

# Kvantové technologie

Technologie založené na poznatcích kvantové fyziky jsou již dnes běžnou součástí našeho života. Příkladem mohou být polovodičové součástky, lasery, jaderná energetika, nukleární magnetická rezonance a mnoho dalších aplikací. Výzkum v posledních desetiletích přinesl velké množství nových kvantových technologií, které jsou přímo založeny na kontraintuitivních kvantových principech a jevech. Jejich budoucí využití zahrnuje oblasti elektronické bezpečnosti, komunikace a výpočtů, medicíny, geofyziky, navigace, chemie a biochemie, farmakologie, satelitní technologie, či materiálové vědy.

Kvantové technologie otevírají zcela nový prostor. Jsou klíčové pro to, aby si Evropa i v budoucnu udržela nejen konkurenceschopný průmysl, ale i vojenskou a civilní bezpečnost. Příkladem komerčně dostupných kvantových technologií jsou zařízení pro kvantovou distribuci kryptografických klíčů umožňující absolutně bezpečnou komunikaci. Budoucí uplatnění těchto technologií zahrnuje kvantové počítače (umožňují řešit problémy neřešitelné na současných počítačích), plně kvantovou komunikaci (plně kvantové distribuované výpočty a cloudy), simulace kvantových systémů (s uplatněním v chemii, farmakologii nebo materiálových vědách, např. návrh energeticky efektivních zařízení), senzorů pro měření gravitace (geologický průzkum, detekce tektonických poruch a zemětřesení), 3D akcelerace a gyroskopů (přesná inerciální navigace – nejen pro armádní využití), velmi přesné měření času (navigace GPS a Galileo, obchodování na burzách) a magnetického a elektrického pole (lékařství).

V současné době hraje Evropa významnou roli ve vývoji kvantových technologiích, zaostává ale za hlavními světovými hráči, jako jsou USA, Japonsko, Čína nebo Kanada. Tuto pozici Evropy potvrzuje počet patentů v kvantových technologiích, kde Evropa zaostává za ostatními, a obsazuje shodně 4. místo například v kvantové distribuci klíče nebo v oblasti kvantových počítačů. Tento trend je viditelný obzvláště v oblasti průmyslu, kde vedou především mimoevropské firmy – MagiQ, DWave, Microsoft, IBM, Northrop Grumman, Toshiba, NEC, HP, Mitsubishi, a skupina čínských kvantových startupů v provincii Anhui. IBM dala veřejně k dispozici pro cloudové výpočty svůj kvantový počítač (IBM quantum experience).

V posledních letech je znatelný razantní nástup Číny v oblasti kvantových technologií. Kvantová komunikace je jedním z hlavních cílů 13té pětiletky. V roce 2016 bude dokončena páteřní kvantová síť pro absolutně bezpečnou komunikaci v délce 2000 km spojující klíčové vládní a vojenské instituce v Pekingu, Jinanu, Hefei a Shanghaji. V srpnu 2016 Čína vypustila první experimentální kvantový satelit, který má pomáhat při výzkumu satelitní kvantové komunikace a kvantové komunikace ve vesmíru, např. pro plánované napojení města Urumqi na páteřní kvantovou síť.

Rozvinuté Evropské země již po řadu let masivně podporují kvantový výzkum (především Německo), některé pak silně navyšují podporu kvantových technologií, aby se mohly v blízké budoucnosti podílet na celosvětovém trhu kvantových technologií. Příkladem jsou Velká Británie (270 mil. liber na 5 let na vytvoření tzv. kvantových hubů – velkých výzkumných center), Nizozemí (výzkumné centrum QuTech s počáteční investicí 135 mil. EUR).

Evropská unie si uvědomuje význam kvantových technologií a rozhodla se jejich rozvoj podpořit vytvořením výzkumného flagshipu v hodnotě jedné miliardy EUR na 10 let, se zaměřením především na podporu spolupráce výzkumných institucí a průmyslu. Objevují se také požadavky na zavedení specializovaných kvantových studijních programů (kvantový inženýr) v rámci EU pro přípravu zaměstnanců firem zabývajících se kvantovými technologiemi.

Nejdůležitějšími představiteli kvantových technologií jsou:

**Kvantová kryptografie.** Zahrnuje algoritmy a protokoly umožňující absolutně bezpečnou komunikaci, ale také distribuované kvantové výpočty a zabezpečení současných kryptosystémů proti budoucím kvantovým útokům (zprávy zašifrované stávajícími kryptosystémy se dají uložit a v budoucnu dešifrovat pomocí kvantových kryptosystémů). Systémy pro absolutně bezpečnou komunikaci jsou komerčně dostupné již nyní.

