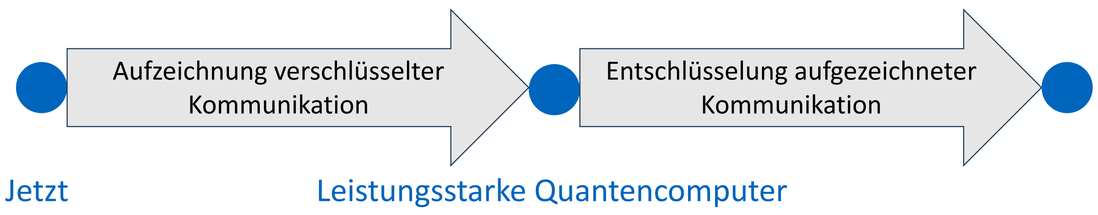
SLICES-Security

Technische Universität München

Eine Forschungsinfrastruktur für IT-Security am Beispiel Post-Quanten Kryptographie

Motivation: Verschlüsselung in einer Post-Quanten Welt

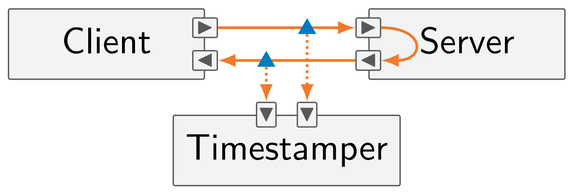
- **Leistungsfähige Quantencomputer** werden künftig in der Lage sein aktuelle Verschlüsselungsverfahren zu entschlüsseln
- Auswirkungen auf **heutige Verschlüsselung**:
  - Angreifer können bereits heute verschlüsselte Kommunikation aufzeichnen
  - Aufzeichnungen werden in Zukunft entschlüsselbar



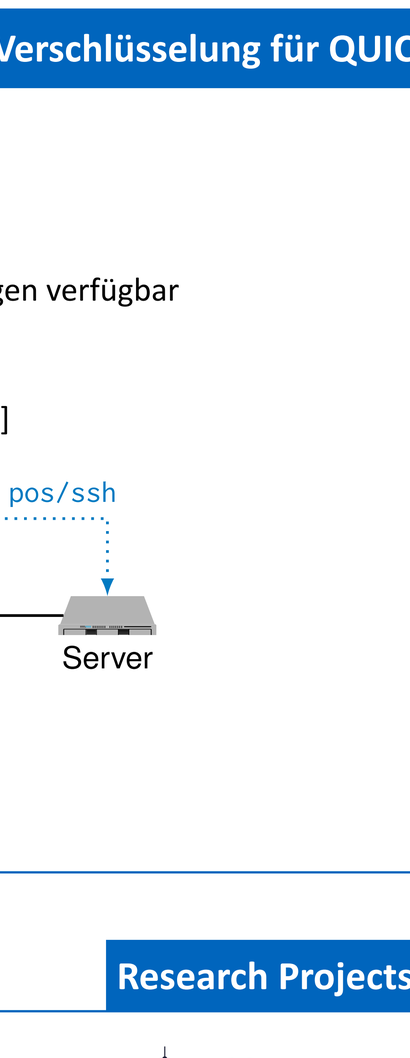
Lösung: Neuartige Verschlüsselungsalgorithmen für eine Post-Quanten Welt
Fragestellung: Sind neue Verschlüsselungsalgorithmen genauso leistungsfähig wie unsere bisherigen Algorithmen?

Forschungsinfrastruktur für Messungen

- Neue **Post-Quanten Algorithmen** befinden sich in der Entwicklung, um Kommunikation weiterhin abzusichern
- **Reproduzierbare Messungen** zur Ermittlung der Leistungsfähigkeit der Algorithmen:



- Endpunkte (**Client/Server**) nutzen PQ-sichere Implementierungen (OpenSSL & QUIC)
- **Timestamper** vermisst Kommunikation mit Hilfe von optischem Splittern und Hardware-Zeitstempeln im Nanosekundenbereich



Leistungsfähige PQ-Verschlüsselung (TCP/TLS) [3]

Szenario

- Mobilfunk (LTE-M), 10% Paketverslust, 200 ms Netzwerkverzögerung, Bandbreite: 1 Mbit/s

