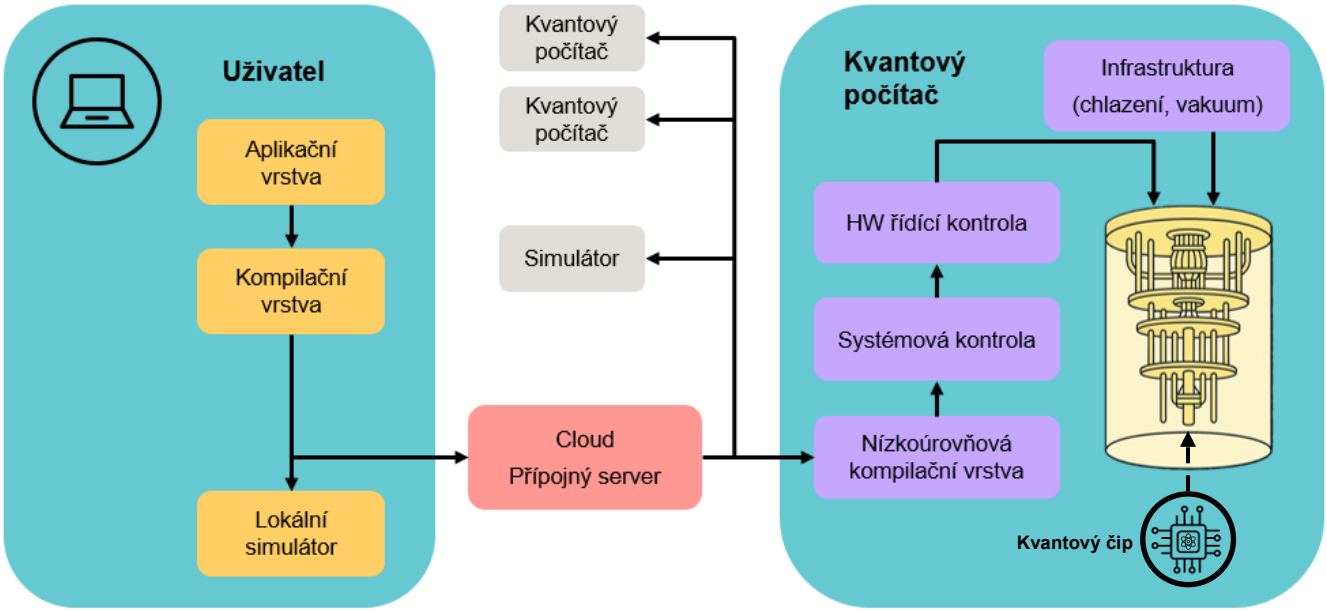



Typicky je tato integrace složena z více vrstev a postup zpracování požadavku uživatele se dá zjednodušeně shrnout do následujících kroků:

1. Uživatel si v aplikační vrstvě navrhne svůj algoritmus.
2. Algoritmus se v kompilační vrstvě zkompiluje – optimalizuje se pro vybraný kvantový počítač a přepíše se do univerzálního jazyka.
3. Požadavek na výpočet se buď provede lokálně (na simulátoru), anebo se odešle do cloudu, který požadavek zpracuje a zařadí do řady na čekání.
4. Když je běh kvantového programu na řadě, požadavek je předán do nízkoúrovňové kompilační vrstvy, kde je přepsán (překompilován) do jazyka, kterému rozumí zařízení, která obsluhují daný kvantový počítač. Program je implementován jako časově specifikovaná sada operací.
5. Požadavek je následně zpracován systémovým řízením, kdy jsou jednotlivé operace v příslušném čase zasílány do jednotlivých zařízení v HW vrstvě, která již generují příslušné signály, jež jsou vysílány do kvantového procesoru.

Přídavná zařízení zabezpečují správné fungování infrastruktury pro fungování samotného kvantového čipu – kryogenní chlazení, udržování vakua, ale také udržování konstantních atmosférických podmínek pro optimální běh veškerých přístrojů. Tento celý systém je znázorněn na obrázku 3.

*Obrázek 3: Propojení klasického a kvantového rozhraní*

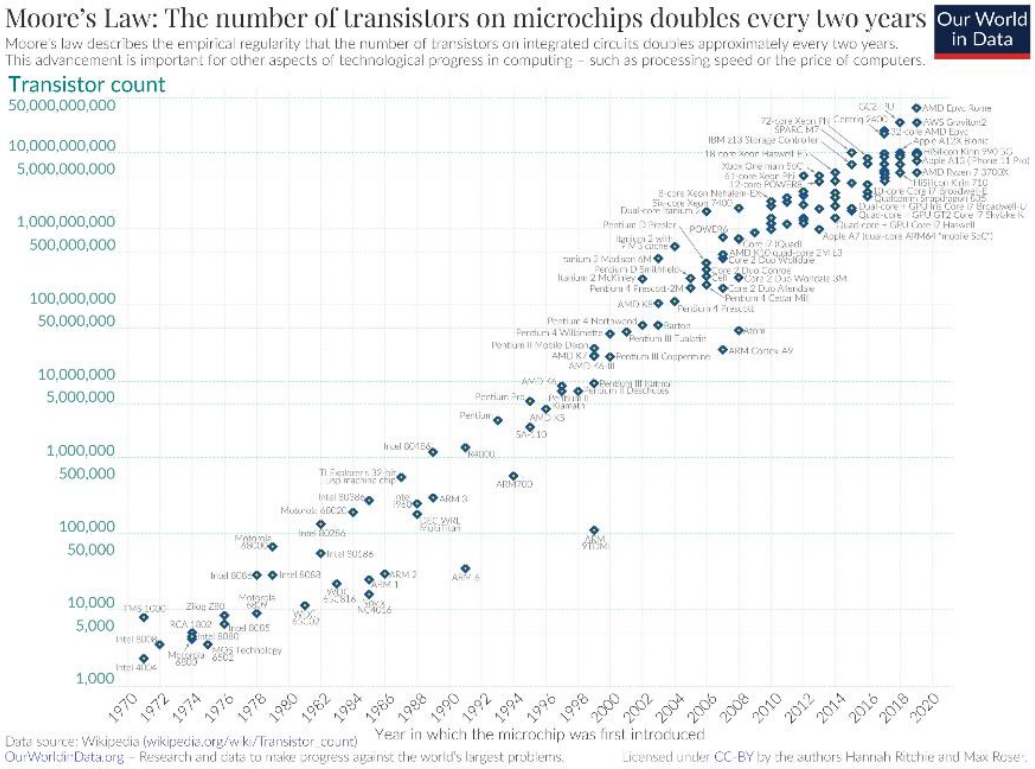



## 1.4.7 Výroba kvantových komponentů

Klasické čipy se vyrábí pomocí technologie CMOS (Complementary Metal-Oxide-Semiconductor). Tento proces zahrnuje fotolitografii, při níž se na křemíkové destičky leptají složité vzory tranzistorů. Z empirických dat vývoje klasických čipů jsou zřejmé zákonitosti, které se obecně nazývají Moorův zákon. Ten tvrdí, že počet tranzistorů v integrovaných obvodech se zdvojnásobuje každé dva roky[2]:

[2] https://ourworldindata.org/moores-law

*Obrázek 4: Moorův zákon v horizontu let 1970–2020*




To znamená, že nutně dochází k zmenšování těchto součástek, a to až k materiální hranici jejich výpočetního výkonu – již nebude možné dále zvyšovat jejich výkon nikoliv kvůli technickým omezením při výrobě, ale kvůli fyzikálním limitům použitého materiálu (křemíku). V dnešní době hovoříme o velikostech na úrovni několika atomů a při vývoji takto malých klasických čipů již není možno ignorovat kvantové efekty, které musí být při jejich návrhu zohledňovány, aby nenarušovaly požadavky na standardní chování čipů. (Tyto kvantové efekty jsou však vysoce lokalizovány a není možné je využít na kvantové výpočty, pro které by byla nutná lepší kontrola nad systémem.) Pomoci překlenout problém se zmenšováním klasických čipů by mohly právě kvantové počítače v roli řešitele specifických složitých podúloh.

Oproti uvedenému je výroba kvantových čipů je závislá na typu implementovaných fyzických qubitů. Čipy supravodivých qubitů se vyrábějí ze supravodivých materiálů, jako je niob nebo hliník. Tyto materiály vykazují nulový elektrický odpor při kryogenních teplotách, což umožňuje efektivní využití těchto qubitů. Spinové qubity využívají spinových stavů elektronů uzavřených v polovodičových kvantových tečkách. Výroba zahrnuje pokročilé nanofabrikační techniky k vytvoření a ovládání těchto kvantových teček. Čipy s fotonickými qubity vyžadují využití optických komponentů, jako jsou rozdělovače paprsků a fázové měniče, často vyráběné na křemíkových fotonických platformách. Každá z těchto technologií vyžaduje specifické přístupy výroby, které ještě nejsou plně standardizovány, jako to je u výroby klasických čipů.

Zatímco klasické počítačové čipy jsou schopné operovat v teplotách od 0 °C do 85 °C v závislosti na aplikaci technologie, tak kvantové komponenty vyžadují extrémně nízké teploty k zachování koherence jednotlivých qubitů. Teploty se rozlišují na základě použitých typů fyzických qubitů, které jsou popsány výše. Většina z těchto typů vyžaduje teploty blízké k absolutní nule, což vyžaduje neustále funkční kryogenní zařízení v okolí qubitů zajišťující odpovídající teplotní podmínky.

Fotonické fyzické qubity jsou výjimkou, mohou fungovat při pokojové teplotě, což nabízí výhody z hlediska jednodušší integrace a škálovatelnosti, avšak zároveň kladou náročné požadavky na přesné řízení optických cest, interferencí a detekce jednotlivých fotonů, což škálovatelnost zatím prakticky omezuje. Dalším omezením je, že na rozdíl od deterministických hradel u supravodivých qubitů jsou fotonická hradla často pravděpodobnostní a vyžadují postselekci, což komplikuje škálování. A nakonec omezení jsou i na detektorech fotonů. Používají se buďto lavinové fotodiodové detektory (APDs), které fungují i při pokojové teplotě, ale mají vyšší šum a nižší výkon, často tedy nestačí pro vysoce přesné kvantové experimenty, anebo jsou využívány supravodivé jednofotonové detektory (SNSPDs), které ale fungují pouze při teplotách pod 1 K. Tyto detektory mají vysokou detekční účinnost (často > 90 %), nízký šum a velmi dobré časové rozlišení, proto jsou preferované pro kvantové aplikace.

## 1.4.8 Stav vývoje kvantových technologií a komunikace

V následující kapitole jsou popsány současné technologie v oblasti kvantové výpočetní technologie napříč různými organizacemi a státy. V rámci popisu technologií jsou uváděny hlavní metriky ukazující na stav vývoje technologie jako je počet qubitů a například i rychlost zpracování složitých matematických úloh. Navazující technické parametry, které by svým popisem zacházely do přílišné odbornosti a jejich rozepsání v rámci této studie není tak relevantní, jsou doplněny odkazem na příslušné zdroje.

- **IBM**

Společnost IBM se zpočátku vývoje kvantových technologií zaměřila zejména na zvyšování počtu qubitů pro neustálé zvyšování výpočetního výkonu zařízení, v této oblasti nyní dominuje procesor IBM Condor s kapacitou 1 121 qubitů. V roce 2023 však IBM změnila strategii a zaměřila se kromě zvyšování kapacity procesorů také na kvalitu a komplexnost využití. Současně využívaný procesor IBM Quantum Eagle s kapacitou 127 qubitů je nyní v experimentech nahrazován nejnovějším procesorem IBM Quantum Heron s kapacitou 133 anebo 156 qubitů. Při srovnání procesoru Condor s procesorem Heron IBM neočekává, že by procesor Condor byl tak užitečný pro provádění kvantových výpočtů jako Heron, a považuje jej spíše za výzkumný úkol zaměřený na rozšíření hardwarového a softwarového balíku společnosti a testování možné kapacity procesorů. Na druhou stranu Heron znamená výrazné zlepšení výkonu a očekává se, že bude přinášet výrazně lepší výsledky při složitých kvantových výpočtech[3]. IBM neustále vyvíjí další generace procesorů s cílem dosáhnout kapacity 100 milionu qubitů s modelem Starling do roku 2030 a integrací kvantové opravy chyb[4].

Při vývoji svých systému se IBM soustřeďuje nejen na samotné kvantové systémy, ale také na zvýšení jejich variability a užitečnosti. Zejména se v současnosti zaměřují na dosáhnutí tzv. kvantové užitečnosti (quantum utility), což znamená, že by jejich kvantové systémy překonaly při řešení konkrétních úloh klasické počítače. To lze dosáhnout nejenom zlepšením kvality procesorů, ale také propojováním klasických a kvantových výpočetních přístupů (Quantum-centric supercomputing), modularitou vedoucí k možností kvantového propojování procesorů (IBM Quantum System Two využívá 3 procesory Heron). K dosažení tohoto pokroku přispívají dále Qiskit SDK, open-source sada pro vývoj softwaru pro kvantové počítače, a Qiskit Runtime, optimalizované spouštěcí prostředí, které IBM vytvořila. Tyto systémy jsou dostupné i vnějším uživatelům, přičemž přístup je placen způsobem pay-as-you-go ($96 / minutu) nebo přes předplatné.

*Obrázek 5: Kvantový počítač IBM*

[3] https://www.allaboutcircuits.com/news/closer-look-at-ibms-heron-and-condor-quantum-processors/

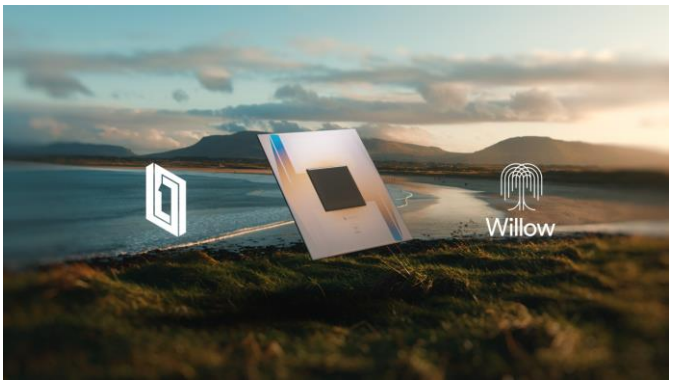
[4] https://www.ibm.com/roadmaps/quantum/

- **Google**

Společnost Google v roce 2019 jako dosáhla průlomu v kvantových technologiích představením modelu Sycamore s kapacitou 53 qubitů, který byl schopný v rámci testování provést specifický výpočetní úkol za zlomek času oproti klasickému superpočítači – jako první ohlásili důkaz kvantové nadvlády (kdy kvantový výpočet je výrazně rychlejší než klasický). Tenhle výsledek byl později zpochybněn ze strany IBM a vědců z Čínské akademie věd, ale nikoli vyvrácen. Na jedné straně z prací plyne, že Google nadhodnotil svůj odhad času pro klasický výpočet (existují i efektivnější metody pro klasický výpočet), ale na straně druhé možné tyto klasické výsledky získat pouze za cenu využití značných zdrojů, překračujících ty kvantové.

V průběhu dalších let Google usilovně pracoval na vývoji nových modelů a vylepšování stávajících, důležitým bodem v současném vývoji je tak představení kvantového čipu Willow s kapacitou 105 qubitů v roce 2024. Tento nejnovější produkt se stal vlajkovou lodí kvantového vývoje Google a v provedených výpočetních testech opět překonal nejvýkonnější superpočítače, kdy dle vyjádření Google za 5 minut provedl výpočet, který by klasickému superpočítači zabral $10^{25}$ let.

*Obrázek 6: Představení kvantového čipu Willow od společnosti Google*




Čip Willow je ale zejména důležitým milníkem na cestě ke kvantové opravě chyb. Zvětšováním pole fyzických qubitů které kódují jeden logický qubit, od mřížky 3x3 kódovaných qubitů přes mřížku 5x5 až po mřížku 7x7 se podařilo snižovat chybovost qubitu, čímž dle tvrzení členů týmu byly dosaženy hodnoty „pod prahem“, který umožňuje škálování. Jelikož implementace jednoho logického qubitu využila téměř celý čip, tato možnost ostává jenom hypotetickou. Navíc oprava chyb se zdařila jenom na qubitu, který nebyl měněn, což je další element, který vnáší chybovost do kvantových výpočtů.

