Česko za stovky milionů postaví kvantovou síť

JAN SEDLÁK

První kvantový přenos už se Česku povedl, nyní je na řadě národní a mezinárodní síť.

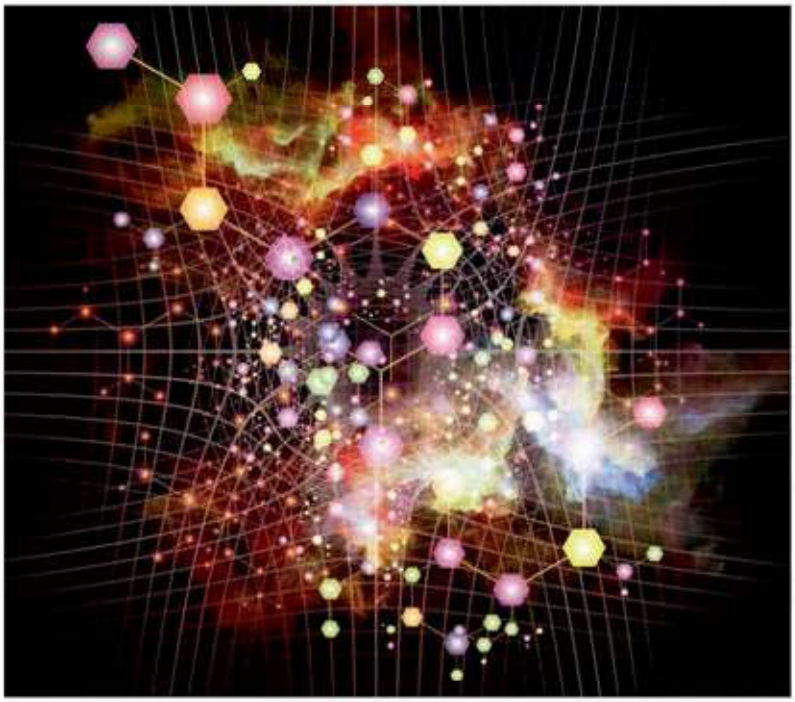
V České republice začaly práce na vybudování kvantové sítě, která propojí vysoké školy, jaderné elektrárny, vybraná ministerstva, důležité nemocnice, Správu železnic a některé další instituce. Síť bude sloužit pro distribuci kvantových klíčů (QKD), jež by měly zajistit velmi bezpečnou komunikaci v rámci kritické infrastruktury.

Teď se rozjíždějí přípravy na testovací národní kvantové sítě. Ty by se následně po roce 2027 měly překlopit do ostré verze a napojit na podobné sítě v dalších evropských zemích, primárně v Německu, Polsku, Rakousku a na Slovensku. Česká republika se totiž stala součástí evropského projektu EuroQCI, za nímž stojí Evropská komise a do kterého se zapojilo 27 států.

Výstavba české kvantové sítě má podle informací Lupa.cz vyjít na nižší stovky milionů korun. Půlku zainvestuje Evropská komise skrze programy Digital Europe a Connecting Europe Facility (CEF). Druhá část půjde z českého rozpočtu, respektive z Národního fondu obnovy. Prostředky přidá i ministerstvo vnitra v rámci projektu Network Cybersecurity in Post-Quantum Era.

Zdejší kvantová síť nepřímo naváže na úspěšný přenos kvantových klíčů, který se nedávno uskutečnil mezi ostravským národním superpočítačovým centrem IT4Innovations a polským Těšínem. Prvního července 2021 byl na optické trase o délce 75 kilometrů sestaven kvantový kanál s kvantovou chybovostí 2,19 procenta.

Přenos se podařil v rámci projektu OpenQKD, do kterého Evropská komise vložila 15 milionů eur, přičemž do Ostravy z toho putovalo 240 tisíc eur.



Fyzikální podstata

Evropská komise chce obecně do ověření a vývoje kvantových technologií vložit zhruba miliardu eur. Na EuroQCI se bude podílet i Evropská vesmírná agentura, díky čemuž se má kvantová síť rozšířit na nízkou orbitu Země. Na družicích mají být umístěna fotonová zařízení.

Popisované QKD přenosy by měly být vysoce odolné proti prolomení. Využívá se symetrické šifrování. Zabezpečení přes QKD je založeno na fyzikální, nikoliv matematické podstatě. QKD generuje náhodné klíče mezi dvěma stranami, kdy je klíč kódován do kvantových stavů fotonů přenášených kvantovým kanálem. Zde jednak platí relace neurčitosti umožňující odhalit odposlech, a zároveň není možné duplikovat neznámý kvantový stav.

Evropská komise chce obecně do ověření a vývoje kvantových technologií vložit zhruba miliardu eur.

Zájem o tuto oblast tedy neprojevují pouze státy a jejich instituce, ale také největší evropští telekomunikační operátoři. Plány Evropské komise hovoří o tom, že by kvantové přenosy bylo možné integrovat do již fungující telekomunikační infrastruktury.

Kvantové krabičky, optická síť

Současná fáze budování české kvantové sítě EuroQCI nepočítá s tím, že by se instalovaly nové datové kabely a podobně.

„Půjdeme za poskytovateli optických vláken a tato vlákna si od nich pronajmeme," uvádí pro Lupu Jan Bouda z Fakulty informatiky na Masarykově univerzitě. Bouda je v Česku projektem EuroQCI pověřen jako koordinátor konsorcia univerzit.