**Univerzální kvantové počítače.** Umožňují zmenšení procesorů na kvantovou úroveň. Dokáží efektivně řešit problémy, které jsou na klasických počítačích neřešitelné (např. rozklad velkých čísel na prvočinitele). Kvantový počítač představuje hrozbu pro většinu v současnosti používaných šifrovacích algoritmů. Realizace prakticky použitelného zařízení však bude vyžadovat ještě hodně úsilí.

**Kvantové simulátory.** Jde v podstatě o jednoúčelové kvantové počítače, které dokáží simulovat složité fyzikální systémy, jejichž modelování běžné počítače nezvládají. Využití mají pro vývoj nových materiálů nebo při zkoumání složitých chemických reakcí, ve farmacii a podobně.

**Kvantové senzory.** Využití částicové interference, kvantových superpozic a provázaných kvantových stavů umožňuje dosáhnout vysoké přesnosti a citlivosti. Například atomové interferometry mohou fungovat jako extrémně přesné akcelerometry a gyroskopy. S jejich pomocí je např. možné odhalit podzemní prostory pouhým měřením gravitačního zrychlení. Hodí se i pro pokročilé vědecké experimenty a samozřejmě pro inerciální navigační systémy. Senzory extrémně slabých magnetických polí, které pracují se spiny jednotlivých elektronů v barevných centrech v nanodiamantu, se hodí např. pro přesnou NMR spektroskopii.

**Kvantové měření času.** Nejmodernější časové a frekvenční standardy, které využívají buď jednotlivých iontů, nebo systému více iontů zachycených v optické mřížce, dosahují relativní přesnosti lepší než  $10^{-17}$ . Přesné měření času je důležité pro navigační systémy, řízení elektroenergetických sítí, vědecký výzkum, automatizované finanční transakce.

**Kvantové zobrazování.** Zobrazovací metody využívající světlo s vysokým časovým rozlišením a detekci jednotlivých fotonů mohou umožnit např. vidění za překážky nebo pod vodní hladinu.

Čím mohou přispět a jaké odborné zkušenosti mají české výzkumné týmy:

**Kvantová komunikace a kryptografie:** Již v roce 1998 byl v Olomouci realizován plně funkční prototyp zařízení pro kvantový přenos kryptografického klíče. Od té doby se rozvíjí teoretický a experimentální výzkum v oblasti kvantových komunikací a jejich informačních protokolů v rámci široké mezinárodní spolupráce a také spolupráce s předním českým provozovatelem nejmodernějších fotonických sítí CESNET. V současnosti se zkoumá i propojení kvantových hradel, senzorů nebo i celých počítačů pomocí kvantové komunikace. V ČR existuje mnoho zkušeností s konstrukcí zdrojů neklasických stavů světla, zejména zdrojů provázaných fotonů, jenž jsou základem optických kvantových technologií. V Brně již více než 10 let probíhá výzkum protokolů pro kvantovou kryptografii a kryptoanalýzu, zejména analýzu kvantové distribuce klíče a šifrování kvantové informace, dále také kvantové generování náhodných čísel pro kryptografické účely.

**Kvantová komunikace:** V Brně probíhá výzkum kvantové komunikace, zejména z hlediska teorie informace – kapacity kvantových komunikačních kanálů.

**Kvantové standardy a sensorika:** V nedávné době se v Brně spojeným úsilím s Olomoucí podařilo zrealizovat náročné zařízení pro zachycení a laserové chlazení iontů. Jeho uplatnění je v současnosti pro vysoce přesné měření času a distribuci ultrapřesné frekvence a pro testování principů kvantových mechanických sensorů a simulátorů kvantových motorů. Také nanomechanické a nanoelektrické kvantové sensory, převodníky a simulátory jsou rozvíjeny v Brně a Olomouci spojeným úsilím ve spolupráci s řadou zahraničních týmů. Týmy v Praze a Brně se také věnují rozvoji velmi perspektivních pevnolátkových kvantových platforem pro sensoriku.

**Optické simulátory a kvantové počítání:** Dlouholeté a rozsáhlé teoretické a experimentální zkušenosti existují v Olomouci a Praze v oblasti optických kvantových bran a vývoje algoritmů s jednotlivými fotony pro kvantové počítání. Tento výzkum probíhá v dlouhodobé mezinárodní spolupráci. V současnosti se pozornost soustřeďuje také na zkoumání nových problémů efektivní kontroly práce a tepla v kvantovém počítání. V Brně je rozvinutý teoretický výzkum informačních algoritmů pro kvantové počítání a kvantové simulátory.