- **IQM**

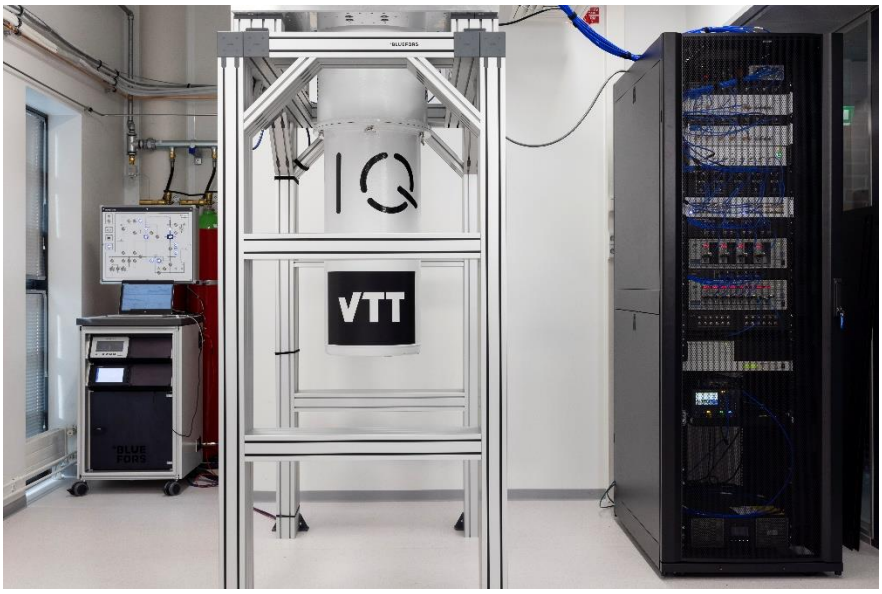
IQM Quantum Computers je finská společnost založená v roce 2018, která se zaměřuje na vývoj kvantových procesorů na míru, zejména pro výzkumné a vládní instituce. IQM staví své procesory na supravodivých qubitech a soustředí se nejen na zvyšování jejich počtu, ale především na zlepšování kvality operací, věrnosti hradel a stabilitu. V roce 2023 oznámila dosažení více než 99,9% věrnosti u dvouqubitových hradel. Kromě toho se věnuje technologiím jako jsou laditelné vazby (tunable couplers) a prvky kvantové korekce chyb.

Namísto budování vlastního cloudového přístupu dodává IQM celé kvantové systémy přímo partnerům, například ve Finsku ve spolupráci se výzkumným centrem VTT[5] (5-, 20- a 50-qubitové systémy), nebo v Německu v rámci projektu Euro-Q-Exa[6]. Plánováno je dodání 24-qubitového systému, kde jsou všechny qubity napojeny na centrální rezonátor, čímž je docílena konektivita každého qubitu navzájem. Společnost usiluje o evropskou technologickou suverenitu a spolupracuje v rámci programů jako Quantum Flagship, OpenSuperQ nebo Qu-Pilot. Snaží se o plně vertikální přístup, od návrhu čipu až po kryogenní infrastrukturu.

[5] https://thequantuminsider.com/2025/03/04/vtt-and-iqm-launch-first-50-qubit-quantum-computer-developed-in-europe/

[6] https://meetiqm.com/press-releases/iqm-selected-to-deliver-two-advanced-quantum-computers-as-part-of-euro-q-exa-hybrid-system/

*Obrázek 7: Kvantový počítač Helmi organizace VTT*




- **Quantinuum**

Quantinuum figuruje jako jedna z předních vývojových institucí na poli kvantových počítačů fungujících na principu iontových pastí. Quantinuum postupným vývojem pomalu odstraňuje hlavní nevýhody iontových pastí, kterou je slabá škálovatelnost. To dosahuje nahrazením lineárních pastí tzv. racetracky, kde je možné uchovávat více iontů za cenu pomalejších operací.
Ve spolupráci se společností Microsoft v Quantinuu dosáhli průlomu ve vývoji kvantových počítačů odolných vůči chybovosti tím, že předvedla vytvoření 4 logických qubitů z 32 fyzických qubitů v kvantovém procesoru Quantinuum H2[7]. Při testu se potvrdila 800krát nižší chybovost než odpovídající fyzická chybovost. Tento model tak dosahuje přesnosti v 99,9 % provedených kvantových operací[8].

V roce 2025 chystá Quantinuum spustit svůj první komerčně dostupný model Helios. Tento systém staví zejména na velmi pokročilých výpočetních kapacitách modelu H2 a jeho možností další spolehlivé škálovatelnosti pro průmyslové použití. Mezi hlavní vlastnosti modelu Helios bude patřit kapacita přes 50 logických qubitů, zároveň s využitím poznatků ze systému H2 v oblasti sofistikované techniky korekce chyb, čímž zvýší stabilitu a spolehlivost kvantových operací. Využití tohoto modelu je očekáváno zejména ve složitých matematických oblastech, jako je teorie uzlů, a to díky efektivní analýze složitých topologických struktur[9]. Dalším očekávaným přínosem je schopnost systému posílení schopností generativní kvantové umělé inteligence, zejména v oblastech, jako je objevování léčiv a věda o materiálech[10].

- **Zuchongzhi**

Vědci z Čínské univerzity vědy a techniky (USTC) v roce 2020 představili kvantový počítač Jiuzhang v návaznosti na předchozí vydání modelu Sycamore od společnosti Google. V tu dobu oba modely dosahovaly na základě testování takzvané kvantové výpočetní výhody neboli „kvantové převahy“, kdy v konkrétních úlohách překonaly nejpokročilejší klasické superpočítače. V roce 2021 Čína pokračovala v posunu této technologie, kdy vyvinula 66-qubitový programovatelný supravodivý kvantový výpočetní systém s názvem Zuchongzhi 2.1. V nedávné době byl představen nástupce tohoto modelu, Zuchongzhi 3.0 s kapacitou 105 qubitů, který dle dostupných informací dosahuje při jednom z klíčových testů kvantových technologií, náhodného vzorkování obvodů (RCS – random circuit sampling) výsledků až milionkrát lepších než nejmodernější model Willow od Google.

Při porovnávání modelů Zuchongzi 3.0 a Willow je však potřeba brát v potaz i směr, kterým se jednotlivé vědecké týmy v rámci vývoje vydali. Zuchongzhi 3.0 se zaměřil zejména na rozsah a rychlost, zatímco Google Willow kladl důraz na přesnost

[7] https://www.quantinuum.com/products-solutions/quantinuum-systems

[8] https://thequantuminsider.com/2024/04/16/three-nines-surpassed-quantinuum-notches-milestones-for-hardware-fidelity-and-quantum-volume/

[9] https://www.nature.com/articles/d41586-025-01094-z

[10] https://thequantuminsider.com/2025/02/04/quantinuum-touts-generative-quantum-ais-massive-commercial-potential/

prostřednictvím qubitů s korekcí chyb. Každé tvrzení o prvenství/výhodě je proto spojeno s výhradami ohledně toho, co bylo měřeno. Experiment USTC maximalizoval velikost a složitost obvodu (při zachování dostatečně nízké chybovosti), zatímco experiment společnosti Google potvrdil, že logické qubity mohou ve spolehlivosti překonat fyzické qubity. Oba tyto pokusy jsou zásadními milníky na cestě k užitečným kvantovým počítačům[11].

- **AQT**

Alpine Quantum Technologies (AQT) je rakouská společnost se sídlem v Innsbrucku, založená v roce 2018 jako spin-off z Universität Innsbruck a Rakouské akademie věd. Specializuje se na kvantové počítače založené na iontové pasti – konkrétně využívá jednotlivé ionty zachycené v lineární Paulově pasti jako qubity. Tento přístup nabízí dlouhé koherence a vysokou přesnost operací, které jsou prováděny pomocí laserových impulsů.

AQT klade důraz na modularitu a kompaktnost – jejich cílem je vyvíjet kvantové počítače jako „rack-mounted" zařízení kompatibilní s klasickou IT infrastrukturou. Nabízí přístup ke svým systémům přes cloud i jako fyzické zařízení pro partnery. V roce 2023 AQT oznámila dosažení fidelit nad 99,9% u jedno- i dvou-qubitových operací a pokračuje v integraci komponent potřebných pro škálování, včetně mikroskopických iontových čipů a fotonických rozhraní. V současnosti nabízí kvantové počítače Marmot (20 plně propojených qubitů) a IBEX Q1 (12 plně propojených qubitů). AQT nabízí také vzdálený přístup do svých kvantových simulátorů a počítače prostřednictvím produktu Arnica[12].

- **D-Wave**

D-Wave Quantum Inc. je kanadská společnost se sídlem v Burnaby (Britská Kolumbie), založená v roce 1999. Patří mezi průkopníky v oblasti kvantových výpočtů, ale na rozdíl od většiny ostatních výrobců se soustředí primárně na kvantové žíhání (quantum annealing) místo univerzálního kvantového počítání. Využívá supravodivé qubity uspořádané do specializovaných topologií (např. Chimera, Pegasus, Zephyr), které umožňují řešit kombinatorické optimalizační úlohy. D-Wave staví systémy s tisíci qubity — v roce 2020 představili systém Advantage se 5000 qubity, v roce 2023 oznámili platformu Advantage2 s cílem dosáhnout přes 7000 qubitů a zlepšenou konektivitou.

Ačkoli žíhací procesory nejsou univerzální (nelze na nich efektivně provozovat kvantové algoritmy jako Shorův nebo Groverův), D-Wave se v posledních letech snaží přiblížit obecnému kvantovému výpočtu — vyvíjí gate-modelový systém (klasický kvantový procesor s hradly), jehož prvotní verze má být přístupná přes cloud. Vedle hardwaru nabízí i komplexní softwarovou vrstvu včetně programovacího jazyka Ocean, nástrojů pro hybridní výpočty a simulační knihovny.

D-Wave spolupracuje s řadou průmyslových partnerů (např. Volkswagen, Lockheed Martin) na reálných aplikacích kvantového žíhání v logistice, plánování nebo strojovém učení. Firma také nabízí přístup ke svým systémům přes cloudovou službu Leap, včetně integrace do AWS. I přes rozdílnou cestu vůči ostatním výrobcům má D-Wave pevnou pozici na trhu a jako první nabídla komerčně dostupný kvantový počítač[13].

## 1.4.9 Vybrané kvantové algoritmy

Jak již bylo řečeno, nacházení kvantových algoritmů, jenž by byly užitečné a rychlejší než jejich klasické alternativy, je složitý proces, jenž je ovlivněn nejenom samotnými omezeními kvantové teorie, ale také fyzickou realitou ztělesněnou obzvláště v dekoherenci. Mezi nejznámější algoritmy se řadí Shorův algoritmus, Groverův algoritmus, anebo HHL algoritmus. Modernější přístupy se zaměřují spíše na hybridní přístupy, kdy kvantové výpočty nahrazují část většího výpočtu. Jedná se o algoritmy VQE anebo QAOA, u kterých zatím není prokázána jejich větší efektivita oproti klasickým algoritmům.

### 1.4.9.1 Shorův algoritmus

Shorův algoritmus představuje jeden z nejvýznamnějších kvantových algoritmů z hlediska kryptografie. Peter Shor (*1959, americký teoretický informatik) ukázal, že kvantový počítač dokáže efektivně faktorizovat velká čísla, což znamená rozložit tato čísla na součiny prvočísel ze kterých se původní velké číslo skládá, a tímto postupem řešit problémy diskrétního logaritmu, tedy komplexních matematických úloh, které lze provést z jedné strany, ale je velmi složité je provést ze strany druhé, a na nichž stojí bezpečnost běžných asymetrických šifer jako RSA a ECC. Teoreticky to znamená, že dostatečně výkonný kvantový počítač by mohl rozložit např. 2048bitové číslo (modulus RSA) v řádu hodin či dní, čímž by zlikvidoval bezpečnost RSA a příbuzných

[11] https://postquantum.com/industry-news/zuchongzhi-3-0-quantum-chip/

[12] https://www.aqt.eu/products/arnica/

[13] https://www.dwavequantum.com/company/newsroom/press-release/d-wave-announces-general-availability-of-advantage2-quantum-computer-its-most-advanced-and-performant-system/

algoritmů (např. Diffie-Hellmanův algoritmus, na základě kterého jsou bezpečně předávány kryptografické klíče skrze veřejné komunikační kanály[14]).

Praktické postřehy:

- Odhaduje se, že k prolomení RSA-2048 by bylo třeba kvantový počítač s „kryptograficky relevantními" parametry, tedy s řádem okolo dvacet milionů qubitů a pokročilou korekcí chyb[15]. Dnešní experimentální kvantové počítače dosahují výkonu v desítkách až stovkách qubitů, což znamená, že v současné době zatím nepředstavují hrozbu pro dobře implementovanou kryptografii.
- Při odhadu je možné snížit počet qubitů za cenu vyššího počtu operací.
- Současné kvantové počítače jsou ještě příliš chybové na to, aby dokázaly Shorův algoritmus spustit pro čísla větší než několik málo bitů, vývoj v oblasti kvantových počítačů nicméně neustále akceleruje. To lze demonstrovat na vývoji kvantových procesorů, jejichž výkon vzrostl z 53 qubitů (procesor Sycamore od společnosti Google[16]) na 1 121 qubitů (procesor IBM Condor[17]) během období pěti let, což představuje více než dvacetinásobný nárůst. V roce 2024 navíc Google představil čip Willow se 105 qubity, který dosahuje průlomu v korekci chyb[18], a čínský tým z Univerzity science a technologie v Hefei na jaře 2025 představil prototyp Zuchongzhi 3.0 se 105 qubity, jenž by měl být ještě rychlejší[19], lze tedy očekávat postupné zvyšování efektivního využití Shorova algoritmu.

#### 1.4.9.2 Groverův algoritmus

Dalším významným kvantovým algoritmem je Groverův algoritmus, který urychluje neřízené prohledávání (brute-force) neboli hledání v nestrukturované databázi (Lov Kumar Grover, *1961, indický fyzik a informatik). Groverův algoritmus snižuje časovou složitost hledání hrubou silou zhruba na druhou odmocninu počtu kombinací. Prakticky to znamená, že kvantový počítač by dokázal prohledávat prostor symetrických klíčů dvakrát rychleji oproti klasickému počítači. Dopad na symetrickou kryptografii (např. AES) je takový, že efektivní bezpečnostní úroveň klíče o délce n bitů klesne na zhruba n/2 bitů. Například 128bitový klíč by měl pro kvantového útočníka sílu jen 64 bitů, což již nemusí být dostatečné. Naštěstí je relativně snadné tuto ztrátu kompenzovat – přechodem na 256bitové klíče. NIST i experti uvádějí, že AES-128 a obdobné algoritmy jsou pro nejbližší budoucnost stále považovány za bezpečné, ale z dlouhodobého hlediska je vhodné plánovat nasazení delších klíčů jako AES-256, aby byla zachována dostatečná bezpečnostní rezerva[20]. V rámci 3GPP proběhla analýza, zda je třeba 5Gstandard rozšířit o podporu 256bitových šifer; závěr zněl, že v Release 16 to ještě není nezbytné, ale v budoucnu se s 256bitovými algoritmy počítá[21].

Praktické postřehy:

- Kódování do kvantové databáze není jediný způsob užití Groverova algoritmu; mnohé výpočetní úlohy obsahují tento algoritmus vyhledávání jako podprogram (některé funkce sítí při strojovém učení apod.). V takovém případě je potenciálně možné využít hybridní schéma, kdy kvantový počítač je opakovaně volán s parciální úlohou.
- Groverův algoritmus je pro implementaci značně náročný a stávající kvantové počítače kvůli jejich chybovosti neposkytují zatím žádné urychlení.
- Urychlení Groverova algoritmu se navíc velice rychle vytrácí už při velice malých chybách[22] a je možné spíše očekávat jenom malé urychlení výpočtů[23].

