

Sicherer Datenaustausch mit Quantenverschlüsselung über Domänen hinweg

7.8.2026 - | Friedrich-Alexander-Universität Erlangen-Nürnberg

In einem neuen Projekt erforschen Wissenschaftlerinnen und Wissenschaftler, wie quantenbasierte Verschlüsselung über Domänengrenzen hinweg flexibel und mit Hilfe von Automatisierungsprozessen in der Netzverwaltung sicher gelingen kann. Beteiligt ist auch die Forschungsgruppe „Netz“ des Regionalen Rechenzentrums Erlangen (RRZE) an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU).

Sektoren mit sensiblen Informationen wie Behörden oder Universitätsklinika sind darauf angewiesen, dass Informationen quantensicher verschlüsselt werden können, das heißt mit informationstheoretisch sicheren Verschlüsselungsverfahren, die nicht auf mathematischer Komplexität beruhen, sondern auf den Prinzipien der Quantenmechanik basieren.

Abhörsichere Schlüsselketten zwischen den Parteien

Ein solches Verfahren ist die **Verschlüsselung mit Quantenschlüsselaustausch (QKD, Quantum Key Distribution)**. Abhörversuche würden hier bemerkt und die abgefangenen Bits nicht mehr für die Schlüsselproduktion verwendet werden. Bisher funktioniert QKD nur über kurze Strecken. Für größere Distanzen bräuchte es sogenannte Trusted Nodes, also speziell geschützte Zwischenstationen, die dabei helfen, abhörsichere Schlüsselketten zwischen zwei Parteien aufzubauen.

Bis zu einem breiten Einsatz von QKD werden daher auch Post-Quanten-Kryptografische (PQK) Verfahren verwendet, die derzeit noch als sicher gelten und entwickelt wurden, um Daten auch vor Angriffen durch extrem leistungsstarke Quantencomputer zu schützen. Beide Verfahren müssen also parallel in ihren lokalen Netzdomänen aufgerufen, gesteuert und auch in den jeweiligen Netzmanagementsystemen verwaltet und überwacht werden können. Für eine Verschlüsselung über mehrere lokale Domänen hinweg können solche Steuerungsprozesse sehr komplex werden und sollten idealerweise durch software-basierte Automatisierung autonom ablaufen. Dies kann durch ein intelligentes Netzwerk-Verwaltungskonzept, wie zum Beispiel Intent-Based Networking (IBN) erfolgen, wo ein Netzadministrator nur noch das gewünschte Ziel (die „Absicht“) festlegt und das System dann diese Vorgabe mithilfe von Sprachmodellen (Large Language Models, LLMs) selbstständig in die nötigen Netzwerkeinstellungen übersetzt. Dazu wird die kontinuierliche Umsetzung mit Hilfe von Regelkreisen, sogenannten Control Loops, überwacht.

Ein solcher software- und LLM-gestützter Ablauf der Arbeits- und Kontrollprozesse im Netz bildet den Schwerpunkt der Arbeiten im Teilprojekt am RRZE „Intent-basierte quantensichere Domänenorchestrierung“.

Weitere Beteiligte im Verbundprojekt

Das Projekt am RRZE ist Teil des Verbundprojekts „**QDD - Quanten-Domänen Dynamik**“. Die Laufzeit des Projekts ist bis 2029 angesetzt. Das **Bundesministerium für Forschung,**

Technologie und Raumfahrt (BMFTR) fördert das Verbundprojekt mit 3,26 Millionen Euro. Das gesamte Projektvolumen beträgt 3,84 Millionen Euro.

Im Verbundprojekt unter der Leitung von Infosim sind neben der Forschungsgruppe Netz des RRZE beteiligt:

- Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF, Jena
- Friedrich-Schiller-Universität Jena
- Julius-Maximilians-Universität Würzburg
- Quant-X Security & Coding GmbH, Hannover
- Telefónica Germany GmbH & Co. OHG, München

Mehr Informationen

Offizielle Projekt-Website:

<https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qdd>

Projektseite Infosim <https://www.infosim.net/innovation/research-projects/qdd/>

Teilprojekt der JMU Würzburg

<https://www.uni-wuerzburg.de/aktuelles/einblick/single/news/quantennetz-sicheren-datenverkehr-internet-zukunft/>

Weitere Forschungsprojekte des RRZE

Informationssicherheit mit Quantenverschlüsselung

<https://www.rrze.fau.de/2025/07/informationssicherheit-mit-quantenverschlueselung/>

<https://www.fau.de/2026/08/news/forschung/sicherer-datenaustausch-mit-quantenverschlueselung-ueber-domaenen-hinweg>