VĚDA A VÝZKUM

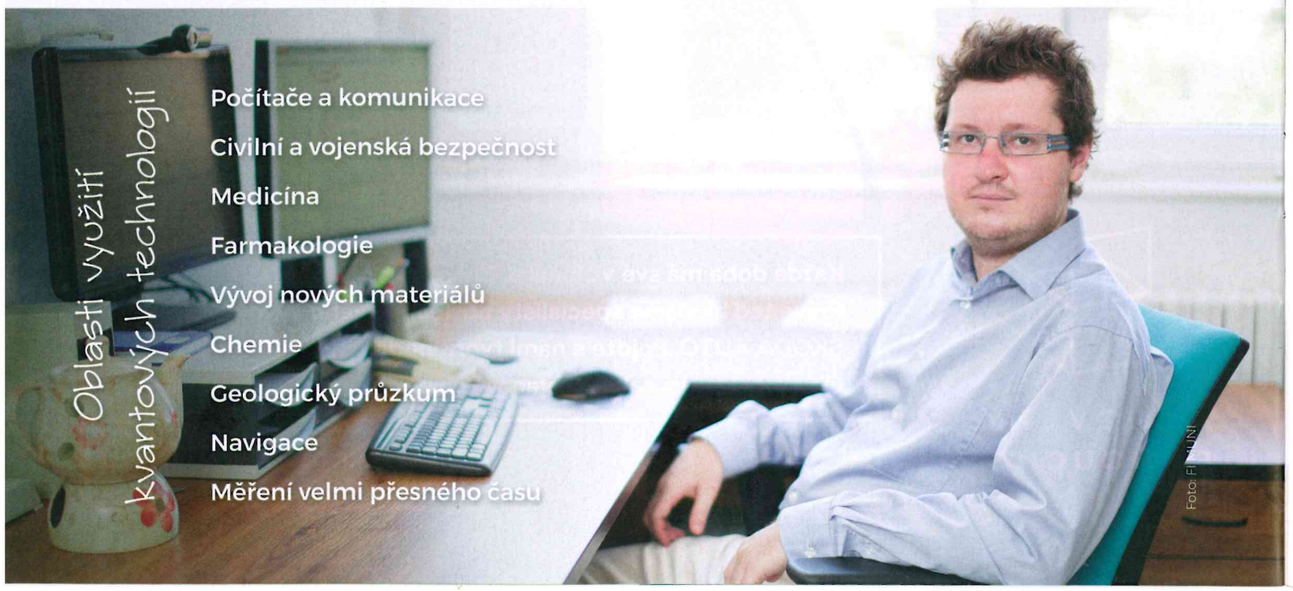
FAKULTA INFORMATIKY MASARYKOVY UNIVERZITY SE ZABÝVÁ VYUŽITÍM KVANTOVÝCH TECHNOLOGIÍ

Autor: Filip Šmejkal

Docent Masarykovy univerzity Jan Bouda je předním českým odborníkem v oblasti kvantové informatiky. Mimo jiné jsme se ptali, zda budou počítačové systémy budoucnosti skutečně bezpečnostně neprolomitelné.

Na Vaší fakultě se kontinuálně zabýváte kvantovými technologiemi. Co si pod tímto pojmem mohou čtenáři představit?
Kvantové technologie jsou velmi širokým pojmem. Jevy kvantové fyziky využíváme v informatice především za účelem zpracování informací. Existují však i čistě fyzikální a technologické aplikace, v budoucnu se uvažuje například o jejich využití v navigacích nebo geologickém průzkumu.

Jak tedy pokračuje výzkum ve Vašem oboru?
Většina projektů s potenciálním využitím se nachází ve velmi rané fázi. Důležitost tohoto výzkumu si však uvědomuje i Evropská komise, která na jejich podporu poskytla grant na podporu vědy a průmyslu ve výši jedné miliardy EUR. V Evropě však prakticky neexistují firmy zabývající se opravdu inovativními technologiemi. Evropské firmy nemají přílišný zájem a ani dostatek prostředků do inovativních technologií investovat. V tomto zaostáváme za Spojenými státy, Kanadou a Japonskem. Čína a Brazílie mají podobný handicap jako Evropa, jsou si ho ale vědomy a kompenzují ho velmi masivní podporou nových technologií. Právě proto Evropu na tomto poli předběhli její konkurenti z Ameriky a Asie. Zahraniční firmy investují do kvantových technologií již 20 let, v poslední době velmi masivně. Čína v srpnu minulého roku vystřelila do vesmíru první kvantový satelit, který provedl test technologie umožňující kvantovou teleportaci ze Země do vesmíru. Tato země také dokončila kvantovou síť o 2000 km, kterou napojila na tento satelit. V takové situaci přichází podpora EU příliš pozdě a v nedostatečném rozsahu.



