**Olomoučtí a dánští vědci navrhli metodu, která výrazně zvyšuje bezpečnost kvantové komunikace v optických sítích**

Olomouc (9. října 2018) *–* **Výrazně vyšší bezpečnost kvantové komunikace v optických sítích zajišťuje nová metoda, kterou navrhl společný tým vědců z katedry optiky Přírodovědecké fakulty Univerzity Palackého v Olomouci a Dánské technické university v Lyngby. Nový postup je založen na využití neklasických stavů světla a díky tomu je přenos informací mnohem více odolný vůči případnému odposlechu. Výsledek práce olomouckých a dánských vědců byl publikován v prestižním časopise npj Quantum Information. Společný tým se zároveň zabývá bezpečným přenosem šifrovacího klíče na tisícikilometrové vzdálenosti pomocí telekomunikačních satelitů.**

Bezpečná kvantová komunikace v optických sítích využívá detekovatelných změn kvantového šumu světla, které principiálně způsobí odposlech během přenosu šifrovacího klíče. Každý, kdo poslouchá na optické lince se slabým optickým signálem, je proto vždy odhalitelný. Pokud odposlech není příliš silný, je možné pomocí náročných výpočetních algoritmů snížit vliv odposlechu v šifrovacím klíči dostatečně pod potřebnou mez. Pokud má ale tato výpočetní procedura být účinná, je typicky složitá a pomalá a snižuje rychlost přenosu klíče, což je velká nevýhoda této metody.

*„Náš tým navrhl radikálně jiný postup. Využít neklasických stavů světla s potlačeným šumem a optimální modulací zvolenou tak, aby odposlech nemohl získat prakticky žádnou informaci nebo pouze její minimum. To, co odposlech slyší, je mu díky tomu prakticky k ničemu. To nabízí možnost velmi rychlého zpracování klíče bez náročných a pomalých algoritmů, avšak za cenu poněkud kratšího šifrovacího klíče přeneseného za sekundu. Klíč za sekundu je možné pak prodloužit využitím mnoha frekvenčních kanálů v optických vláknech, tak jako v existujících moderních komunikacích,“* vysvětluje profesor Radim Filip z katedry optiky Přírodovědecké fakulty Univerzity Palackého.

Použitím této metody v mnoha frekvenčních kanálech optických vláken současně je možné v budoucnu dosáhnout velké kapacity, husté přenosové sítě i uvnitř velkých měst a stabilní bezpečnosti s méně účinným, ale rychlým zpracováním dat. Nový protokol pro kvantovou komunikaci v optických sítích se poprvé podařilo otestovat na Dánské technické univerzitě v Lyngby, která nejenže disponuje potřebnými zdroji stlačeného světla a detektory, ale především je kvantová distribuce šifrovacího klíče tohoto typu jejím stěžejním výzkumným programem.

„*Tento experiment završil dlouhodobý program vedoucí k naší účasti ve velkém projektu CiViQ začínajícího programu FET Flagship on Quantum Technologies. V tomto projektu jsme zodpovědni za klíčový teoretický balíček. Navíc dánský tým je důležitým partnerem i v CiViQu, zodpovědným za nejvíce příbuzný experimentální balíček. Spolu s první realizací kvantové distribuce klíče se stlačenými stavy se tento experiment stal pilířem našeho výzkumu v této oblasti,*" uvedl Vladyslav Usenko, řešitel prestižního projektu za UP.

Pozornost olomouckých vědců je zároveň upřena na bezpečný přenos šifrovacího klíče na obrovské vzdálenosti, k čemuž se používají telekomunikační satelity. První krok v tomto směru již udělala Čína, kde skupina profesora Jian-Wei Pana otestovala v roce 2017 první distribuci klíče mezi satelitem a pozemní stanicí vzdálených 1200 kilometrů. Pro obrovské ztráty na takových vzdálenostech je potřeba použít jiný kvantový přenosový protokol s vysoce citlivými detektory registrujícími jednotlivé fotony. Zároveň je nutné pečlivě analyzovat důvěryhodné a nedůvěryhodné části protokolu, aby stále dovoloval bezpečnou distribuci šifrovacího klíče. Na tuto vědeckou výzvu okamžitě reagoval německý výzkum a průmysl.

„*Naše aktivita v tomto směru je navázána na partnerské pracoviště na Max-Planck Institutu pro vědu o světle v německém Erlangenu. Naším cílem je analýza proveditelnosti a bezpečnosti vhodných protokolů pro satelitní komunikace. To je důležitá znalost, která může další generaci mladých vědců posunout ještě více k aplikacím a národním i nadnárodním telekomunikačním firmám, jako je tomu ve vyspělých zemích,*“ popisuje strategii Vladyslav Usenko, který je řešitelem i tohoto projektu.

Max-Planck Institut už spolu s německými firmami Tesat-Spacecom a SES Satellites připravil projekt pro program Scylight Evropské kosmické agentury, který zahrnuje i další klíčové týmy z Evropy. Finance pro účast českých vědců zajistilo ministerstvo dopravy ČR. „*Bez ministerstva dopravy by naše účast a plány konsorcia byly nemožné,”* podotkl Vladyslav Usenko.

Kvantová komunikační technologie je nyní v centru pozornosti Evropské unie a jejích firem. Nadnárodní podporu v této oblasti výzkumu zajišťuje nový a největší program EU – FET Flagship on Quantum Technologies, jehož rozpočet činí miliardu EUR. Už v první grantové výzvě tohoto programu se podařilo konsorciu, zahrnujícímu tým na katedře optiky kolem dr. Vladyslava Usenka a prof. Radima Filipa, vyhrát klíčový velký projekt v oblasti bezpečných kvantových komunikací. Nový tříletý projekt Continuous Variable Quantum Communications (CiViQ) sdružující 21 zahraničních partnerů (včetně firem, jako jsou německý Telekom a Huawei, francouzský Orange či španělská Telefonica, a laboratoří jako francouzské Nokia Bell Labs nebo španělské ICFO) rozvine platformu bezpečné kvantové komunikace se spojitými vlastnostmi světla směrem k jejímu komerčnímu využití. Kvantová distribuce klíče byla již implementována v několika optických vláknových sítích v Rakousku, Švýcarsku, Číně, Japonsku a USA. Její rozvoj je již nyní atraktivní pro průmysl ve vyspělých zemích světa*.*

**Kontaktní osoba**:  
Šárka Chovancová | redaktorka  
Přírodovědecká fakulta Univerzity Palackého v Olomouci   
E: [sarka.chovancova@upol.cz](mailto:sarka.chovancova@upol.cz) | M: 776 095 547