[14] https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf

[15] https://arxiv.org/pdf/1905.09749

[16] https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all

[17] https://www.ibm.com/quantum/blog/quantum-roadmap-2033

[18] https://blog.google/technology/research/google-willow-quantum-chip/

[19] https://english.news.cn/20250303/727767580e4a472ca44fd08f25666a25/c.html#:~:text=HEFEI%2C%20March%203%20%28Xinhua%29%20,in%20China%27s%20quantum%20computing%20advancements

[20] https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf#:~:text=Asymmetric%20key%20cryptography%20faces%20significant,posing%20a%20profound%20security%20risk

[21] https://journal.accsindia.org/show.article.php?id=44#:~:text=introducing%20256,bit%20algorithms%20in%20future%20releases

[22] https://iopscience.iop.org/article/10.1088/1367-2630/16/7/073033

[23] https://journals.aps.org/pra/abstract/10.1103/PhysRevA.99.012339

#### 1.4.9.3 HHL algoritmus

Lineární systémy rovnic $A\vec{x}=\vec{b}$, kde $A$ je známá matice a $\vec{b}$ pravá strana, představují základní výpočetní problém přítomný ve vědeckých i průmyslových aplikacích, od simulací fyzikálních systémů po strojové učení. Klasické řešení soustavy o rozměru $n$ vyžaduje čas závislý alespoň lineárně na velikosti vstupu. Pokud ale dokážeme vhodným způsobem zakódovat jak vektor $\vec{b}$, tak matici $A$ do kvantového stavu a operace, je možné využít HHL algoritmus, který, za určitých podmínek, poskytuje řešení v čase polylogaritmickém v $n$, tedy $O(\log n)$. Tento rozdíl je exponenciální oproti klasickým metodám.

HHL algoritmus (Harrow–Hassidim–Lloyd) nevrací řešení ve formě explicitního vektoru $\vec{x}$, ale v podobě kvantového stavu $|\vec{x}\rangle$, s nímž je možné dále kvantově manipulovat. Urychlení je možné tehdy, pokud je matice $A$ řídká, dobře podmíněná a existuje efektivní procedura pro její kvantové exponentování. V takovém případě je možné využít kvantového algoritmu k získání informací o řešení, například výpočtu očekávaných hodnot nebo korelací bez nutnosti úplného dekódování výsledku.

Praktické postřehy:

- HHL algoritmus neřeší klasický problém „vynásobit inverzi matice“, ale spíše umožňuje získat výpočetně dostupné kvantové reprezentace řešení.
- Podmínkou pro urychlení je nejen řídkost matice, ale také její dobrá kondice (nízké číslo podmíněnosti). U špatně podmíněných úloh se výpočetní náročnost zhoršuje.
- Kvantová reprezentace výsledku neumožňuje snadné vyčtení všech složek řešení, ale je vhodná např. pro výpočty průměrů nebo vnořených výpočetních kroků v kvantovém algoritmu.
- Jako u jiných algoritmů, i HHL vyžaduje rozsáhlou kvantovou paměť a nízkou míru šumu, což současné kvantové procesory zatím neposkytují[24].
- Praktické aplikace HHL se očekávají spíše v hybridních scénářích, kdy kvantová část řeší specifický podproblém ve větší klasické architektuře.

#### 1.4.9.4 VQE (Variational Quantum Eigensolver)

Mnohé důležité úlohy ve fyzice, chemii či optimalizaci spočívají v nalezení základního stavu nějakého kvantového systému, tj. stavu s nejnižší možnou energií. Klasické algoritmy pro hledání základních stavů kvantových systémů (např. molekul) trpí exponenciálním růstem výpočetní složitosti s velikostí systému.

Algoritmus VQE tento problém obchází hybridním přístupem: kvantový počítač připravuje parametrizovaný kvantový stav a měří očekávanou hodnotu energie, zatímco klasický počítač optimalizuje parametry kvantového stavu, aby minimalizoval energii.

Tento variační přístup je dobře přizpůsoben současným kvantovým počítačům s omezenou hloubkou obvodů. Výpočetní složitost neroste exponenciálně s počtem parametrů, ale úspěšnost algoritmu silně závisí na volbě ansatzu (tj. zvolenému tvaru parametrizovaného kvantového stavu) a optimalizační strategie.

Praktické postřehy:

- VQE je jedním z hlavních algoritmických kandidátů pro využití NISQ zařízení v oblasti kvantové chemie.
- Přesnost výpočtu může být zásadně ovlivněna šumem v kvantovém hardware a neschopností optimalizace nalézt globální minimum.
- Mnoho praktických implementací VQE kombinuje s pokročilými klasickými optimalizátory a error-mitigation technikami.
- Pro VQE neexistuje obecný důkaz, že dokáže najít řešení rychleji než nejlepší známé klasické metody.

#### 1.4.9.5 QAOA (Quantum Approximate Optimization Algorithm)

Mnohé optimalizační problémy, jako je rozvrhování, rozdělování zdrojů nebo problémy typu MAX-CUT, jsou NP-těžké (s exponenciálně narůstající složitostí od velikosti problému) a klasické algoritmy na ně poskytují pouze přibližná řešení. QAOA je kvantový algoritmus navržený pro tyto úlohy, který využívá střídání dvou typů kvantových operací: jeden odpovídá klasické energii problému (tzv. cost Hamiltonian) a druhý slouží k míchání stavů (mixer Hamiltonian).

Tímto způsobem QAOA připravuje kvantový stav, který má vysokou pravděpodobnost odpovídat dobrému řešení optimalizační úlohy. Parametry operací se optimalizují (stejně jako ve VQE) klasickým algoritmem. Při dostatečném počtu kroků (hloubce algoritmu) se algoritmus teoreticky blíží exaktnímu řešení, ale v praxi je omezen reálnou fyzickou implementací.

[24] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.050502

Praktické postřehy:

- QAOA se ukazuje jako perspektivní algoritmus pro kombinované kvantově-klasické řešení kombinatorických problémů.
- Účinnost algoritmu závisí nejen na hloubce obvodu, ale i na výběru iniciálních parametrů a vlastnostech optimalizačního prostředí.
- Praktické implementace naráží na omezení současného hardwaru – omezená konektivita, chybovost a nízká fidelita mohou znemožnit dosažení výhod oproti klasickým heuristikám.
- Schopnost kvantového urychlení zůstává otevřenou otázkou – u QAOA neexistuje důkaz, že by dosahoval výhod ani kvadratických, natož exponenciálních oproti klasickým algoritmům.

# 1.5 Kvantová komunikace

Na rozdíl od klasických komunikačních metod se v rámci rozvíjející se kvantové komunikace využívá principů kvantové fyziky pro bezpečný a efektivní přenos informací a dat. Klasické způsoby komunikace se při přenosu spoléhají na elektromagnetické vlny, kvantové přenosy využívají qubity pro přenos informací, které díky vlastnosti superpozice mohou existovat ve více stavech současně. Kritickou podmínkou pro efektivnost kvantové komunikace je také vlastnost kvantové provázanosti jednotlivých qubitů. Takto provázané částice mají vzájemně propojené stavy, což znamená, že stav jedné částice okamžitě ovlivňuje stav druhé částice bez ohledu na vzdálenost, která je dělí. Tento jev má zásadní význam pro kvantovou komunikaci, protože umožňuje okamžitý přenos informací mezi provázanými částicemi[25].

Jak již bylo popsáno výše, jedním z klíčových problémů kryptografie je hledání postupů, jak ustavit kryptografický klíč mezi dvěma komunikujícími stranami tak, aby každá z těchto stran měla stejný klíč, a nikdo další neměl žádnou (ani částečnou) informaci o tomto klíči. Od roku 1994 je známo, že všechny původně používané algoritmy (RSA, Diffie-Hellman, …) budou v okamžiku vytvoření tzv. kvantového počítače poskytovat nulové zabezpečení. Hůře, veškerá dnes zasílaná komunikace je v širokém rozsahu útočníky ukládána a bude zpětně dešifrována až budou k dispozici kvantové počítače s dostatečným výkonem.

To vedlo k hledání alternativ, například algoritmů, o kterých není znám postup, jak je prolomit klasickým či kvantovým počítačem (tzv. postkvantové algoritmy). Tyto algoritmy však stále mohou být prolomeny, a to nejen kvantovým, ale i klasickým počítačem, jak už se stalo u několika finalistů soutěže NIST.

## 1.5.1 Kvantová distribuce klíčů (QKD)

Další alternativou jsou takzvaná zařízení pro Kvantovou distribuci klíče (QKD – Quantum Key Distribution). Tato zařízení využívají principy kvantové teorie k tomu, aby sdílení klíče bylo extrémně bezpečné. V následující kapitole zaměřené na QKD jsou zjednodušeně popsané hlavní rysy jeho fungování. Pojem kvantová komunikace zde bude užíván pro klasickou komunikaci podpořenou kvantovými technologiemi pro sdílení kryptografického klíče.

### 1.5.1.1 QKD zařízení pro vytváření klíčů

QKD zařízení pro vytvoření klíče jsou zatím experimentální zařízení s velkými rozdíly v parametrech, tj. dosud ve fázi vývoje. V současné době neexistují standardizace, co přesně mají QKD zařízení splňovat, neexistují standardizace v oblasti bezpečnostních požadavků, neexistují testovací metodiky, ani laboratoře, které by tyto parametry ověřily. V současné době teprve probíhá řešení těchto problémů na úrovni EU.

Princip vytvoření klíče v kvantovém prostředí lze vysvětlit na protokolu BB84. V protokolu vystupují dvě strany, obvykle nazvané Alice a Bob, které chtějí vytvořit bezpečný sdílený klíč (Alice a Bob jsou ve skutečnosti zařízení vykonávající tento protokol). Alice opakovaně a náhodně připravuje stavy (systémy) ze čtyř specifických možností. Každý systém je potenciálním zdrojem jednoho bitu klíče. Čtyři volby u Alice kódují nejen potenciální bit sdíleného klíče (2 možnosti), ale také náhodný bit, který označuje tzv. bázi pro kódování (2 možnosti). Takto připravený stav ze čtyř (2 x 2) možností výběru Alice je zaslán Bobovi, který si náhodně vybere bázi pro měření zaslaného systému. Alice a Bob si pak pošlou přes běžný (nešifrovaný, ale autentizovaný) kanál informace o tom, jak měřili. Jelikož jsou kvantová měření typicky destruktivní, bude-li Alicina báze kódování odlišná od Bobovy báze pro měření, protokol je nastaven tak, že výsledky měření kvantového stavu budou u Boba nahodilé a nebudou nijak korespondovat s bitem klíče, který Alice odesílá. Pokud tedy zjistí chyby, vědí, že někdo odposlouchával, a klíč zahodí. Naopak v případě, kdy se báze kódování Alice s bází Bobova měření shoduje, nedochází ke změně stavu, která by ovlivnila

[25] https://arxiv.org/abs/quant-ph/0702225

výsledek měření u Boba, ten tak vždy naměří bit, který mu Alice zasílá. Pokud je vše v pořádku, použijí zbylé bity jako bezpečný šifrovací klíč.

Výhodou užití QKD zařízení je také jejich odolnost vůči kvantovým počítačům – kvantové počítače není možné použít na jakékoliv narušení ustanovení klíče tak jak to je u klasických šifrovacích algoritmů. Jde tedy o bezpečnost založenou na fyzikálních vlastnostech, která není závislá na důvěře v algoritmus. Použití QKD zařízení tak vede k vyšší bezpečnosti komunikace.

QKD v návaznosti na kryptografii v kvantovém prostředí je dále popsáno v kapitole 3.3.

#### 1.5.1.2 Praktické využití QKD při komunikaci

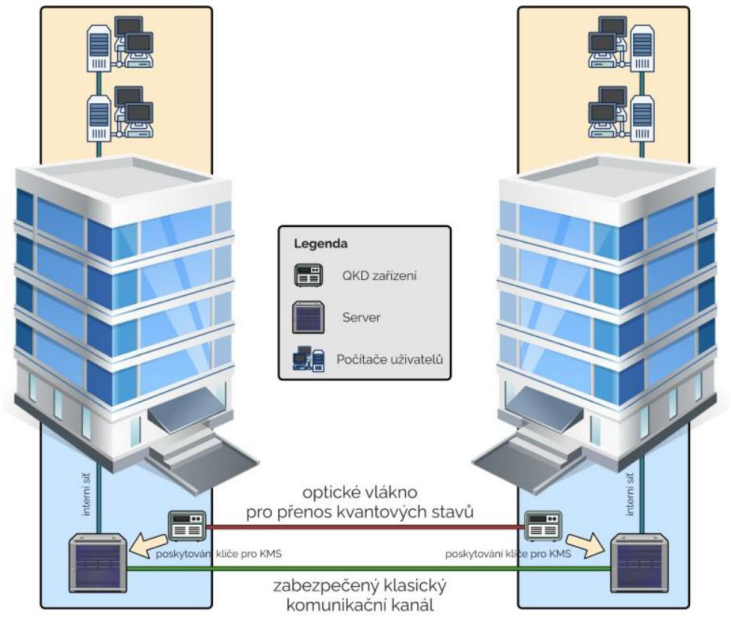
Prakticky si kvantově zabezpečenou komunikaci můžeme představit jako propojení dvou zařízení, které všechny zabezpečovací úkony, včetně testování přítomnosti potenciální odposlouchávající třetí strany, dělají samy. Výhodou je, že pro propojení mohou být použity stávající optické sítě. Pro překlenutí větších délek optického vlákna a dosažení přijatelného množství kryptografického klíče generovaného za vteřinu (bit rate klíče, měřeno v kbps) je v současné době ale důležité, aby komunikace mezi zařízeními probíhala přes tzv. dark-fiber, nenasvícené optické vlákno (resp. pár vláken), vyhrazené pouze pro tuto komunikaci. Navíc spojení musí být nepřerušené, bez zesilovačů nebo přepínačů, které by narušily kvantový přenos.

Využití QKD zařízení je tak omezeno strukturou a existencí optické infrastruktury, jejími kvalitativními parametry (útlumy) a dostupností nepoužívaných vláken. Velkou roli hraje také cena pronájmu optických vláken, která se pro temná vlákna v ČR pohybuje podle oblasti a poskytovatele od 0,5 až po 2,5 CZK za metr vlákna a měsíc pronájmu (bez DPH).

Systém QKD je tvořen dvojicí zařízení, vysílajícím a přijímajícím zařízením. Vysílající zařízení vysílá jednofotonové signály se zakódovanou kvantovou informací. Tyto signály jsou optickým vláknem přenášeny do přijímacího zařízení, které se je pokouší zachytit a dekódovat. Útlum (v rámci přenosové cesty) a bit rate klíče jsou zásadními parametry této technologie.

Po vytvoření společného klíče pak QKD zařízení předají tento klíč systému pro správu klíčů Q-KMS (Quantum Key Management System), který ho poskytne systémům pro šifrování standardní komunikace podobně jako jakýkoliv jinak vytvořený klíč. Rozdíl proti klasickým (nekvantovým) klíčům je však právě v jeho vysoké bezpečnosti při vytváření a distribuci. Schéma zapojení QKD zařízení do komunikační infrastruktury je naznačena na přiloženém obrázku 8.

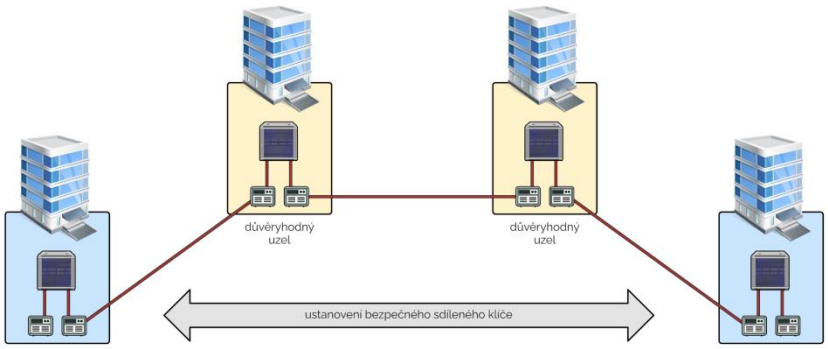
*Obrázek 8: Vizualizace využití QKD pro přenos dat*




Výše popsané zapojení propojuje pouze dva komunikační uzly. V reálném provozu však existuje síť různě propojených uzlů. Typicky mezi sebou komunikují uzly, které nejsou propojeny přímo. I v takovém případě lze zajistit vysoce bezpečnou komunikaci za pomoci QKD zařízení. V praxi se použije pro každé přímé propojení jeden pár QKD zařízení, který vytvoří unikátní klíč mezi těmito uzly. Pro spojení vzdálených uzlů existují algoritmy, které z ‚po párech' vygenerovaných klíčů na přímo propojených

uzlech bezpečně vygenerují klíč na uzlech vzdálených. Jelikož v současné době neexistují metody, které by takto generovaly klíč bez nutnosti vytvoření klíče i na propojovacích uzlech, tyto propojovací uzly musí být důvěryhodné (tzv. trusted nodes). Z teoretického hlediska tyto metody nejsou nepřípustné, jsou jenom technologicky náročné na implementaci.