Jaké mají technologie využití v praxi?
Momentálně známe několik desítek jejich aplikací. Některé z nich se uplatňují už dnes a v blízké budoucnosti se očekává jejich masové rozšíření, u jiných lze budoucí vývoj jen těžko odhadnout. V kryptografii se již komerčně využívá kvantová distribuce klíče, kdy na začátku sdílejí dvě kvantová zařízení relativně velmi malou tajnou informaci v podobě bitového řetězce (podobně jako v běžném počítači). Tuto informaci potom dále zvětšují zasíláním fotonů polarizovaných v několika náhodných přednastavených směrech. Přijímací zařízení provádí testy polarizace příchozích fotonů opět v několika náhodně zvolených přednastavených směrech. Odesílatel následně sdělí, která měření provedl správně. Pokud při dalším testování nezjistí ani jedno zařízení pochybení, z pořadí správných měření se vytvoří oběma zařízením známý klíč. Samotná informace tedy bývá skryta ve stavech těchto kvantových částic. Další, dnes již masivně rozšířená aplikace kvantových technologií, je generování náhodných čísel, kdy využíváme například nepředvídatelnosti odrazu fotonů po jejich vstřelení do krystalové mřížky určitého materiálu. Tato zařízení využívají například banky (pro zabezpečení komunikace) nebo loterijní společnosti.

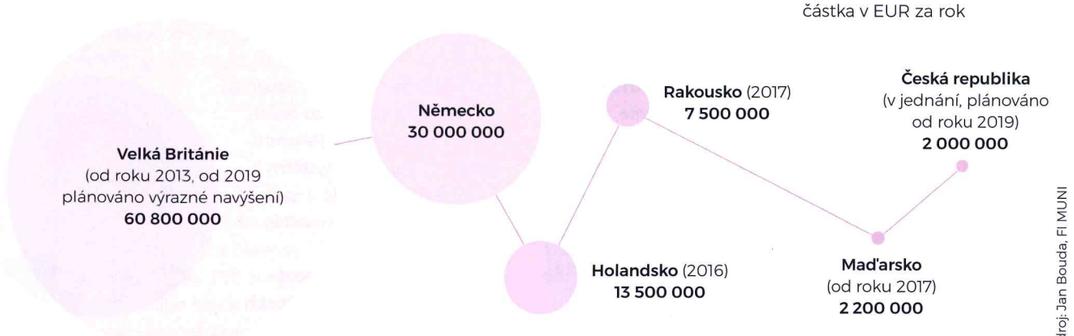
V čem tedy kvantové technologie předčí ty běžné?
Poslední výzkumy v oblasti kvantových technologií ukázaly, že při uplatnění pravidel kvantové fyziky nám k popsání mnoha problémů běžné počítačové technologie fungující na principu nul a jedniček nestačí. Jak jsem již naznačil, v oblasti zpracování informací vynikají svou bezpečností. Dále dokážou urychlit výpočty a pomohou zefektivnit dálkovou komunikaci.

A zjistili jste i nějaké jejich nedostatky?
S užíváním technologií hrozí i jejich zneužití. Pomocí kvantových algoritmů lze například prolomit zabezpečení široce používaného šifrovacího systému RSA. To by mohlo vést ke kolapsu celého internetu. Banky proto kvůli hrozbě budoucího zneužití začínají vylepšovat své zabezpečovací systémy. Technologie naráží také na technická omezení. Přesun dat by se měl ideálně odehrávat přímým optickým kabelem, čehož lze v praxi dosáhnout jen stěží. Toto lze obejít kvantovými routery a repeatery, ty by pak kvůli zachování bezpečnosti musely data teleportovat. Toto řešení je však finančně velmi nákladné.

Jak dlouho tedy potrvá, než se technologie dostanou do běžných firem a domácností?
Nejvyspělejší veřejně známý kvantový počítač disponuje velmi malým procesorem, dosud navíc neexistují ani žádné programovací jazyky vhodné pro kvantové programování. V navigacích by se v budoucnu mohly používat extrémně zmenšené kvantové gyroskopy. Některé firmy také před několika lety testovaly používání technologií k ověření autenticity platebních karet.

SPECIALIZOVANÁ PODPORA VÝZKUMU KVANTOVÝCH TECHNOLOGIÍ V ZEMÍCH EU (VÝBĚR)

částka v EUR za rok



Zdroj: Jan Bouda, FI MUNI

Kde se v Česku uplatněním kvantové fyziky v praxi dále zabývají?
Z pohledu přenosu a zpracování informací pouze náš tým z brněnské Masarykovy univerzity, z fyzikálního hlediska se jimi na vysoké úrovni zabývají například Palackého univerzita v Olomouci, ČVUT v Praze a Fyzikální ústav Akademie věd v Brně.

Táhnou kvantové technologie studenty na Vaši fakultu?
V rámci magisterského studia získají studenti jen základní představu o kvantových technologiích, díky grantům však v Evropě začínají pro kvantové inženýry vznikat různé postgraduální programy. U nás na univerzitě studium kvantové informatiky zaměřujeme především na výzkum.

Zaujala vás problematika kvantových technologií a láká vás její studium? Pro bližší informace se podívejte na **www.fi.muni.cz**