Lehrstuhl für Netzarchitekturen und Netzdienste, Prof. Carle
School of Computation, Information, and Technology
Technische Universität München

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Robuste und sichere Kommunikation für die Mobilfunknetze der Zukunft

im Kontext der BMBF Projekte 6G-ANNA und 6G-life

Problembeschreibung

Ziel: Ermöglichen neuer Mobilfunkanwendungen

- z.B. für Mensch-Maschine-Interaktion, Telemedizin oder tele-operiertes Fahren
- dadurch hohe Anforderungen bzgl. Informationssicherheit, Resilienz, Echtzeiteigenschaften und Datenraten

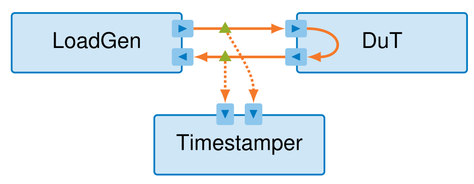
Herausforderungen:

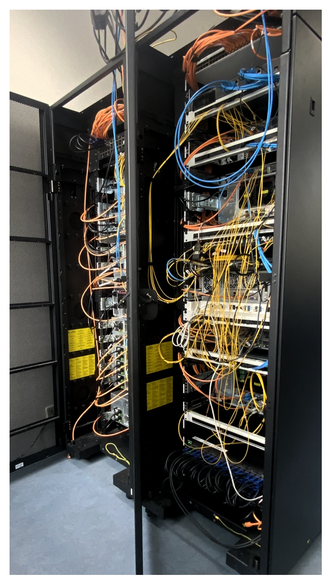
- Quantencomputer bedrohen herkömmliche Kryptoverfahren
- zeitkritische und zuverlässige Netzwerkprotokolle
- Konsensalgorithmen für Byzantinische Fehlertoleranz sind kommunikationsintensiv

Präzise Messungen im Testbed

Vier Testbeds für Netzwerkexperimente

- mehr als 50 Hosts und vier P4-Switches
- 1, 10, 25 und 100 Gbit/s Adapter
- optische Splitter
- Automatisierung und Reproduzierbarkeit mittels Testbedverwaltung pos [3]
- Teil der EU-weiten SLICES Testplattform





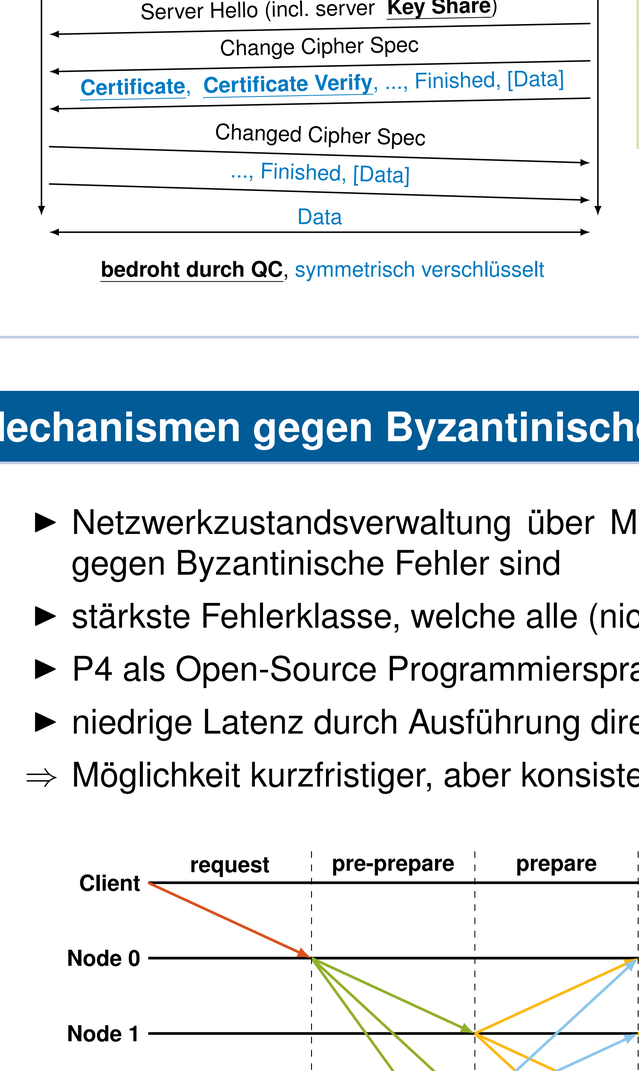
⇒ Messungsbasiertes Vorgehen für praxisrelevante Ergebnisse

Verschlüsselung im Zeitalter der Quantencomputer

- Verschlüsselungsverfahren basieren auf Komplexität von Berechnungen (z.B. Primfaktorzerlegung)
- Quantencomputer lösen diese sehr schnell
- ↯ Beeinträchtigung der Vertraulichkeit

⇒ Schutz durch Post-Quanten-Kryptoverfahren (z.B. KYBER)

