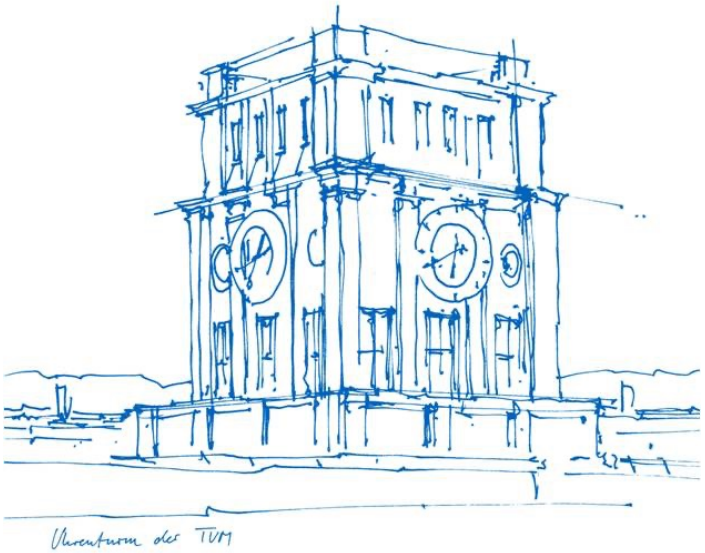
Chair of Network Architectures and Services
Department of Computer Engineering
School of Computation, Information and Technology
Technical University of Munich

GRNVS - Additional Material

Georg Carle

carle@net.cit.tum.de

Acknowledgements:
All members of the Chair of
Network Architectures and Services



Quantenkommunikation

Quantenkommunikation

- Übertragung, Verarbeitung oder Nutzung von Information unter Verwendung quantenmechanischer Zustände (z. B. einzelner Photonen)
- nutzt Phänomene der Quantenmechanik, insbesondere:
  - Superposition (Zustände können überlagert sein)
  - Verschränkung (Entanglement)
  - Messprozess verändert den Zustand

Anwendungen von Quantenkommunikation

- Quanten-Netzwerke
  - Zur Verbindung von Quantencomputer
  - Vernetzte Quantensensorik
- Quantum-Key-Distribution

Quantum-Key-Distribution (QKD)

Problem

- Quantum-Computer könnte mit Shor‘s Algorithmus konventionelle Public-Key-Crypto-Algorithmen brechen (die auf Faktorisierung oder diskretem Logarithmus aufbauen)

Idee

- Ausnutzung von Phänomenen der Quantenmechanik (Messprozess verändert Zustand) zum Entdecken von Abhören
- Verteilen eines Kryptographischen Schlüssels mittels Quanteneffekten zwischen zwei Kommunikationspartnern
- Konventionelle Hochgeschwindigkeits-Kommunikation und Verschlüsselung

Stand

- Zahlreiche Artikel auch in nicht-wissenschaftlichen Medien
- Zahlreiche QKD-Forschungsprojekte (teure Hardware etc.)
- Kommerzielle Produkte

Reflektion

Kompetenzübung: Informationen bewerten

WIKIPEDIA
25 Jahre freie Enzyklopädie

Quantenschlüsselaustausch

- NZZ: Quantenkryptografie-Systeme der zweiten Generation auf dem Markt

WIKIPEDIA
25 Jahre freie Enzyklopädie

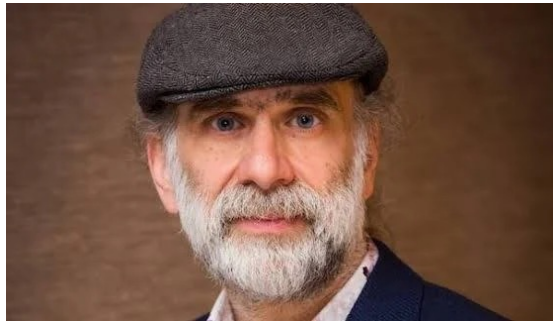
Quantenkryptographie

Fraunhofer IPMS
https://www.ipms.fraunhofer.de › ... · Diese Seite übersetzen

Quantum Key Distribution (QKD) - Fraunhofer IPMS

QKD not only enables secure key exchange but also detects any eavesdropping attempts, ensuring that any interference is immediately flagged to the parties ...

BSI - Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de



Bruce Schneier

Quantum-Key-Distribution (QKD) - Kritik

- https://www.schneier.com/blog/archives/2007/10/switzerland_pro.html
  Switzerland Protects its Vote with Quantum Cryptography
  This is so silly I wasn't going to even bother blogging about it. But the sheer number of news stories has made me change my mind.
- https://www.schneier.com/essays/archives/2008/10/quantum_cryptography.html
  Quantum Cryptography: As Awesome As It Is Pointless
  Wired - October 16, 2008
- https://en.wikipedia.org/wiki/Quantum_key_distribution
  Deprecation of quantum key distributions from governmental institutions
  Given the practical challenges raised below, several organizations recommend using "post-quantum cryptography" instead of quantum key distribution.
  - USA National Security Agency,[114]
  - European Union Agency for Cybersecurity of EU (ENISA),[115]
  - United Kingdom's National Cyber Security Centre,[116]
  - French Secretariat for Defense and Security (ANSSI),[117]
  - German Federal Office for Information Security (BSI)[118]
  - …

Post-Quantum Cryptography (PQC)

Problem

- Quantum-Computer könnten mit Shor‘s Algorithmus konventionelle Crypto-Algor. brechen

Idee

- Kryptografische Algorihmen, die mit Shor‘s Algorithmus nicht brechbar sind

Stand

- Zahlreiche Post-Quantum Cryptography Forschungsprojekte (Theorie, Software)
- NIST standardisiert Post-Quantum Cryptography (PQC)
- Browser, OpenSSL mit PQC verfügbar

Probleme

- Eingeschränkte Krypto-Agilität in Software-Stacks
- Geringere Erfahrung mit PQC-Algorithmen => Hybride Kryptographie-Verfahren

Questions?