*Obrázek 9: Vytváření bezpečného sdíleného klíče skrze důvěryhodné propojovací uzly*




### 1.5.1.3 Vybrané protokoly pro kvantové vytvoření klíče

Lze uvést několik typů protokolů, jejichž úkolem je zajistit bezpečnou distribuci šifrovacích klíčů mezi dvěma stranami (např. Alice a Bob) pomocí principů kvantové mechaniky. Jejich hlavní funkce a kroky jsou generování a výměna kvantových stavů, detekce odposlechu a korekce chyb a zesílení soukromí (Post-Processing) a výstupem je bezpečný tajný klíč, který lze použít pro symetrické šifrování.

- **BB84 protokol**

Bezpečná distribuce kryptografického klíče mezi dvěma stranami bez předchozího sdíleného tajemství je zásadním problémem. BB84 protokol [BB84] (v zásadě popsaný výše) byl navržený v roce 1984 a je nejstarší a nejpoužívanější QKD protokol. Jeho konceptuální jednoduchost ho činí ideálním pro první praktické implementace. Využívá kvantové bity, které jsou náhodně připraveny v různých polarizačních nebo spinových stavech, a přenášeny mezi odesílatelem (Alice) a příjemcem (Bobem). Alice připravuje qubit v jedné náhodně zvolené bázi z dvou a Bob měří přijatý qubit taky v jedné náhodně zvolené bázi. Až zpětně si porovnají použité báze přes veřejný kanál, aniž by zveřejnili výsledky měření. Shodující se báze měření determinují sdílený klíč. Jakýkoli pokus útočníka (Eve) odposlouchávat kvantový kanál zanechává detekovatelnou stopu v podobě zvýšené chybovosti.

Protokol vyžaduje, aby jeden uzel byl schopný generovat kvantové stavy, přičemž u druhého uzlu je podstatnější schopnost měření přijatého stavu. Pro zvýšení bezpečnosti se používají tzv. decoy states. Tyto (občasně generované) stavy jsou bezpečnostní past, která umožňuje rozpoznat, zda někdo zasahuje do přenosu bez znalosti toho, které pulzy byly klíčové.

- **BBM92 protokol**

Zatímco BB84 využívá aktivní přípravu a měření kvantových stavů, BBM92 protokol [BBM92] staví na kvantovém provázání. Dvojice fotonů v provázaném stavu je rozdělena mezi Alici a Boba, kteří provádějí měření v náhodně volených bázích. Z provázanosti vyplývá korelace měření, z nichž lze odvodit klíč. Narozdíl od BB84 není potřeba aktivně připravovat jednotlivé kvantové stavy – provázaný zdroj může být centrální a pasivně rozesílat páry.

BBM92 je považován za entanglement-based analogii k BB84, s výhodou v možnosti distribuovaného generování klíče. Provázané protokoly obecně lépe odolávají některým typům útoků, ale jsou technicky náročnější na realizaci; obzvláště je nutné mít trojici zařízení – jedno pro generování provázaného stavu a dva pro komunikující uzly.

- **Ekert91 protokol**

Ekertův protokol [Ekert91], navržený v roce 1991, využívá kvantové provázání a teorii Bellových nerovností ke kontrole bezpečnosti komunikace. Alice a Bob měří provázané stavy ve volených směrech, a kromě generování klíče testují korelace výsledků pomocí Bellových testů. Pokud výsledky porušují Bellovy nerovnosti, znamená to, že komunikace nemohla být klasicky simulována – což zároveň znamená, že nedošlo k odposlechu.

Bezpečnost protokolu vychází z porušení Bellových nerovností, což poskytuje teoreticky silnou ochranu vůči útokům i při neznámém chování zařízení. Praktická implementace je však velmi náročná kvůli potřebě přesného měření kvantových korelací a citlivosti vůči šumu.

- **COW protokol (Coherent One-Way)**

Kvantová distribuce klíče se nemusí spoléhat výhradně na jednotlivé částice nebo kvantové provázání – alternativní přístup nabízí COW protokol, který využívá koherentní světelné pulzy vysílané jedním směrem. Klíč se kóduje do přítomnosti nebo nepřítomnosti světelného pulzu v časovém okně. Přijímač (Bob) zaznamenává, zda detekoval pulz, a zároveň testuje koherenci mezi sousedními pulzy pomocí interferometrie, což umožňuje detekovat přítomnost odposlouchávače.

COW protokol je navržen s ohledem na praktickou realizaci v běžných optických sítích, s nízkými nároky na kvantové zdroje a detektory. Díky své odolnosti vůči ztrátám a schopnosti pracovat s intenzitní modulací je vhodný pro dlouhé vzdálenosti. Neposkytuje stejnou úroveň teoretické bezpečnosti jako protokoly s jednotlivými kvantovými částicemi, ale je atraktivní pro komerční nasazení v reálných sítích, např. v rámci metropolitních QKD sítí.

## 1.5.2 Stav vývoje kvantové komunikace

- **Toshiba Europe**

V rámci testování možností zabezpečené kvantové komunikace proběhl přenos kvantově zašifrovaného signálu přes 254 km dlouhou komerční telekomunikační síť v Německu pomocí standardních optických vláken za použití jednoduché polovodičové technologie, aniž by potřeboval kryogenní zařízení. Tento pokrok umožňuje integrovat kvantovou distribuci klíčů (QKD) a další kvantově bezpečné komunikační protokoly do stávající telekomunikační infrastruktury v národním měřítku, což výrazně snižuje náklady a překážky při zavádění. Zkouška představuje významný krok směrem ke globálnímu kvantovému internetu, protože ukazuje, že kvantová data mohou zůstat stabilní na velké vzdálenosti pomocí běžně dostupného vybavení ve standardních datových centrech[26].

- **Čína**

V roce 2016 byl čínským výzkumným týmem vypuštěn kvantový satelit Micius, který jako první svého druhu dosáhl úspěšného experimentu s distribucí kvantových klíčů (QKD) z vesmíru na zem. V roce 2017 bylo v rámci dalšího testování satelitu Micius dosaženo kvantového propojení na vzdálenost 7 600 km s protistranou v Rakousku[27].

V návaznosti na úspěchy satelitu Micius vědci z Jihoafrické republiky a Číny dosáhli v roce 2024 pomocí čínského kvantového mikrosatelitu Jinan-1 na nízké oběžné dráze Země zatím nejdelšího kvantového propojení ve vzdálenosti 12 900 km. Mezinárodní tým předvedl generování kvantových klíčů v reálném čase pomocí technologie kvantové distribuce klíčů (QKD). Tento proces umožnil bezpečné šifrování snímků přenášených mezi pozemními stanicemi v Číně a Jihoafrické republice pomocí jednorázového šifrování a umožnil přenést mezi oběma zeměmi více než milion kvantově zabezpečených bitů během jediného oběhu[28].

- **Boeing USA**

V roce 2026 plánuje společnost Boeing vypustit satelitní misi Q4S, která má demonstrovat výměnu kvantových provázaností na oběžné dráze, což je významný krok k vybudování bezpečného globálního kvantového internetu. Cílem této první iniciativy svého druhu, vyvinuté ve spolupráci s laboratořemi HRL, je prozkoumat, jak mohou kvantové sítě fungovat na obrovské vzdálenosti při zachování synchronizace a minimalizaci ztráty dat. Mise Q4S bude testovat komunikaci založenou na kvantové teleportaci, což může v budoucnu umožnit aplikace, jako jsou kvantové výpočty odolné vůči poruchám, bezpečné hlasování a slepé kvantové výpočty. Vizí společnosti Boeing je zprovoznit tyto kvantové technologie ve velkém měřítku a satelity, vybavené zdroji provázaných fotonů, poskytnou kritická data pro rozvoj vesmírných kvantových sítí a ultrabezpečné komunikace[29].

[26] https://www.toshiba.eu/newsroom/toshiba-breakthrough-brings-quantum-communications-to-existing-national-scale-telecommunications-infrastructure/

[27] https://www.sciencedaily.com/releases/2025/03/250319142833.htm

[28] https://spaceinafrica.com/2025/03/20/south-africa-and-china-establish-12900-km-quantum-satellite-link/

[29] https://boeing.mediaroom.com/2024-09-10-Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite

# 2 Architektura 5G a její kryptografická ochrana

## 2.1 Bezpečnostní architektura 5G

### 2.1.1 Autentizační protokoly

Účelem postupů primární autentizace a dohody o klíči (AKA) je umožnit vzájemnou autentizaci mezi uživatelským zařízením (UE) a sítí a poskytnout klíčový materiál, který lze použít mezi UE a obsluhující sítí v následných bezpečnostních postupech. Základními autentizačními protokoly dle specifikace 3GPP TS 33.501 (Rel-15) jsou[30]:

- **5G-AKA**

Tento autentizační protokol je přímým pokračováním protokolu známého z 3G a 4G sítí využívající symetrické klíče mezi UE a sítí pouze v rámci 3GPP přístupů (např. NR, LTE) a je jednou ze dvou povinných autentizačních metod v rámci 5G architektury.

- **EAP-AKA**

Druhým autentizačním protokolem nutným pro přístup k 5G jádru přes jakýkoli typ přístupu je EAP AKA. Tato metoda integruje EAP (Extensible Authentication Protocol) rámec pevně do 5G bezpečnosti, na rozdíl od EPS (Evolved Packet System), kde byla podpora EAP-AKA/EAP-AKA' využívána pouze pro ne-3GPP přístup. Na rozdíl od 5G AKA je tento autentizační protokol použitelný také pro ne-3GPP přístup (např. Wi-Fi, LAN, neautorizovaný přístup) čímž nabízí širší možnosti a flexibilitu použití.

### 2.1.2 Šifrování a ochrana dat

Architektura 5G v návaznosti na předchozí generace pokračuje ve využívání osvědčených bezpečnostních a šifrovacích algoritmů k poskytování bezpečných komunikačních služeb pro koncová zařízení, ale i vlastní infrastrukturu. Stejně jako ve 4G jsou tak použity šifrovací algoritmy založené na SNOW 3G, AES-CTR a ZUC a algoritmy integrity založené na SNOW 3G, AES-CMAC a ZUC[31]. Hlavní funkce odvození klíče je založena na bezpečném HMAC-SHA-256.

V rámci systémů 5G je zahrnuta také ochrana proti odposlechu a útokům modifikujícím signál. Novou funkcí oproti předchozím generacím je ochrana integrity dat nejen pro data na úrovni řídící roviny (control plane), ale také pro uživatelská data (user plane). Tato nová funkce umožňuje efektivně detekovat jakékoliv pokusy o modifikaci dat během přenosu a je obzvlášť cenná pro přenosy malých objemů dat, zejména co se týče IoT zařízení[32].

V rámci 3GPP Rel-15 byla pro 5G zavedena také nová a klíčová funkce network slicing. Tato technologie umožňuje poskytovatelům komunikačních služeb (CSP) vytvářet virtuální sítě, které jsou optimalizovány pro konkrétní potřeby konkrétních uživatelů nebo aplikací. Tento koncept umožňuje doslova rozdělit fyzickou infrastrukturu sítě do virtuálních segmentů, které lze spravovat nezávisle a poskytovat specifické úrovně výkonu, propustnosti a zabezpečení.

5G network slicing je jinak řečeno síťová architektura, která umožňuje multiplexování virtualizovaných a nezávislých logických sítí na stejné fyzické síťové infrastruktuře. Každý segment sítě je izolovaná síť typu end-to-end přizpůsobená tak, aby splňovala různé požadavky pro konkrétní aplikaci. Network slicing tedy v praxi znamená, že operátor 5G sítě může vytvořit různé virtuální

[30] https://www.3gpp.org/technologies/sec-npn

[31] https://www.3gpp.org/dynareport?code=35-series.htm

[32] https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system

sítě, které budou garantovat i různé parametry potřebné pro různé zákazníky a aplikace. Logická část sítě tedy slouží pouze pro daný účel nebo daného zákazníka, čímž poskytuje jedinečnou nezávislost a bezpečnost jednotlivých virtuálních sítí.

## 2.2 Rizikové body napadení

- **Autentizace mezi UE a jádrem sítě**

V sítích 5G je ochrana identity uživatele zajištěna pomocí Subscription Concealed Identifier (SUCI), který nahrazuje trvale identifikující Subscription Permanent Identifier (SUPI). SUCI je generován zařízením uživatele (UE) pomocí asymetrické kryptografie, konkrétně schématu Elliptic Curve Integrated Encryption Scheme (ECIES), využívajícího veřejný klíč domácí sítě. Tento mechanismus zajišťuje, že skutečná identita uživatele není odhalena během počátečního připojení k síti, čímž se chrání proti odposlouchávacím útokům typu IMSI catcher. Ochrana identity uživatele a jeho dat je součástí autentizačních protokolů 5G-AKA a EAP-AKA a specifikována v rámci 3GPP TS 33.501.

- **Transportní šifrování**

Přenos dat mezi základnovými stanicemi (gNB) a jádrem sítě (5GC) probíhá přes nezabezpečené transportní sítě, což vyžaduje implementaci bezpečnostních opatření pro zajištění důvěrnosti a integrity dat.

Specifikace 3GPP 33.501 doporučuje použití protokolů jako IPsec (šifrovací algoritmus chránící přenos dat mezi zařízeními šifrováním jednotlivých IP paketů a současným ověřováním zdroje těchto dat) nebo TLS (protokol využívající šifrování veřejného klíče, ověřování pravosti informace a odhalování nedovolených manipulací s daty) pro zabezpečení těchto spojení. Tyto protokoly poskytují šifrování a ochranu integrity dat, čímž chrání před odposlechem a neoprávněnými zásahy.

- **Řídící kanály**

Řídicí kanály v 5G, které přenášejí data mezi UE a sítí, jsou chráněny pomocí standardních šifrovacích algoritmů 128-NEA1/2/3 a integritních algoritmů 128-NIA1/2/3. Díky těmto algoritmům je zabráněno odposlouchávání a modifikace dat během přenosu.

- **Softwarově definované prvky**

V rámci 5G jsou využívány nové technologie virtualizující služby dříve zajišťované hardwarem. Mezi tyto služby patří:

1) Virtualizace síťových funkcí (NFV)

Tato technologie umožňuje oddělit komunikační služby od vyhrazeného hardwaru, jako jsou routery a firewally. Toto oddělení znamená, že síťový provoz může poskytovat nové služby dynamicky a bez instalace nového hardwaru. Nasazení síťových komponentů s virtualizací síťových funkcí trvá zlomek času nasazování tradičních sítí. Virtualizované služby také mohou běžet na levnějších generických serverech namísto proprietárního hardwaru.

2) Softwarově definované sítě (SDN)

je přístup k síti, který využívá softwarové ovladače nebo rozhraní pro programování aplikací (API) ke komunikaci se základní hardwarovou infrastrukturou a k řízení provozu v síti. Tento model se liší od tradičních sítí, které k řízení síťového provozu používají vyhrazená hardwarová zařízení. SDN může vytvářet a řídit virtuální síť, nebo ovládat tradiční hardware prostřednictvím softwaru.

Zatímco virtualizace sítí umožňuje segmentovat různé virtuální sítě v rámci jedné fyzické sítě nebo propojit zařízení v různých fyzických sítích a vytvořit tak jedinou virtuální síť, softwarově definované sítě umožňují nový způsob řízení směrování datových paketů prostřednictvím centralizovaného serveru.

