



Quantencomputer gefährden IT-Systeme? Nicht mit uns.

Karolin Varner

<https://rosenpass.eu>

Der Plan



1. Wir stellen uns vor
2. Safety & Security: Kulturelle Aspekte
3. Kryptografie und Avionik im Dialog
4. Kryptoagilität erreichen



Folien

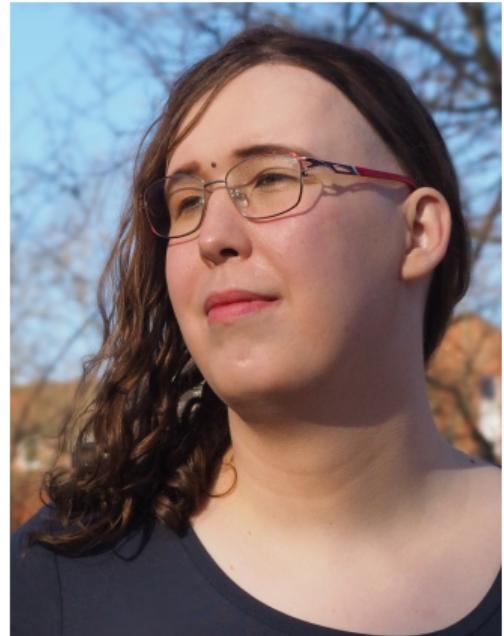


Full Paper

Karolin Varner



- Software-Entwicklerin & Kryptografin
- 11 Jahre in der Industrie bei Startups und Konzernen
- Seit 2024 am Max-Planck-Institut für Sicherheit und Privatsphäre
- Initiatorin & Leiterin des Rosenpass e.V.
- Arbeit an weiteren Projekten wie zum Beispiel der X-Wing Chiffre



- 2023 gegründet zur Betreuung des gleichnamigen Projekts
- Absicherung von WireGuard gegen Attacken durch Quantencomputer mittels protocol-level Hybridisierung
- Institution für Translationsforschung in der Kryptografie
- Schnittstelle zwischen Forschung, Industrie und Gesellschaft



rosenpass.eu

Was ist Kryptografie

Was ist Kryptografie



Bild: Schutz Privater Kommunikation
"Niemand soll es Mitlesen"

- Küchentisch
- Briefgeheimnis
- Arztgespräch

Räume im Internet, die wie im Rest des Lebens funktionieren.

Bild Schutz vor Kriminalität

- Bankraub (Online Banking)
- Betrug
- Spionage
- Vandalismus

Das Internet ist öffentlich



Bild:

- Öffentlicher Platz mit ganz viel geheimer Kommunikation die öffentlich geteilt wird

Wie das funktioniert



Bild:

- Patient und Doktor sprechen via Internet
- Zwei computer (oder andere geräte) kommunizieren miteinander
- Haben geheime Schlüssel
- Absicherung von Kommunikation via Mathematik
- Internet ist an sich öffentlich

Endzeitstimmung

Quantastriophe: Die Zerstörung der Kryptografie



Todo (Karo): Reisserische Youtube Headings Einfügen

- <https://www.youtube.com/watch?v=e-llgqD5Nxk>
- <https://www.youtube.com/watch?v=h6w4SX7ZJMQ>
- <https://www.youtube.com/watch?v=-UrdExQW0cs>
- <https://www.youtube.com/watch?v=05Uy-hFFkRU>
- <https://www.youtube.com/watch?v=ON5pVc9bIRo>

Quantencomputer – So schnell wie Fusion



TODO: Karo – Insert poll from

<https://postquantum.com/post-quantum/q-day-crqc-predictions/>

Quantencomputer – Ein Risiko Besteht



Bild: Erde Stoppt

- "Ahh wir haben vergessen die Erde zu tanken"
- "Hmm, riecht nach huhn" (helle seite)
- "Yeah, schlitten fahren" (dunkle seite)
- "Technoparty, die ewige nacht lang" (dunkle seite)

Quantencomputer – Jetzt speichern, später angreifen



Bild: Store now decrypt later attack

Migration zur Post-Quanten Sicherheit

Migration zur Post-Quantum-Sicherheit



Bild: Timeline

- 1978: McEliece Kryptosystem publiziert (erstes mit PQ-Sicherheit)
- 1994: Shors Algorithmus Publiziert (Quantenangriffe Entdeckt)
- 2016: NIST-Wettbewerb für PQ-Sichere Kryptosysteme angekündigt
- 2019: Experiment zur nutzung von PQ-Sicherheit auf Websites
- 2022: OpenSSH-Release abgesichert
- 2023: Rosenpass veröffentlicht (WireGuard abgesichert)
- 2023: Signal Messenger abgesichert
- 2024: NIST-Wettbewerb führt zum ersten Standard
- Zukunft: Umfassender Einsatz von PQ-Sicherheit

Die Systeme sind die Probleme



Bild:

- Doktor / Patient kommunizieren
- Dritter Server der Schlüssel verteilt (Vierter fünter server)
- Pfeil auf patientencomputer: Windows XP, Virusverseucht
- Mensch mit Besen beim Arzt "Haut computer wenn das internet stottert"
- "Heriberts-Kneipe" – Promo USB Stick (Einzigster Speicher der Geheimen Schlüssel) steckt im Zertifikatscomputer

Sichere Verschlüsselungssysteme bestehen aus vielen Komponenten, die müssen alle abgesichert werden.

- Es gibt keine Garantie dass Kryptografische Systeme für immer sicher bleiben
- Wir müssen bei der Aktuellen Migration systeme so umbauen, dass zukünftige migration einfacher wird

Bild: Buzzer "Crypto agility" mit Hand die ihn Drückt

Werbесendung

Rosenpass: PQ-Zusatzkomponenten für WireGuard



Bild:

- -> Outcome two: "Systemupgrade mit Zusatzkomponente" - I bolted an extra heisenberg crypto condensator (Rosenpass)

Der Große Vorteil von VPN-Systemen



Bild:

- Arztgesprächsbild von vorhin mit Rosenpass als Middelbox die beide enden schützt

TODO: Karo – Turn into nice slide with logos

- OpenSSH – Post Quantum Secure Server Administration
- Signal – Post-Quantum Secure Messaging
- Rosenpass – Post-Quantum Secure (Site to site VPN)
- Mullvad – Post-Quantum Secure Internet Gateway (Internet Gateway VPN)
- SSL
 - WolfSSL – Post-Quantum Capable TLS
 - Chromium
 - Nginx
 - Apache