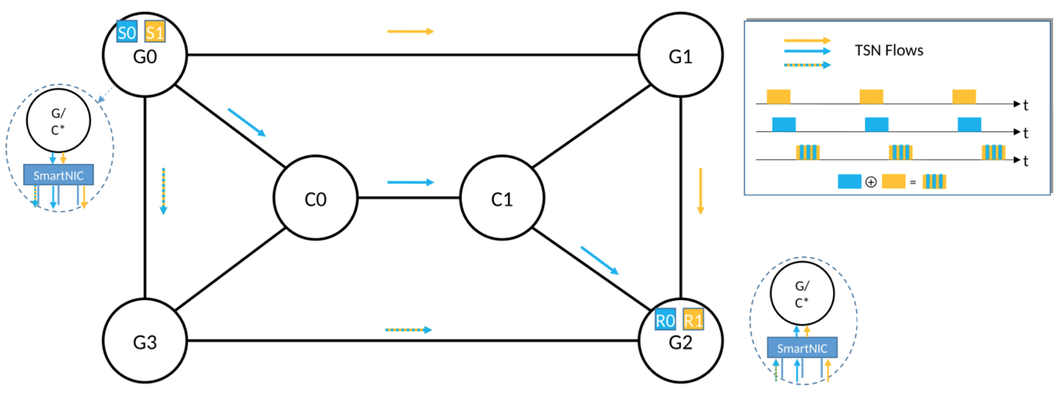
- Auswirkungen auf Datenrate und Latenz unklar



bedroht durch QC, symmetrisch verschlüsselt

Welche Strategien für effiziente und sichere Kommunikation gibt es im Post-Quanten-Zeitalter?

Fehlerkorrektur und Multipfad-Protokolle

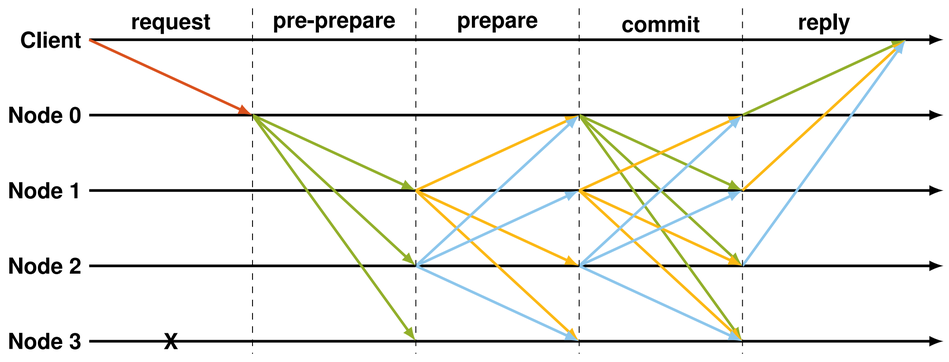


- zuverlässige Kommunikation trotz Fehler, Angriffe und Überlast
- flexibel konfigurierbar für verschiedene Bedrohungsszenarien
- geringer zusätzlicher Kommunikationsaufwand durch Network Coding und Vorwärtsfehlerkorrektur

Mechanismen gegen Byzantinische Fehler

- Netzwerkzustandsverwaltung über Mechanismen, welche sicher gegen Byzantinische Fehler sind
- stärkste Fehlerklasse, welche alle (nicht-byz.) Fehler einschließt
- P4 als Open-Source Programmiersprache für Netzwerkknoten
- niedrige Latenz durch Ausführung direkt in der Data Plane

⇒ Möglichkeit kurzfristiger, aber konsistenter Reaktionen



Nachrichtenaustausch in “Practical BFT” [1]

6G-ANNA und 6G-life

Mobilfunknetze der 6. Generation für hochzuverlässige Anwendungen benötigen eine robuste und sichere Architektur

Ausgewählte Kooperationspartner:

6G-life

- TU-Dresden: Zuverlässige Data Planes für Echtzeit-Kommunikation

6G-ANNA

- Siemens: Ausfallsichere und zeitkritische Kommunikation im Kontext Industrie 4.0
- Airbus: Vernetzung zur Steuerung von Flugtaxis

[1] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Trans. Comput. Syst.*, 20(4), Nov. 2002.
[2] P. Emmerich, S. Gallenmüller, D. Raumer, F. Wohlfart, and G. Carle. MoonGen: A Scriptable High-Speed Packet Generator. In *Internet Measurement Conference*, Tokyo, Japan, 2015.
[3] S. Gallenmüller, D. Scholz, H. Stubbe, and G. Carle. The pos Framework: A Methodology and Toolchain for Reproducible Network Experiments. In G. Carle and J. Ott, editors, *CoNEXT '21: The 17th International Conference on emerging Networking EXperiments and Technologies, Virtual Event, Munich, Germany*. ACM, Dec. 2021.
[4] S. Günther, M. Riemensberger, and W. Utschick. Efficient GF Arithmetic for Linear Network Coding using Hardware SIMD Extensions. In *Proceedings of the International Symposium on Network Coding (NetCod)*, Aalborg, Denmark, June 2014.

Kilian Holzinger, Henning Stubbe, Manuel Simon, Sebastian Gallenmüller, Georg Carle *{ holzinger | stubbe | simonm | gallenmu | carle }@net.in.tum.de*