Tyto technologie zvyšují flexibilitu a efektivitu sítě, ale zároveň zvyšují riziko napadnutí virtualizovaných síťových služeb zneužitím zranitelnosti softwarových komponentů, nebo neoprávněným přístupem k síťovým funkcím.

# 3 Kryptografie

## 3.1 Úvod do kryptografie

Šifrování informací je jedním ze základních předpokladů v digitálním prostředí, jelikož zabezpečuje přenos informací a dat a zamezuje zneužití těchto materiálů. Zabezpečení dat vychází ze dvou základních šifrovacích metod, symetrického a asymetrického šifrování klíče.

#### 3.1.1.1 Symetrické šifrování

V rámci symetrického šifrování je pro odesílanou zprávu využíván stejný klíč pro šifrování i dešifrování, což tomuto způsobu zabezpečení přináší několik výhod, jako je například rychlost zpracování zprávy vzhledem k jednomu šifrovacímu klíči (oproti asymetrické metodě), efektivitu ve využití výpočetní síly a energie potřebné k zašifrování a odšifrování zprávy a kompatibilitu s velkou řadou systému a zařízení, což znamená velmi snadnou integraci do stávajících a fungujících aplikací a systému bez nutnosti zásadních úprav. Naproti tomu právě jednoduchost jednoho klíče tohoto modelu představuje bezpečnostní riziko v situacích, kdy se tento klíč dostane do špatných rukou, tato metoda je tak v tomto ohledu zranitelnější v oblasti distribuce klíčů než asymetrická metoda.

Mezi nejvyužívanější algoritmy symetrického šifrování patří:

- AES (Advanced Encryption Standard)
- 3DES (Triple Data Encryption Standard) – starší standard, dnes nahrazován AES
- Blowfish

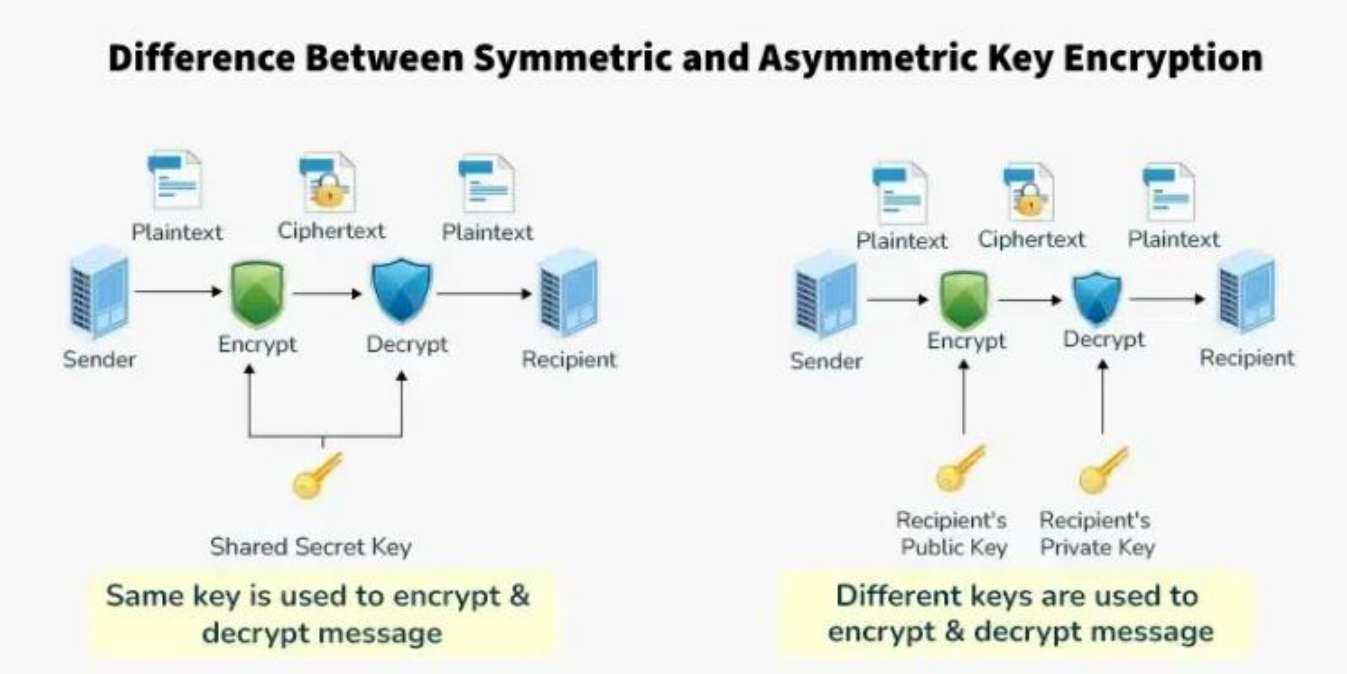
#### 3.1.1.2 Asymetrické šifrování

Na rozdíl od předchozí, symetrické, metody šifrování je v tomto případě využíván jeden ‚veřejný' klíč pro zašifrování zprávy, který je veřejně dostupný všem uživatelům sítě k zašifrování dat, a další ‚soukromý' klíč pro dešifrování zprávy, který je unikátní pro každého uživatele. Tento soukromý klíč lze také využít k digitálním podpisům a ověření autenticity. Výhodou tohoto principu je vyšší zabezpečení informací, zejména díky tomu, že není třeba předem sdílet tajný klíč (oproti symetrickému šifrování). Kdokoli může zašifrovat data pro příjemce pomocí svého veřejného klíče, ale pouze příjemce je může dešifrovat pomocí svého soukromého klíče.

Mezi nejvyužívanější algoritmy asymetrického šifrování patří:

- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptic Curve Cryptography) – silnější zabezpečení s menšími klíči, ideální např. pro IoT zařízení
- DSA (Digital Signature Algorithm)

*Obrázek 10: Rozdíl mezi symetrickým a asymetrickým šifrováním klíče*




## 3.2 Postkvantová kryptografie (PQC)

Postkvantová kryptografie představuje oblast kryptografie, která se zabývá vývojem a implementací algoritmů odolných proti kvantovým útokům bez nutnosti použití nových hardwarových komponent. Tyto algoritmy jsou navrženy tak, aby byly bezpečné jak vůči klasickým, tak kvantovým počítačům a jejich integrace do existujících sítí vyžaduje minimální změny v dosavadní infrastruktuře. Důvodem pro nasazení PQC je schopnost kvantových počítačů řešit matematické problémy, které jsou základem současných asymetrických kryptografických systémů (např. RSA nebo ECC) mnohem efektivněji než klasické počítače. Zejména Shorův algoritmus umožňuje faktorizovat velká čísla nebo řešit problémy diskrétních logaritmů, na kterých jsou tyto klasické metody založeny.

K odolnosti kryptografických systémů vůči novým hrozbám využívají PQC algoritmy matematické problémy, které jsou považovány za obtížně řešitelné i za pomocí kvantových algoritmů. Hlavní třídy algoritmů zahrnují kryptografii:

- Lattice-based (mřížky)
- Code-based (kódy)
- Hash-based (hashovací funkce)
- Multivariate (multivariační polynomy)

V roce 2024 představil NIST nové standardy[33], které vynikají svou kompaktností klíčů a efektivitou operací, což je činí vhodnými pro integraci do současných komunikačních systémů. Mezi tyto klíče patří:

- **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism)[34]: postkvantový kryptografický mechanismus pro zapouzdření klíče (KEM), který umožňuje dvěma stranám bezpečně vytvořit sdílený tajný klíč přes veřejný kanál a vychází z algoritmu CRYSTALS-Dilithium. Jeho bezpečnost je založena na matematickém problému Module Learning with Errors a aktuálně se předpokládá, že odolá i útokům kvantových počítačů; standard definuje tři úrovně zabezpečení: ML-KEM-512, -768 a–1024.

[33] https://csrc.nist.gov/projects/post-quantum-cryptography

[34] https://csrc.nist.gov/pubs/fips/203/final

- **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm)[35]: slouží k ověření integrity dat a identity podepisující osoby, přičemž umožňují i tzv. nezpochybnitelnost, tedy nemožnost pozdějšího popření podpisu. Standard ML-DSA definuje algoritmus CRYSTALS-KYBER pro generování a ověřování digitálních podpisů, které jsou považovány za bezpečné i vůči útokům kvantových počítačů.

- **SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm)[36]: standard definuje bezstavový algoritmus digitálního podpisu založený na hashi, jehož cílem je ověřit integritu dat a identitu podepisujícího, a zároveň zajistit nezpochybnitelnost podpisu. SLH-DSA vychází z algoritmu SPHINCS+, který byl vybrán k standardizaci v rámci procesu NIST pro postkvantovou kryptografii.

V březnu 2025 byl navíc vybrán ke standardizaci algoritmus **HQC** (Hybridní kódové šifrování) pro rozšíření portfolia postkvantových KEM šifer[37].

### 3.2.1 Výhody PQC

- **Kompatibilita a snadné nasazení**: Na rozdíl od QKD nevyžaduje žádné nové fyzikální kanály či zařízení. Lze ji implementovat jako softwarovou aktualizaci do stávajících systémů, což usnadňuje její nasazení. V přechodném období lze navíc PQC kombinovat s tradičními kryptografickými protokoly, což umožňuje postupný přechod na kvantově odolné systémy bez narušení stávajících operací. Tento hybridní přístup by tak měl zajistit kontinuitu a bezpečnost během období migrace.
- **Širší záběr kryptografických funkcí**: PQC nabízí nejen náhradu za výměnu klíčů, ale rovněž za digitální podpisy a další asymetrické funkce. To je důležité pro 5G sítě, jež využívají kryptografii v celé řadě služeb od autentizace uživatelů po zabezpečení aplikačních rozhraní. PQC algoritmy umožňují vytvářet kvantově odolné digitální podpisy, které mohou nahradit stávající ECDSA podpisy (algoritmus asymetrické kryptografie) v protokolech a certifikátech 5G jádra. Naproti tomu QKD řeší pouze distribuci symetrických klíčů.

### 3.2.2 Nevýhody PQC

- **Velikost klíčů a jejich vliv na výkon**: PQC zpravidla vyžadují větší velikost klíčů v porovnání s tradičními veřejnými klíči. To by mohlo mít vliv na delší čas potřebný k šifrování a dešifrování klíčů. Dalšími potenciálními úskalími jsou větší požadavky na úložiště, zvýšené používání paměti a požadavky na šířku pásma. V menším měřítku by tyto překážky mohly být bez povšimnutí, nicméně problém představuje potřeba užití klíčů ve velkých objemech. Zároveň mohou vznikat problémy u výkonu starších zařízení, které by mohly brzdit nasazení této kryptografie.
- **Nedostatečná prověřenost a riziko budoucích útoků**: Přestože algoritmy od NIST prošly intenzivním testováním v rámci standardizačního procesu, jejich dlouhodobá odolnost vůči dosud neznámým útokům není zaručena. Historie ukazuje, že i dobře prověřené algoritmy mohou být prolomeny pomocí běžného počítače. Příkladem může být výše zmíněný algoritmus SIDH, který je zranitelný vůči efficient key recovery attack[38]. I v rámci závěrečného kola výběrového řízení NIST došlo k prolomení několika algoritmů pomocí klasického počítače[39].

## 3.3 Využitelnost kvantové distribuce klíčů (QKD)

Principy a stav vývoje kvantové distribuce klíčů coby metody kvantové kryptografie, která využívá princip kvantové mechaniky k bezpečnému sdílení tajných klíčů mezi dvěma stranami, kdy nelze změřit kvantový stav bez jeho ovlivnění, byly představeny v kapitole 1.5.1. V praxi tato metoda funguje tak, že jedna strana vysílá jednotlivé fotony ve specifických kvantových stavech, které reprezentují bity informace. Druhá strana posléze tyto fotony měří. Pokud se někdo pokusí odposlouchávat přenos, kvantové vlastnosti fotonů se změní, což způsobí detekovatelné chyby v komunikaci. Tato schopnost detekce odposlechu je klíčovým prvkem bezpečnosti QKD.

[35] https://csrc.nist.gov/pubs/fips/204/final

[36] https://csrc.nist.gov/pubs/fips/205/final

[37] https://csrc.nist.gov/pubs/ir/8545/final

[38] https://eprint.iacr.org/2022/975.pdf

[39] https://www.cryptomathic.com/blog/nist-pqc-finalists-update-its-over-for-the-rainbow

Smyslem použití QKD je možnost kombinovat standardní a kvantové technologie – bezpečně distribuovat šifrovací klíč mezi dvěma stranami pomocí kvantových jevů, přičemž samotná šifrovaná komunikace pak probíhá po klasických (legacy) komunikačních systémech. Samotný kvantový klíč je distribuován speciálním kvantovým kanálem, avšak také prostřednictvím standardně dostupných technologií.

### 3.3.1 Výhody QKD

- **Detekce odposlechu**: Jakýkoliv pokus o odposlech je detekovatelný díky kvantovým vlastnostem přenášených částic, tzn že když dojde k nárůstu chybovosti v přenesených kvantových bitech. Komunikující strany provádějí statistickou kontrolu chyb a odchylek v části sdíleného klíče, a pokud zjistí překročení prahové hodnoty chyb, kvantový kanál je považován za kompromitovaný a klíč se nepoužije.
- **Jasně definovaná bezpečnost:** Na rozdíl od algoritmů asymetrické kryptografie, které jsou založeny na matematických problémech a předpokladu, že neexistuje jejich efektivní řešení na klasickém ani kvantovém počítači (tento předpoklad už se u mnoha algoritmů ukázal jako chybný, u některých i se zpožděním desítek let), je bezpečnost QKD založena na velmi transparentních a přímočarých zákonech kvantové fyziky.
- **Dlouhodobá bezpečnost**: Na rozdíl od klasických metod, které mohou být v budoucnu prolomeny kvantovými počítači, QKD poskytuje bezpečnost založenou na fyzikálních principech. Komunikační sítě, které jsou zabezpečeny jen pomoci matematických operací mohou podléhat Harvest Now Decrypt Later útokům (viz dále).
- **Integrace do existující infrastruktury**: Nedávné experimenty ukazují, že QKD může být implementováno pomocí stávajících optických i satelitních sítí, což snižuje náklady a zvyšuje předpokládanou dostupnost technologie.