Ergebnisse

NIST Security	Key Agreement	Signature Algorithm	Handshake Latency Median [ms]
Level 1	X25519	rsa:2048	214.13
	hqc128	rsa:2048	251.31
	ml-kem512	rsa:2048	220.02
Level 3	**hqc192**	rsa:2048	568.28
	ml-kem768	rsa:2048	222.57
Level 5	**hqc256**	rsa:2048	706.85
	ml-kem1024	rsa:2048	226.95

Legend: **post-quantum** ▢ Full handshake (Client Hello → Client Finished)

- PQ-Schlüsselaustausch: Vergleichbare Leistungsfähigkeit zu X25519
- PQ-Schlüssellängen: Problematisch bei langsamen Verbindungen
- PQ-Signaturverfahren: Schneller als übliche RSA_2048 Signaturen
- Hohe Security-Level: PQ-Verfahren leistungsfähiger als p521/RSA_2048

Post-Quanten Verschlüsselung für QUIC

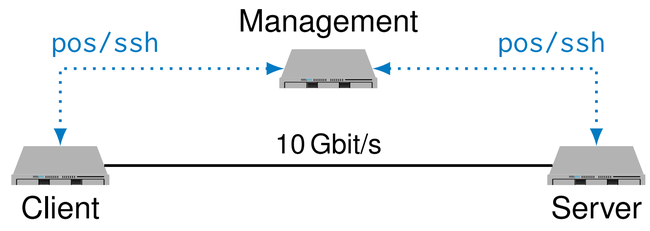
QUIC: modernes Transportprotokoll

- Läuft im Userspace basiert auf UDP
- Grundlage für HTTP/3
- Unterschiedliche Open Source Implementierungen verfügbar

PQ-Algorithmen bereits in QUIC+TLS integriert

- LSQUIC, MsQuic, quiche: BoringSSL

Reproduzierbare Experimentausführung mit pos [1]



ML-KEM und **ML-DSA** für PQ-sicheres QUIC [2]

- Vergleichbare Länge des Handshake-Verfahrens
- Hybride Ansätze kaum langsamer

TUM-NET: Reproduzierbare Vermessung für IT-Sicherheit

Schlüsselbeiträge

- Post-Quanten TCP/TLS:
  - Vergleichbare Leistung zwischen traditionellen Verschlüsselungs-algorithmen und Post-Quanten Algorithmen
  - Schlüssellängen von Post-Quanten Algorithmen sind um ein vielfaches länger als bisher, was die Leistungsfähigkeit, gerade für langsame Verbindungen negativ beeinflusst
  - Protokollanpassungen nötig, um mit Post-Quanten Algorithmen die bisherige Leistungsfähigkeit zu erreichen
- Post-Quanten QUIC:
  - Vergleichbare Leistungsfähigkeit bei kurzen Schlüssellängen

Forschungsinfrastruktur ist Voraussetzung für praxisnahe und realistische Messungen

Research Projects

Beiträge zum BMBF-Projekt **6G-ANNA**:

- Fokus auf sichere, industrielle Kommunikation

Ergebnisse:

- Vermessung von Verfahren für sichere und zuverlässige Kommunikation

SLICES-RI & GreenDIGIT:

- EU-Initiative mit Teilnehmern aus 16 Mitgliedsländern
- **Ziel:** Digitale Forschungsinfrastruktur für die IKT
- Im Betrieb seit Ende 2024:
  - *Post-5G Blueprint*
- Innovative Ansätze zur Verringerung des ökologischen Fußabdrucks digitaler Forschungsinfrastrukturen

[1] S. Gallenmüller, D. Scholz, H. Stubbe, and G. Carle. The pos Framework: A Methodology and Toolchain for Reproducible Network Experiments. In CoNEXT, 2021.
[2] M. Kempf, N. Gauder, B. Jaeger, J. Zirngibl, and G. Carle. A Quantum of QUIC: Dissecting Cryptography with Post-Quantum Insights. In IFIP Networking, 2024.
[3] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, and G. Carle. The Performance of Post-Quantum TLS 1.3. In CoNEXT, 2023.

Kontaktdaten

- Sebastian Gallenmüller, Kilian Holzinger, Daniel Petri, Georg Carle
- +49 (89) 289 18032
- gallenmu | holzingk | petriroc | carle @net.in.tum.de
- https://net.in.tum.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung