

Kvantová bezpečnost na dosah: CESNET otestoval novou generaci šifrování dat

10.12.2025 - | CESNET

Bezpečná komunikace mezi počítači je základem dnešního digitálního světa. S příchodem kvantových počítačů, které mohou prolomit současné šifrovací metody, je proto nezbytné hledat nové způsoby ochrany dat. Jedním z nich je kvantová distribuce klíčů (QKD) - technologie využívající zákonitosti kvantové fyziky k naprosto spolehlivé výměně šifrovacích klíčů.

Měření v laboratoři optických sítí CESNET potvrdilo, že kvantovou distribuci klíčů lze začlenit i do běžných vysokorychlostních optických sítí bez samostatného vlákna. To je klíčový krok k zajištění bezpečné komunikace v době rozvoje kvantových technologií.

Testování probíhalo v rámci mezinárodního projektu SEQRET (Secure and Industrialized Quantum Key Distribution for European Telecom Networks). CESNET se zaměřil na ověření systému CV-QKD (Continuous Variable Quantum Key Distribution), který vyvíjí německá společnost KEEQuant. Cílem bylo prověřit, zda může tato technologie fungovat společně s běžnými datovými přenosy v optických sítích využívajících DWDM - technologii, která umožňuje přenášet více datových kanálů současně po jednom vlákne. Při zkoušce integrace QKD odborníci využili také SDN DWDM Flex ROADM z rodiny CzechLight, tedy softwarově řízené optické zařízení vyvinuté ve sdružení CESNET pro flexibilní směrování více kanálů v DWDM síti.

Na ověření se podílela také americká společnost Ribbon, která poskytla šifrovací kartu s přenosovou rychlostí 400 Gbit/s. Šifrovací karta byla propojena se systémem CV-QKD a rozšířena o Key Management System (také od společnosti KEEQuant) pro správu kvantově generovaných klíčů. Celou konfiguraci potvrdil živý šifrovaný videopřenos, který prokázal stabilitu a spolehlivou spolupráci všech částí systému.

Kvantově bezpečné šifrování, které zahrnuje i technologii QKD, využívá principy kvantové fyziky k bezpečné výměně šifrovacích klíčů a ochraně přenosu dat. Systém tak umožňuje detekovat jakýkoli pokus o odposlech nebo zásah do přenosu dat. V budoucnu tak může zajistit bezpečný přenos citlivých informací.

Mezinárodní projekt SEQRET je financován z programu Digital Europe a sdružuje partnery z několika evropských zemí, kteří společně pracují na vybudování kvantově odolné komunikační infrastruktury nové generace.

<https://www.cesnet.cz/novinky/kvantova-bezpecnost-na-dosah-cesnet-otestoval-novou-generaci-sifrovani-dat-288>