V praxi by to mělo vypadat tak, že se do jednotlivých úřadů a institucí nakoupí specializovaná kvantová komunikační zařízení, přenos ovšem „poteče" přes standardní optiku od firem jako CETIN nebo ČD-Telematika.

Stát na tato zařízení vypíše výběrové řízení. V současné době jsou největšími dodavateli společnosti IDQ (Švýcarsko) a Toshiba (Japonsko). QKD je mladá oblast, proto v případě výrobců komunikačních přístrojů nelze mluvit o nějaké pokročilé standardizaci a kompatibilitě.

„Vize, že od jednoho výrobce bude vysílač a od druhého přijímač, je v této chvíli daleko," přibližuje pro Lupu Miroslav Vozňák z Vysoké školy báňské – Technické univerzity v Ostravě, který se podílí na popisovaném projektu OpenQKD.

„Projekt OpenQKD prakticky dostal do pracovního balíčku zástupce dvou největších výrobců QKD zařízení a spolupráce aktuálně vede k tomu, že se oba zavázali implementovat identické standardy postavené na RESTful API pro jednotný systém správy klíčů (KMS). QKD link sice bude pořád tvořit dvojice zařízení jednoho výrobce, ale za sebou budete moci řetězit QKD linky různých dodavatelů a spravovat je z jednoho KMS," doplňuje Vozňák k situaci na trhu.

Kvantový signál bez zesilovače

Česká kvantová síť bude muset vyřešit i další problémy. Komerční kvantová zařízení dnes s rozumným

bitratem zvládnou komunikaci na vzdálenost do 80 kilometrů. Kvantový signál zároveň nelze zesilovat, na to by byl potřeba malý kvantový počítač.

Bude tak nutné vybudovat segmenty, mělo by jich být patnáct až dvacet. Například mezi Prahou a Brnem vzniknou dedikovaná místa, kde budou kvantová zařízení a předají si klíče. Zde hrozí riziko nabourání, proto se v této komunikaci kromě symetrické šifry zavede také šifrování asymetrické. Využijí se již existující propojovací objekty, které jsou na optických trasách k dispozici.

Zdejší kvantová síť má zároveň obsahovat několik typů zařízení. Ta na páteřní síti mají dosáhnout na co největší bitrate a být co nejméně nápadná. S dalšími prvky mají pracovat odborníci z bezpečnostní komunity a k jiným mají mít přístup lidé od optických sítí. Ti budou potřebovat přímý přístup kvůli výměně komponent a podobně.

„Obecně bychom chtěli získat nízkoúrovňový přístup k softwaru zařízení, mimo jiné kvůli nízkoúrovňovým (low key) klíčům,“ nastiňuje Bouda.

EuroQCI by mimo jiné mělo pomoci rozšířit počty zdejších odborníků na kvantovou problematiku.

„V České republice v současné době existuje extrémně málo lidí, kteří mají dostatečné znalosti z oblasti kvantového zpracování informace, a právě v tom by měla pomoci první fáze projektu EuroQCI. Cílem je, aby v době plné implementace a nasazení EuroQCI měla ČR dostatečný počet odborníků pro její provozování,“ vysvětluje Bouda. Vzniknout proto mají školicí programy, do kterých se zapojí ČVUT a další.

Český kvantový počítač?

Z akademického sektoru zaznívají hlasy, že by se na provozování české kvantové sítě mohl podílet Cesnet, který dlouhodobě provozuje akademickou síť a nyní ji za 325 milionů modernizuje.

„Podle mého názoru by to bylo rozumné rozhodnutí,“ uvádí Vozňák. Právě Cesnet je zapojený do ostravsko-těšínských přenosů OpenQKD. Bouda ale roli této organizace vidí spíše ve vzdělávání, a to i proto, že sám Cesnet si řadu vláken pronajímá od providerů.

V kuloárech rovněž zaznívají nápady na téma, že by Česko mohlo postavit vlastní kvantový počítač.

V kuloárech rovněž zaznívají nápady na téma, že by Česko mohlo postavit vlastní kvantový počítač.

Zaujal vás tento příspěvek? Čtěte související články s příbuznou tematikou on line.

K tomu se zatím nikdo moc konkrétně vyjadřovat nechce. Podle Boudy to není příliš realistické.

„NÚKIB v současné době o stavbě kvantového počítače neuvažuje,“ vzkazuje například Národní úřad pro kybernetickou a informační bezpečnost, který je do kvantových aktivit zapojený.

Skloňuje se jméno Miloše Nesládka. Ten se zabývá kvantovým výzkumem a jeho tým nedávno na toto téma publikoval článek v časopisu Science.

„Pracujeme na vývoji nových metodologií pro realizace kvantového procesoru. Jde o základní výzkum, zatímco OpenQCI může bez problémů využít existující platformy na vývoj post quantum kódu,“ uvádí Nesládek pro Lupu.

„Boudův“ CyberSecurity Hub se bude postupně rozrůstat a dostane vlastní budovu. Řešit se v ní bude provozování páteřní sítě a školení v oblasti kvantových aktivit a také zde bude operovat evropský digitální inovační hub v kybernetické bezpečnosti. Zvažují se i další aktivity jako certifikace kyberbezpečnostních zařízení. ■

Text vyšel na sesterském webu Lupa.cz