### 3.3.2 Nevýhody QKD

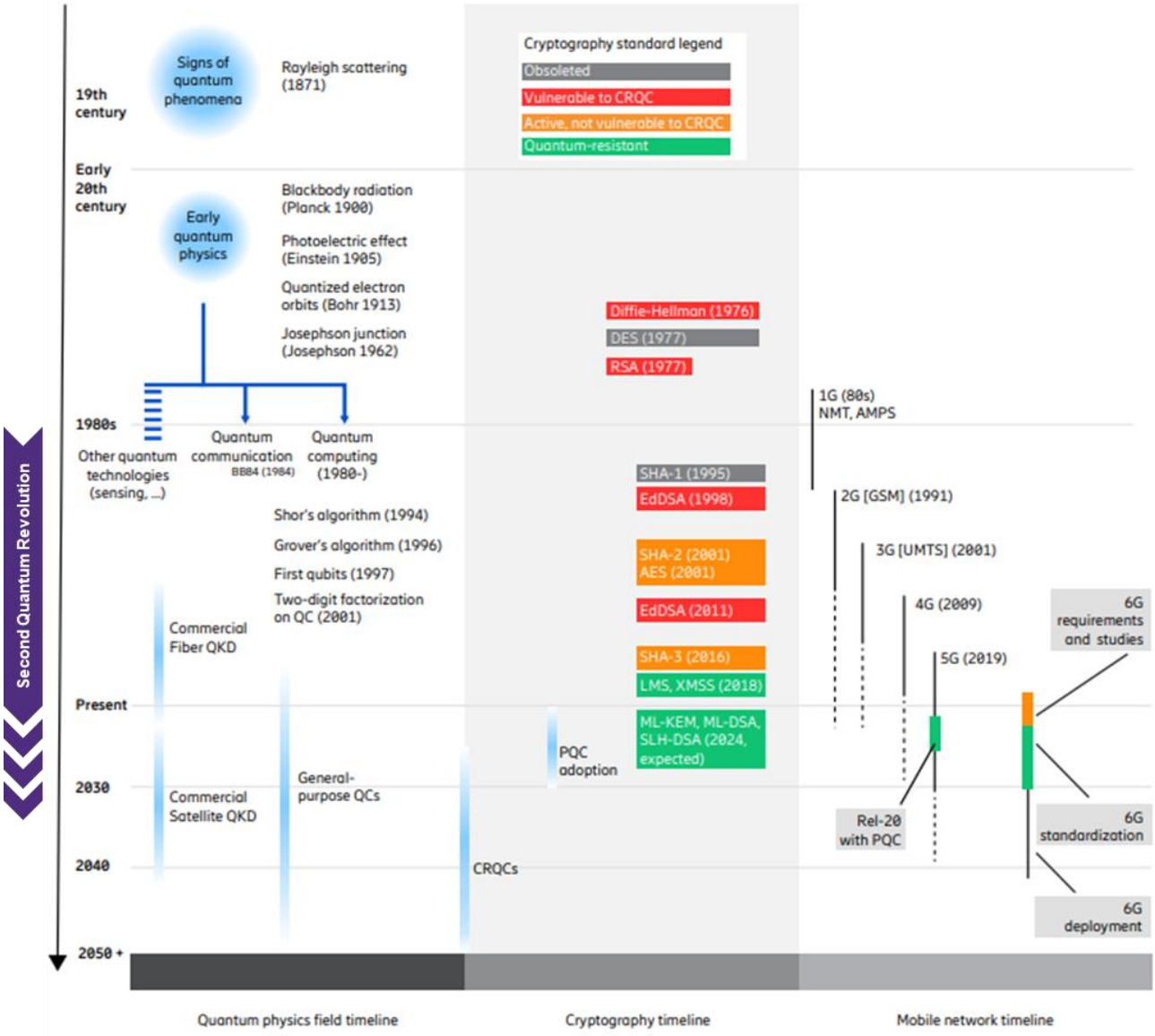
- **Omezený dosah**: Extrémní citlivost kvantové komunikace na šum limituje v současné době maximální délku jednoho kvantového spoje na na zhruba 170 km u komerčních systémů. Kvůli tomu je nutné vybudovat fyzickou infrastrukturu anebo prodloužit tuto vzdálenost pomocí kvantových opakovačů, které jsou stále ve vývoji, nebo pomocí speciálně umístěných uzlů, které ale zase zvyšují potenciální rizika (QKD systémy lze v tomto “trusted” uzlu napadnout). V prostředí 5G sítí toto znamená, že QKD je zatím využitelná jen pro páteřní a metropolitní propojení (např. mezi ústřednami, datovými centry, základnovými stanicemi a jádrem sítě), kde lze natáhnout dedikovaná vlákna. Nelze ji použít přímo k mobilnímu uživateli.
- **Vysoká nákladovost**: QKD systémy vyžadují specializovaná zařízení, přesné optické komponenty, kryogenní chlazení detektorů pro potlačení šumu apod. Tato zařízení jsou zatím drahá a jejich instalace a údržba je náročná. Kromě samotných kvantových vysílačů je nutná i klasická doprovodná infrastruktura (pro servisní spojení, synchronizaci, management), která zvyšuje komplexitu. Ericsson přímo uvádí, že QKD vyžaduje specializovaný hardware, vysokou údržbu a je spojen s vysokými náklady, což činí jeho širší nasazení nepraktickým.
- **Potřeba autentizace**[40]: QKD sama o sobě nezajišťuje autentizaci komunikujících stran, což vyžaduje kombinaci s klasickými kryptografickými metodami. kvantový kanál vyžaduje důvěryhodný klasický autentizovaný kanál (např. pomocí předem sdíleného tajemství nebo klasického digitálního podpisu) k zamezení man-in-the-middle útoku. Tuto pupeční šňůru do klasické kryptografie je nutné bránit pomocí algoritmů, které jsou opět potenciálně zranitelné kvantovým výpočtem. Například britské Národní centrum kybernetické bezpečnosti (NCSC) varuje před spoléháním se výhradně na QKD a zdůrazňuje, že pro kritickou infrastrukturu je vhodnější nasazení standardizované PQC.

[40] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

# 4 Historie vývoje

Účelem následující grafiky je společně zobrazit historii vývoje jednotlivých technologií, jimž se tato studie věnuje, tedy kvantové fyziky, resp. QC, kryptografie a technologie mobilních sítí a zasadit zejm. uvedené kryptografické standardizační aktivity do časového rámce oproti vývoji QC a vývoji v mobilních technologiích.

*Obrázek 10: Historie technologického vývoje ve kvantové fyzice, kryptografii a mobilních sítích*



# 5 Hrozby kvantového computingu pro 5G

Kvantový počítač dostatečné síly, označovaný též jako CRQC (schopný prolomit současné šifry), by měl zásadní dopad na bezpečnostní prvky 5G sítí. Hrozby lze rozdělit na dvě hlavní kategorie: (1) Prolomení asymetrické kryptografie, která zajišťuje autentizace a výměnu klíčů, a (2) oslabení symetrické kryptografie používané pro šifrování dat. Doplňkově lze uvažovat i nové typy útoků, které kvantové technologie umožní (např. Side-channel attacks, QMITM, HNDL).

## 5.1 Prolomení asymetrické kryptografie

Jakmile bude k dispozici kvantový počítač schopný spustit Shorův algoritmus pro klíče běžných délek (např. 2048bit RSA nebo silnější 256bit ECC), veškeré bezpečnostní protokoly 5G využívající tyto algoritmy se stanou zranitelnými. Útočník s CRQC by mohl v reálném čase odposlouchávat a dešifrovat komunikaci, která je dnes považována za zabezpečenou. V kontextu 5G to znamená, že takový útočník by mohl zlomit důvěrnost i integritu kanálů zabezpečených DTLS/IPsec uvnitř jádra nebo mezi sítěmi. Například šifrované spojení mezi jádrem operátora a základnovou stanicí by mohlo být kompromitováno, pokud útočník rozloží použité RSA/ECDH a získá šifrovací klíče. Dále by mohl falšovat digitální podpisy a potenciálně se vydávat za legitimní síťové prvky. To by vedlo k tomu, že přestane platit autentizační infrastruktura: útočník by mohl vystupovat jako „man-in-the-middle“ mezi uživatelem a sítí, aniž by to stávající mechanismy detekovaly, protože by dokázal napodobit platné certifikáty či podpisy. Taková situace by mohla ohrozit nejen soukromí uživatelů (odposlech hovorů, získání citlivých dat), ale i bezpečnost kritických služeb (manipulace s příkazy v průmyslových aplikacích využívajících 5G, narušení IoT senzorů atd.).

## 5.2 Dopady na symetrickou kryptografii

I když Groverův algoritmus nepředstavuje tak akutní a totální hrozbu jako Shorův, nelze jeho efekt opomíjet. V prostředí 5G by potenciální útočník mohl urychlit hrubou sílu proti šifrovaným zprávám nebo autentizačním kódům. Například pokud by používaná šifra měla jen 128bitový klíč, kvantový útok jej efektivně zmenší na 64 bitů, což by za určitých okolností mohlo umožnit prolomení (pokud by útočník disponoval extrémním výpočetním výkonem a časem). Obecně se má za to, že 128bitové symetrické algoritmy zatím poskytují dostatečnou bezpečnostní rezervu i vůči kvantovým útokům, avšak u systémů s požadavkem na dlouhodobou bezpečnost (horizont 20 let a více) již řada odborníků doporučuje přejít na 256bitové klíče jako standard. V rámci 5G tedy do budoucna zřejmě dojde k posílení symetrických komponent, např. postupné nahrazení algoritmu 128-EEA3 (ZUC se 128b klíčem) variantou 256-EEA4 s 256b klíčem, jakmile bude standardizována[41]. Již v Rel-17 rozšířilo 3GPP podporu algoritmů na 192bitové klíče v některých případech a 256bitové klíče jsou jen dalším logickým krokem k posílení zabezpečení. Tím by se vliv Groverova algoritmu eliminoval (256bitový klíč by Grover zmenšil na efektivních ~128 bitů, což je stále považováno za bezpečné)[42].

Další aspekt symetrické kryptografie je délka a bezpečnost hashovacích funkcí a MAC. Kvantové útoky mohou urychlit i hledání kolizí hashů (např. pomocí Groverova algoritmu modifikovaného na problém nalezení předpisu). To by mohlo teoreticky ovlivnit integritní kódy v 5G, které využívají hash (např. HMAC-SHA256). Očekává se však, že přechod na delší hash (SHA-384/512) či využití tzv. kvantově odolných hashů (např. založených na větší výstupní entropii) by byl dostatečným opatřením. V současných 5G specifikacích se již s SHA-256/384 počítá, takže i zde je určitá rezerva[43].

[41] https://www.3gpp.org/ftp/tsg_SA/WG3_Security/TSGS3_94AH_Kista/SA_83/33841-g10.docx

[42] https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_115_Athens/SA_103/33246-j00.doc

[43] https://atis.org/?download_id=1961732&sdm_process_download=1

## 5.3 Quantum decryption

V rámci tzv. kvantových dešifrovacích útoků využívají útočníci schopnosti budoucích výkonných kvantových počítačů (CRQC) k prolomení současných šifrovacích metod. Tento proces nemusí být okamžitý a může vyžadovat určitý čas, během něhož útočníci zachycují šifrovanou komunikaci. Jakmile kvantový počítač data úspěšně dešifruje, útočník získá přístup k citlivým informacím, aniž by komunikující strany o tomto narušení věděly.

Příkladem takového útoku na infrastrukturu sítí 5G může být situace, kdy je komunikace mezi mobilními zařízeními a síťovými uzly zabezpečena systémy založených na veřejném klíči (PKI), například pomocí systémů RSA či ECC (kryptografie využívající eliptických křivek). Útočník disponující kvantovým počítačem s implementací Shorova algoritmu zachytí šifrované zprávy proudící v rámci této komunikace. Kvantový počítač následně dokáže rychle prolomit použitý veřejný klíč, čímž získá klíče používané pro šifrování dat.

V okamžiku, kdy útočník tyto klíče získá, je schopen dešifrovat nejen zachycenou komunikaci, ale také všechny další zprávy, minulé, současné i budoucí, které byly či budou zašifrovány pomocí příslušného veřejného klíče. To může vést k rozsáhlým únikům dat, odhalení citlivých osobních informací, důvěrných obchodních dat nebo dokonce kritických informací týkajících se národní bezpečnosti. Tyto útoky tedy představují závažnou bezpečnostní hrozbu, kterou musí organizace v rámci přípravy na příchod kvantových technologií brát velmi vážně.

### 5.3.1 “Harvest now, decrypt later” (HNDL)

Útočníci při tomto typu útoku zachycují a ukládají dnes šifrovaně přenášená data s cílem je rozšifrovat, jakmile budou mít k dispozici dostatečně výkonný kvantový počítač (tzv. CRQC). To představuje značné riziko pro data, která mají zůstat důvěrná po dlouhou dobu.

To lze ilustrovat na příkladu infrastruktury mobilních sítí 5G. Útočník může strategicky zachytávat šifrovanou komunikaci mezi uživateli a základnovými stanicemi nebo mezi jednotlivými prvky sítě. Taková citlivá data (jako např. vládní nebo firemní tajemství), jsou dnes typicky šifrována pomocí moderních standardů, jako je Advanced Encryption Standard (AES-128) nebo Elliptic Curve Integrated Encryption Schemes (ECIES), které jsou vůči klasickým počítačovým útokům považovány za bezpečné. Útočníci se však tato data nesnaží okamžitě dešifrovat. Místo toho je bezpečně uloží a čekají na příchod dostatečně výkonných kvantových počítačů, které by dokázaly prolomit současné šifrování například pomocí Shorova algoritmu (pro veřejné klíče) nebo Groverova algoritmu (pro symetrické klíče). Tato strategie umožňuje obejít dnešní bezpečnostní opatření a činí z HNDL útoku vysoce nebezpečnou hrozbu pro dlouhodobou důvěrnost dat v sítích 5G.

Před několika lety se všeobecně předpokládalo, že Groverův algoritmus vyžaduje zdvojnásobení délky symetrických klíčů, tedy použití AES-256 místo AES-128, aby byla zajištěna stejná úroveň bezpečnosti proti kvantovému útoku. Podle současného stanoviska Národního institutu pro standardy a technologie (NIST) však Groverův algoritmus nepředstavuje bezprostřední hrozbu pro AES-128. Přesto platí, že odolnost AES-128 výrazně závisí na kvalitě entropie použité při generování klíčů. Nízká kvalita entropie může šifru AES-128 učinit zranitelnou nejen vůči budoucím kvantovým, ale i současným klasickým útokům, jak uvádí studie ATIS „Důsledky entropie na odolnost symetrického šifrování vůči kvantovým útokům“.

Vzhledem k charakteru HNDL útoků mohou zachycená citlivá šifrovaná data zůstat ohrožená po mnoho desetiletí. V této souvislosti vyvstává zásadní otázka: Jak dlouho zůstane AES-128 dostatečně bezpečný tváří v tvář rychle se vyvíjejícím kvantovým technologiím? Přestože současná stanoviska NIST poskytují krátkodobou jistotu, organizace by měly aktivně zvažovat strategie pro zajištění dlouhodobé bezpečnosti. Jednou z možností je včasný přechod na robustnější algoritmy, jako je AES-256 nebo jiné kvantově odolné šifrovací metody. Tento proaktivní přístup pomůže ochránit citlivou komunikaci před aktuálními i budoucími hrozbami v dynamicky se vyvíjejícím kyberbezpečnostním prostředí.

### 5.3.2 Quantum-Impersonation Attack

Kvantové personifikační útoky (Quantum Impersonation Attacks) představují typ kybernetické hrozby, při níž útočník rovněž využívá schopnosti kvantových počítačů k prolomení kryptografických systémů založených na veřejném klíči (PKI). Podstatou takového útoku je vydávání se za jinou osobu nebo entitu prostřednictvím odcizení digitální identity. To znamená, že útočník může využít prolomených klíčů pro digitální podpisy k podepisování dokumentů, rozesílání falešných zpráv či provádění transakcí, které se tváří, jako by pocházely od legitimních uživatelů. Tento druh útoku tedy nespočívá jen v možnosti dešifrovat komunikaci, ale také umožňuje rozsáhlé podvody a falšování identity.

Toho lze využít v infrastrukturách, kde se PKI používá například při autentizaci mezi jednotlivými síťovými operátory. K autentizaci často dochází při propojování sítí různých provozovatelů, například v různých geografických oblastech či oddělených administrativních doménách. PKI je zde využito k ověření identity a zajištění toho, že obě strany komunikují s důvěryhodnými

protějšky pomocí digitálních certifikátů. Pokud však dojde k prolomení PKI kvantovým útokem, může útočník získat přístup k operačním a konfiguračním údajům přenášeným mezi operátory, a tím získat citlivé informace o struktuře sítě, včetně lokalizace klíčových síťových prvků, jako jsou gNB (5G základnové stanice), UPF (User Plane Function) nebo AMF (Access and Mobility Management Function). Tyto znalosti může následně využít k plánování cílených útoků, například k vyřazení důležitých síťových uzlů pomocí útoků typu „odmítnutí služby“ (DoS) nebo k obcházení zabezpečení díky pochopení cest datových toků v síti.

### 5.3.3 Quantum Man-in-the-Middle (QMITM)

Kvantový Man-in-the-Middle (QMITM) útok je pokročilá forma klasického útoku typu Man-in-the-Middle, při kterém útočník využívá schopností kvantových počítačů (CRQC) k zachycení a úpravě komunikace mezi dvěma stranami v reálném čase. Podstatou útoku je, že útočník zachytí šifrovanou zprávu, okamžitě ji dešifruje, modifikuje její obsah, znovu zašifruje a předá dál, přičemž žádná z komunikujících stran nepozná, že ke změně došlo. Tímto způsobem je přímo ohrožena nejen důvěrnost, ale zejména integrita a autenticita komunikace.

Představme si typickou situaci, kdy útočník využívající kvantový počítač s pokročilými metodami (např. Shorův algoritmus) zachytí komunikaci v rámci 5G sítě. Díky schopnosti efektivně faktorizovat klíče nebo počítat diskrétní logaritmy získá původní šifrovací nebo podpisové klíče, aniž by si toho uživatel či server všimli. Útočník může poté snadno upravit obsah zprávy, například změnit částku nebo cílový účet u finanční transakce, a zprávu znovu zašifrovanou předat adresátovi. Obě komunikující strany přitom věří, že spolu bezpečně komunikují, takže zásah útočníka zůstává zcela bez povšimnutí.

Na rozdíl od kvantového dešifrovacího útoku, který se zaměřuje primárně na prolomení důvěrnosti dat a nezasahuje do jejich obsahu v průběhu přenosu, QMITM útok umožňuje přímou, nepozorovanou manipulaci se zprávami v reálném čase. Tato schopnost představuje významný posun v hrozbách spojených s nástupem kvantových výpočetních technologií a vyžaduje zcela nová bezpečnostní opatření.

### 5.3.4 Side-Channel Attacks

Útoky přes postranní kanály (side-channels) představují specifický typ bezpečnostní hrozby, která se netýká přímo použití kvantových počítačů, ale přesto významně ohrožuje současnou i postkvantovou kryptografii (PQC). Principem tohoto útoku je využití nepřímých informací, které zařízení mimoděk poskytuje během své činnosti (časové odezvy, spotřeby energie, elektromagnetického vyzařování nebo odchylek určitých parametrů). Pomocí detailní analýzy těchto údajů lze odvodit informace o používaných šifrovacích klíčích, aniž by útočník přímo prolomil šifru samotnou. Protože postkvantové kryptografické protokoly zatím neprošly rozsáhlým testováním v reálném nasazení, mohou být vůči takovým útokům ještě zranitelnější.

Cílem postranního útoku může být například chytrý telefon nebo zařízení internetu věcí (IoT). Ačkoli tato zařízení běžně využívají kryptografické metody k zabezpečení komunikace, jejich běžný provoz současně generuje celou řadu vedlejších fyzikálních signálů, jako jsou drobné odchylky ve spotřebě elektrické energie nebo elektromagnetické záření, které mohou útočníci analyzovat. V budoucnu by dokonce mohly existovat specializované kvantové algoritmy, které by efektivněji detekovaly a interpretovaly tyto sotva postřehnutelné změny, a tím ještě více usnadnily útoky přes postranní kanály. Takové možnosti představují výzvu pro vývoj bezpečných kryptografických řešení, která by byla odolná nejen vůči kvantovým, ale i těmto nepřímým hrozbám.

### 5.3.5 Efficient Key Recovery Attacks

Tento typ útoku se ukázal jako efektivní způsob prolomení kryptografického protokolu SIDH (Singular Isogeny Diffie-Hellman), který byl dříve jedním z kandidátů pro zajištění zabezpečené postkvantové kryptografie. Hlavní podstata tohoto typu útoku spočívá v umožnění efektivní rekonstrukce soukromého klíče v SIDH. konkrétně ve variantě SIKEp434 (Supersingular Isogeny Key Encapsulation), metodě kódování klíčů v SIDH, která dříve odpovídala bezpečnostní úrovni 1 dle NIST. Útok proběhl na běžném procesoru za přibližně 10 minut. Ještě rychlejší průniky byly možné u variant SIKEp182 a SIKEp217 (za 55 a 85 sekund). Tyto výsledky naznačují, že všechny odvozené varianty protokolu SIDH jsou potenciálně ohroženy při použití v moderní kryptografii. Vzhledem k této hrozbě a úspěšnému prolomení SIDH/SIKE nebyl tento protokol zařazen mezi standardy postkvantové kryptografie dle NIST[44]. Nejedná se tedy přímo o útok s pomocí prostředků quantum computingu, ale spíše o ilustraci rizika, jemuž čelí a budou čelit snahy o PQC ochranu před typy útoků, které byly zmíněné výše.

[44] https://eprint.iacr.org/2022/975.pdf

# 5.4 Posílení odolnosti kryptografie vůči kvantovým útokům

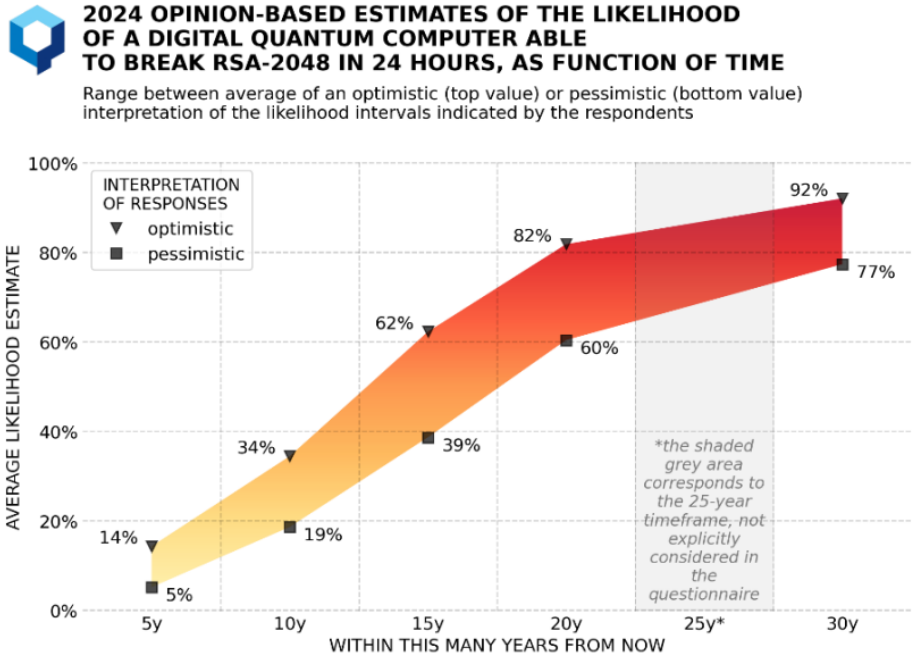
Z výše popsaných rizik, zejména HNDL, kdy s výrazným zlevněním úložných kapacit se již nyní některá data ukládají k dešifrování později, jednoznačně plyne doporučení se již dnes bránit pomocí známých postupů proti budoucím útokům. V této souvislosti lze použít v odborné komunitě běžně akceptovanou nerovnost, která říká, že společnost by měla zahájit přechod na quantum-ready technologie dříve, než je součet času potřebný na přípravu (migrační čas) a času jenž je vyžadován na uchovávání tajemství.

Kromě využití postkvantové kryptografie (u asymetrické kryptografie) a zdvojnásobení velikosti klíče v protokolech (u symetrické) lze s dostupnými technologiemi využít koncept dvojího šifrování, kdy je jedna zpráva postupně šifrována jednou prekvantovou a jednou postkvantovou šifrou. Získají se tak výhody obou přístupů. V případě prekvantové šifry jde o ověřenou zkušenost s jejím používáním, spojenou s často mnohaletými pokusy o její prolomení. V případě postkvantové šifry pak jde o výhody spojené s očekávanou odolností vůči kvantové kryptografii.

Jako další posílení lze využít generování klíčů pomocí QKD a použít i tento klíč pro dodatečné šifrování, tedy použít trojí šifrování – prekvantovou šifrou, postkvantovou šifrou a šifrou s klíčem získaným pomocí kvantově mechanických jevů, QKD. Poslední krok ale vyžaduje, aby oba komunikační uzly měly spojení pomocí kvantových technologií (zatím nejčastěji po optických kabelech) a jednalo by se tudíž o technologicky náročnější přípravu.

Global Risk Institute[45] (GRI) každoročně vytváří dotazník mezi experty na kvantové technologie, ve kterém zjišťuje odhady pro vývoj QC do budoucnosti. Pro rok 2024 je dostupný report „Quantum Threat Timeline Report 2024“[46] ve kterém se mj. odhaduje pravděpodobnost, kdy vznikne kvantový počítač, který bude schopen prolomit RSA-2048 klíč během 24 hodin (tzv. Q-Day). Z těchto údajů lze odvodit, že nyní odhadovaná doba, kdy dojde k prolomení současných šifrovacích algoritmů kvantovým počítačem se pohybuje okolo 15 až 20 let, přičemž míra rizika se zhruba zdvojnásobuje každých 5 let. Tyto odhady je třeba vzít v úvahu při plánování migrace na quantum-ready technologie a vytváření příslušného harmonogramu /roadmapy ze strany příslušných státních institucí a regulátorů.

*Obrázek 11: Graf - Quantum Threat Timeline Report 2024*




[45] https://globalriskinstitute.org/

[46] https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

# 6 Regulace a standardizace

## 6.1 Mezinárodní iniciativy

Úspěšné zvládnutí přechodu na kvantově odolné zabezpečení telekomunikačních sítí vyžaduje koordinaci na mezinárodní úrovni i na úrovni národních regulací. Na mezinárodní úrovni hrají klíčovou roli především standardizační organizace NIST, ETSI a ITU-T, ale i 3GPP:

### 6.1.1 NIST (Národní institut pro standardy a technologie USA)

Vede již zmíněný proces standardizace postkvantové kryptografie. V červenci 2022 oznámil výběr algoritmů a roku 2024 zveřejnil návrhy federálních standardů FIPS pro postkvantovou výměnu klíčů a podpisy. NIST také vydává doporučení, do kdy by mělo dojít k přechodu. Například v květnu 2022 Bílý dům vydal Národní bezpečnostní memorandum 10, které stanovuje politiky pro kvantovou odolnost: federální agentury musí inventarizovat své kryptografické systémy a plánovat migraci na PQC s cílem zmírnit co nejvíce kvantových rizik do roku 2035. Toto datum reflektuje očekávání, kdy by mohl být k dispozici CRQC. USA tedy oficiálně plánují být připraveny nejpozději v polovině 30. let. NIST úzce spolupracuje s IETF (Internet Engineering Task Force) na začlenění PQC do protokolů, a s průmyslem na testování implementací. Americká NSA vydala též nové pokyny (Suite 3) pro národní bezpečnostní systémy, jež počítají s nasazením schválených PQC algoritmů co nejdříve po jejich standardizaci.

### 6.1.2 ETSI (Evropský institut pro telekomunikační normy)

V Evropě zastřešuje standardizaci kvantově bezpečné komunikace zejména technická komise CYBER a pracovní skupina QSC (Quantum-Safe Cryptography) a samostatná ISG (Industry Specification Group) pro QKD. ETSI QSC se zabývá praktickou implementací PQC: vydává technické zprávy o výkonnosti a vhodnosti PQC pro různé aplikace, o kombinaci klasických a postkvantových algoritmů do hybridních schémat, o dopadech kvantových útoků na symetrické algoritmy apod. V roce 2024 QSC dokončil například zprávu TS 104 016 o rámci migrace na kvantově bezpečné algoritmy a inventář protokolů vyžadujících úpravy. Paralelně ISG-QKD v ETSI stanovuje společná rozhraní a požadavky pro kvantové distribuční sítě tak, aby různé QKD systémy byly interoperabilní a bezpečné. Například definuje standardy pro QRNG (kvantové generátory náhodných čísel) tím způsobem, jak mají vypadat bezpečnostní důkazy QKD systémů, a pro integraci QKD do síťových architektur (standard ETSI TS 104 014 řešící interoperabilitu systémů). ETSI tím podporuje rozvoj evropského ekosystému kvantových komunikací a zajišťuje, že nové technologie bude možné zapojit do existující infrastruktury. Evropa také skrze organizace CEN/CENELEC koordinuje standardizační mapu pro kvantové technologie obecně. V roce 2025 vydalo ETSI standard TS 104 015[47] pro bezpečnou a efektivní hybridní výměnu klíčů kombinující klasické a postkvantové šifry (tzv. schéma Covercrypt), který umožňuje plynulý přechod k postkvantové ochraně dat, na což navazují další zpřesňující standardizační aktivity.

### 6.1.3 ITU-T (Mezinárodní telekomunikační unie, sektor standardizace)

ITU zavedla studijní skupiny zaměřené na bezpečnost kvantových sítí. Např. studijní skupina ITU-T SG13 vydává řadu doporučení Y.3800 pro architekturu QKD sítí a studijní skupina SG17 zaměřená na bezpečnost vydala rámec X.1710 pro zabezpečení QKD sítí. ITU tedy vytváří globální rámec pro kvantové klíčové sítě, aby různé implementace (z Evropy, Číny, USA atd.) mohly spolupracovat. To je důležité, neboť existuje reálné riziko roztříštěnosti standardů s ohledem na různé přístupy např. Číny nebo USA. ITU se snaží v této oblasti zprostředkovat konsenzus, např. vydáváním roadmap dokumentů a přehledů technických řešení.

### 6.1.4 GSMA

Kromě těchto standardizačních orgánů existují také průmyslová sdružení přímo pro telekomunikační sektor. Například GSMA (sdružení mobilních operátorů) založila Post Quantum Telco Network Task Force, která sdílí osvědčené postupy mezi operátory

[47] https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption#:~:text=Today%2C%20ETSI%20announces%20the%20launch,sensitive%20data%20to%20decrypt%20them

a vytváří jednotná doporučení pro migraci telekomunikačních sítí na PQC. Již dříve 3GPP analyzovalo dopady kvantových dopadů, kdy především studie 3GPP TR 33.841 z roku 2019 zkoumala podporu delších 256bitových klíčů v 5G jako možnou okamžitou reakci na kvantovou hrozbu. V únoru 2025 vydala 5G Americas (regionální sdružení v Americe) podrobný white paper s doporučeními, jako je provést inventuru všech kryptografických systémů v sítích, spolupracovat s dodavateli na kvantové migraci a zavádět kryptografickou agilitu do infrastruktury. Tato doporučení jsou relevantní i globálně.

# 7 Kvantové aktivity EU a ČR

Evropská unie od roku 2018 realizuje ambiciózní iniciativu Quantum Flagship[48], která má celkový rozpočet jedné miliardy eur rozložený na desetileté období. Tento program podporuje rozvoj čtyř klíčových oblastí kvantových technologií: kvantové výpočetní technologie, kvantová komunikace, kvantové metrologie a senzoriky a kvantové simulace. K tomu je nutno připočítat další miliardy eur zahrnuté v národních programech členských států Evropy, například Německa, Holandska, Dánska, Finska, ale i Polska, Maďarska a států Balkánu.

## 7.1 Kvantové výpočetní technologie EU a jejich náklady

Odhad ceny kvantových počítačů je velmi problematický, dostupné údaje jsou minimální a mohou být zavádějící. Nejpokročilejší hráči (Google, IBM, Microsoft, Rigetti, …) prodej kvantového počítače nenabízejí a v současné době s ním ani nepočítají. Jimi vyvinuté počítače jsou umístěny v rámci firemních superpočítačových center a zpřístupněny prostřednictvím cloudových výpočetních řešení formou pronájmu strojového času.

Ceny strojového času na kvantových počítačích lze potom stanovit pouze orientačně, rozsáhlejší smlouvy poptávající větší množství strojového času jsou důvěrného charakteru, chráněny prostřednictvím dohod o mlčenlivosti. Pronájem strojového času je však také nepřesný termín, neboť výpočetní operace představuje celý projekt: pronájem samotného strojového času na kvantovém počítači a služby odborníků obsluhujících toto zařízení. Zadavatel specifikuje zadání úlohy, tým (pronajatých) odborníků provede převod úlohy do formy kvantového algoritmu, provede optimalizaci pro konkrétní kvantové zařízení, provede výpočet (zadá operace do systému a provede měření) a interpretuje výsledky.

Omezený odhad možné ceny kvantových počítačů poskytuje několik nákupů kvantových počítačů v rámci EuroHPC Joint Undertaking (JU), které jsou blíže popsány níže. Tyto údaje mají ale omezenou vypovídací hodnotu, jelikož je nelze vnímat jako komerční nákupy, ale spíše jako smlouvy o vědecké spolupráci, v rámci kterých výrobci kvantových počítačů vytvoří, dodají a sestaví kvantový počítač v HPC centru. Takováto dodávka má mimo jiné velkou prestižní složku pro výrobce kvantového počítače. O prodeji kvantového počítače mimo EuroHPC program tito dodavatelé nesdílejí žádné informace a nejeví ochotu k rozkrytí cenové politiky.

V EU bylo vybráno šest lokalit pro umístění kvantových počítačů, které budou provozovat kvantové počítače v rámci projektu EuroHPC Joint Undertaking. Celkový rámec investice překračuje 100 milionů eur, přičemž polovinu hradí Evropská komise a druhou polovinu jednotlivé členské státy či konsorcia. Každé z kvantových zařízení má být integrováno do existující superpočítačové infrastruktury a cílem je vytvořit evropský hybridní ekosystém schopný provozovat kvantově-klasické výpočty. Jedním z cílů celé aktivity bylo nasazení a následné otestování různorodých kvantových technologických platforem, od iontových pastí přes supravodivé qubity až po fotonické technologie.

Česká republika se zapojila do evropského kvantového vývoje prostřednictvím projektu LUMI-Q, který bude realizován v Ostravě v Národním superpočítačovém centru IT4Innovations. Kvantový počítač VLQ49 se 24 qubity od IQM Quantum Computers zde bude napojen na stávající superpočítač Karolina. Celková výše investice činí přibližně 5 milionů eur, přičemž polovina prostředků pochází z evropského rozpočtu (EuroHPC JU) a druhou polovinu hradí konsorcium 9 členských států.

Polsko v rámci EuroHPC JU pořizuje 20 qubitový kvantový počítač Piast-Q[50] za 12,3 mil. EUR od společnosti AQT. Dále prostřednictvím společnosti Creotech Instruments realizuje projekt na vývoj kvantového počítače schopného škálování až na 1000 qubitů do roku 2029[51]. První fáze projektu, která cílí na vývoj systému se 100 qubity, je plně financována z evropského programu Quantum Flagship a má rozpočet v rozmezí 18 až 20 milionů eur. Projekt zahrnuje vývoj hardwaru, řízení kvantových operací a integraci s klasickými výpočetními systémy.

[48] https://qt.eu/about-quantum-flagship/

[49] https://www.it4i.cz/en/infrastructure/vlq-quantum-computer

[50] https://www.datacenterdynamics.com/en/news/aqt-to-deliver-rack-based-piast-q-quantum-computer-to-psnc/

[51] https://creotech.pl/news/creotech-instruments-has-signed-an-executive-agreement-with-the-european-commission/

Německo patří mezi hlavní evropské lídry v oblasti kvantových technologií. V roce 2020 ohlásila spolková vláda plán přímé veřejné investice ve výši 2 miliard eur zaměřený na vytvoření kvantového ekosystému, podporu výzkumu i průmyslových aplikací. Z těchto prostředků bylo financováno několik vlajkových projektů. Například kvantový počítač Euro-Q-Exa[52], který vzniká v rámci EuroHPC JU a je vyvíjen společností IQM ve spolupráci s LRZ a Fraunhofer-Gesellschaft, získal přímé financování ve výši 25 mil. EUR. Jedná se o dva systémy, kde jeden systém bude pracovat s 54 a druhý se 150 qubity. V roce 2024 otevřela společnost IBM v Ehningenu u Stuttgartu první evropské Quantum Data Center, určené k provozu komerčních kvantových počítačů na evropské půdě. Do výstavby a provozu centra investovala IBM a její partneři zhruba 290 mil. eur.

Španělsko v rámci strategie Quantum Spain představilo v roce 2025 první kvantový počítač ve Španělsku, vyvinutý výhradně s využitím evropských technologií, který je integrován do superpočítače MareNostrum 5[53]. Tento počítač je výsledkem spolupráce mezi startupem Qilimanjaro Quantum Tech a skupinou GMV. V rámci projektu EuroHPC JU podepsalo na začátku roku 2025 smlouvu na projekt MareNostrum-Ona, kvantového počítače, který bude rovněž umístěn v BSC-CNS. Tento projekt, s celkovým rozpočtem 8,5 milionu EUR, bude prvním evropským kvantovým žíhacím počítačem (quantum annealing computer), který se bude dát využít zejména při řešení optimalizačních problémů a má za cíl doplnit stávající kvantové technologie dostupné evropským výzkumníkům.

Francie v rámci projektu EuroHPC JU očekává 12 qubitový kvantový počítač Lucy[54] od firem Quandela a attocube v závěru roku 2025[55]. Celkový rozpočet na tento projekt je 8,5 mil EUR.

Odhad nákladů QC lze rovněž odvodit z dostupných dat ze spolupráce mezi již zmíněným Finským výrobcem kvantových počítačů IQM a VTT Technical Research Centre of Finland. V rámci spolupráce byly vybudovány tři kvantové počítače (5 qubitů, 20 qubitů a 50 qubitů), které jsou poskytovány i pro komerční využití; rozpočet přes 20 mil. eur pro tyto počítače byl poskytnut finskou vládou. Do roku 2027 je plánováno mít k dispozici 300 qubitů s cílem posílit výzkum v oblasti modelování materiálů. VTT pro tento účel získalo speciální vládní grant ve výši 70 mil. EUR. IQM nabízí kvantový výpočetní čas na svých zařízeních přes svůj produkt IQM Resonance ve formě pay-as-you-go přístupu za 0,30 USD za sekundu, což sice poskytuje určitou představu o ceně této formy využití kvantových počítačů, ale ta je zjevně závislá na typu/náročnosti požadované úlohy.

## 7.2 Kvantové aktivity ČR

Na evropské úrovni je vytvoření infrastruktury pro kvantově zabezpečenou komunikaci pod záštitou projektu EuroQCI[56]. V první fázi se jedná o vytvoření testovací národní kvantové infrastruktury. V případě České republiky toto zajišťuje projekt CZQCI[57], obdobné projekty jsou realizovány i v ostatních evropských zemích. V navazující fázi by pak tyto národní infrastruktury měly být propojeny mezi sebou. Technologicky se jedná převážně o propojení na optické bázi pomocí optických vláken a satelitní komunikace.

Samotný projekt CZQCI je zaměřen na vybudování testovací verze národní páteřní kvantové komunikační infrastruktury, která propojí Prahu, Brno a Ostravu. Cílem je ověřit technologie pro kvantově zabezpečenou komunikaci a připravit Českou republiku na integraci do evropské infrastruktury EuroQCI plánované do roku 2030. Součástí projektu jsou vzdělávací programy pro širokou veřejnost i odborníky, možnost testování kvantové komunikace pro partnery z veřejné správy i průmyslu a specializovaná laboratoř pro výzkum a výuku.

[52] https://eurohpc-ju.europa.eu/signature-procurement-contract-eurohpc-quantum-computer-located-germany-2024-10-15_en

[53] https://quantumspain-project.es/en/quantum-spain-presents-the-first-quantum-computer-in-spain-developed-with-100-european-technology/

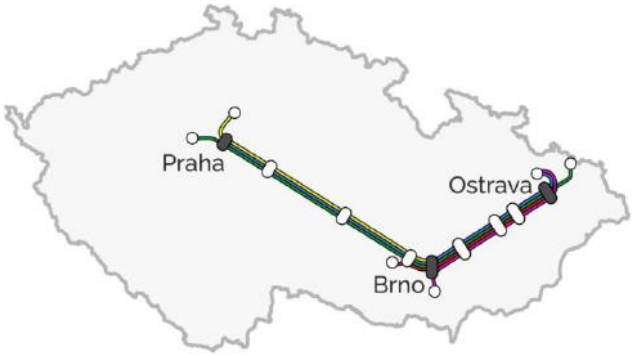
[54] https://www.quandela.com/qpus/lucy/

[55] https://quantumzeitgeist.com/european-researchers-gain-remote-access-to-cutting-edge-12-qubit-quantum-computer-via-euroqcs-france-initiative/

[56] https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci

[57] https://www.cybersecurityhub.cz/strategicke-projekty/czqci

*Obrázek 12: Vizualizace testovací kvantové infrastruktury v ČR*




Prostřednictvím projektu CZQCI získají čeští partneři zkušenosti s nasazením a provozem kvantové sítě, což jim umožní lépe posoudit možnosti jejího využití v praxi, zejména v oblastech kyberbezpečnosti a telekomunikací. Projekt také podpoří mezinárodní spolupráci a výměnu zkušeností v rámci evropského prostoru, a zároveň rozšíří povědomí o kvantových technologiích mezi odbornou i laickou veřejností.

Projekt CZQCI je koordinován CyberSecurity Hub, z.ú. a je řešen konsorciem, které se skládá z:

- Českého vysokého učení technického v Praze,
- CESNET z.s.p.o.,
- Masarykovy univerzity,
- Ústavu přístrojové techniky Akademie věd České republiky,
- Univerzity Palackého v Olomouci,
- VŠB – Technické univerzity Ostrava,
- Vysokého učení technického v Brně.

V ČR existuje již od roku 2016 Národní iniciativa pro kvantové technologie (NIKT[58]), která byla založena v souvislosti s iniciativou EU Quantum Flagship. Cílem této iniciativy je propagace a podpora rozvoje kvantových technologií. Jejími členy jsou Matematicko-fyzikální fakulta Univerzity Karlovy, Přírodovědecká fakulta Univerzity Palackého v Olomouci, Fakulta jaderného a fyzikálního inženýrství Českého vysokého učení technického v Praze, Fakulta informatiky Masarykovy univerzity, Ústav přístrojové techniky Akademie věd, Středoevropský technologický institut Masarykovy univerzity a Cybersecurity Hub z.ú.

V oblasti kvantových výpočtů se chystá spuštění 24 qubitového kvantového počítače v národním superpočítačovém centru IT4Innovations při VŠB-Technické Univerzitě Ostrava (viz předchozí kapitola).

ČR se zapojila také do projektu evropské kvantové komunikační infrastruktury EuroQCI prostřednictvím projektu CZQCI (viz předchozí kapitola). Tento projekt je koordinován CyberSecrurity Hub, z.ú, který v současnosti připravuje i konzultační službu v oblasti kvantových technologií.

Mezi české instituce, které poskytují reálný přístup ke kvantovým technologiím, patří:

- ČVUT: lze využít spolupráce mezi IBM a ČVUT, díky níž je možné získat procesorový čas na kvantovém počítači, kde ČVUT také koordinuje alokaci procesorového času. Dále poskytuje laboratoř se zařízeními pro kvantové generování klíče (QKD) a organizuje setkání vývojářů a vzdělávání v oblasti kvantových technologií již od středoškolského věku[59]. ČVUT také spolupracuje s výzkumnými i komerčními partnery na evropském projektu fotonického kvantového počítače (Epique), který je financován EU.IT4Innovations při VŠB Ostrava bude zprostředkovávat přístup ke kvantovému počítači LUMI-Q.
- Projekt CZQCI poskytuje vzdělávací kurzy v oblasti kvantových komunikačních technologií a pro veřejné institice i komerční sféru umožňuje fyzické připojení pro testování připravenosti pro kvantovou komunikaci.

[58] https://nikt.cz/

[59] https://qworld.net/

- Ústav přístrojové techniky Akademie věd ČR (ÚPT AV ČR) se podílí na řadě výzkumných projektů v rámci konsorcií, například vlastní vývoj kvantových iontových hodin a realizaci a rozšiřování sítě koherentních přenosových tras pro distribuci přesného času odvozeného z těchto hodin.
- Projekt QEENTEC[60] koordinovaný ÚPT AV ČR řešený Ústavem fotoniky a elektroniky, Ústavem fyzikální chemie Jaroslava Heyrovského, Palackého univerzitou v Olomouci a CESNETem je zaměřen na vývoj hybridních kvantových hradel pro kvantové počítače.
- Projekt QM4ST[61] vedený ZČU v Plzni a sdružující UK, ČVUT a VUT se zaměřuje na studium materiálů vykazujících zcela nové vlastnosti vysvětlitelné kvantovou fyzikou, např. spintroniku, supravodivost, fotokatalýzu, elektrolýzu, palivové články a fotoniku.

V současnosti se připravuje národní kvantová strategie, která by měla poskytnout strategický rámec státní podpory vzdělávání a průmyslu v kvantových technologiích.

[60] https://www.jh-inst.cas.cz/grant/quantum-engineering-and-nanotechnology-queentec

[61] https://qm4st.zcu.cz/cs/

# 8 Závěr

Kvantové technologie představují zásadní změnu v oblasti výpočetní techniky, komunikace a bezpečnosti. Nasazení kvantových počítačů umožní řešit složité vědecké problémy a praktické simulace, ale současně přinese i bezpečnostní riziko pro současné postupy šifrování. Příklady oblastí, na něž bude mít rozvoj QC bezpochyby dopad jsou navrhování materiálů se specifickými vlastnostmi, baterií, chemických sloučenin, léků, logistika, učení neuronových sítí - AI, kryptografie a bezpečnost komunikačních sítí obecně.

Vývoj je rychlý, ale praktické použití kvantových počítačů a kvantové komunikace v běžném provozu vyžaduje překonání technologických a infrastrukturních bariér. Jde zatím o velmi ranou fázi využívání QC, veškerá dostupná zařízení jsou dosud experimentální, a i když některá mohou nabízet komerční přístup, jde o velmi složitý a nákladný proces. Investice do výzkumu QC tak vedle největších světových hráčů vynakládají samotné státy jednotlivě, nebo společně – v EU jde o iniciativu Quantum Flagship a konkrétní projekty výstavby kvantových počítačů EuroHPC Joint Undertaking a EuroQCI. Česká republika je do evropského vývoje aktivně zapojena ve formě výzkumných kapacit i financování.

Jelikož kvantové počítače dokáží efektivně řešit specifické dílčí úlohy, které jsou pro standardní systémy neřešitelné v představitelném čase, nejschůdněji se aktuálně jeví kombinované použití standardních výpočetních systémů společně s kvantovými. V praxi si složité úlohy řešené klasickými výpočetními systémy budou moci vyvolat v cloudu specifickou podúlohu, řešenou kvantovým počítačem.

Kvantové počítače budou v dohledné době způsobilé prolomit současné kryptografické protokoly (zejména RSA, ECC), které jsou využívány v 5G sítích pro autentizaci a výměnu klíčů a narušit tak celkovou bezpečnost digitální komunikace. Pro zajištění bezpečnosti v éře kvantových počítačů je proto nutné kombinovat postkvantovou kryptografii, kvantovou distribuci klíčů a modernizaci komunikační infrastruktury. Tyto kroky k ochraně dat je třeba podniknout dostatečně brzo, aby předcházely vývoj samotného QC, neboť již dnes existují hrozby, které se projeví později, jakmile budou kvantové počítače dostupné pro potenciální útočníky. K tomu je na mezinárodní úrovni určena standardizace nových šifrovacích algoritmů (NIST, ETSI), ale bude třeba přijmout i další kroky na národní úrovni.

Investice do postkvantové kryptografie, aktivní podpora standardizace a budování kapacit v oblasti kvantové bezpečnosti jsou klíčové kroky, které by měly podniknout jak veřejné instituce, tak soukromý sektor.

Nad rámec nového zákona o kybernetické bezpečnosti (nZKB-NIS2 ve schvalovacím procesu) lze doporučit následující kroky, které by ze strany státních institucí a regulátorů pomohly zajistit přechod ke kvantově bezpečné infrastruktuře:

a) Formulovat minimální (závazná) metodická pravidla pro operátory pro zajištění kybernetické bezpečnosti 5G a ostatních komunikačních sítí v souvislosti s nástupem quantum computingu, které by zahrnovaly:
    - Termín a způsob (roadmapu) zavedení pokročilých šifrovacích standardů (PQC nebo kombinovaných), připravených na budoucí kvantové dešifrování, včetně kroků vícefázové migrace.
    - Minimální technické nároky na auditní /detekční /monitorovací systémy
    - Jednotný postup pro bezpečnostní audit dodavatelů systémů
    - Pravidla pro ochranu interních dat a (bezpečnostní) nároky na personál

b) Vytvořit referenční rejstřík PQC kompatibilních zařízení

c) Stanovit minimální nároky na interoperabilitu mezi klasickou a QKD kryptografií