



Quantencomputer gefährden IT-Systeme? Nicht mit uns.

Karolin Varner

<https://rosenpass.eu>

1. Was ist Kryptografie
2. Endzeitstimmung (Quantenattacken)
3. Migration zu Post-Quanten-Kryptografie
4. Werbesendung (Die Migration im Eigenen Betrieb)



Folien

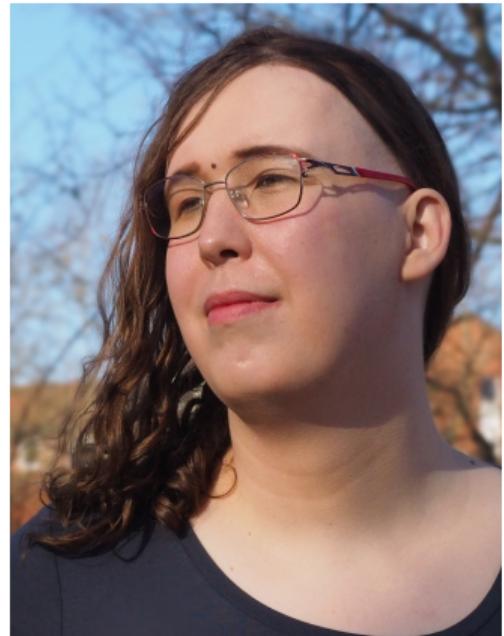


Full Paper

# Karolin Varner



- Initiatorin & Leiterin des Rosenpass e.V.
- Software-Entwicklerin & Kryptografin
- 12 Jahre in der Industrie bei Startups und Konzernen
- Seit 2024 am Max-Planck-Institut für Sicherheit und  
Privatsphäre
- Arbeit an Rosenpass & weiteren kryptografischen 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



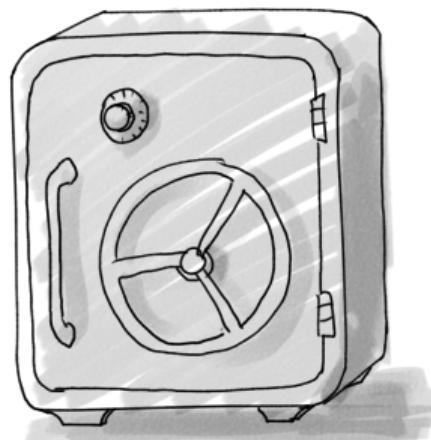
[rosenpass.eu](http://rosenpass.eu)

# Was ist Kryptografie

# Sichere Kommunikationsräume Schaffen



Schutz von Privatem



Schutz vor Diebstahl & Vandalismus

# Digitale Räume, so sicher wie die analogen



# Datenkommunikation ist öffentlich



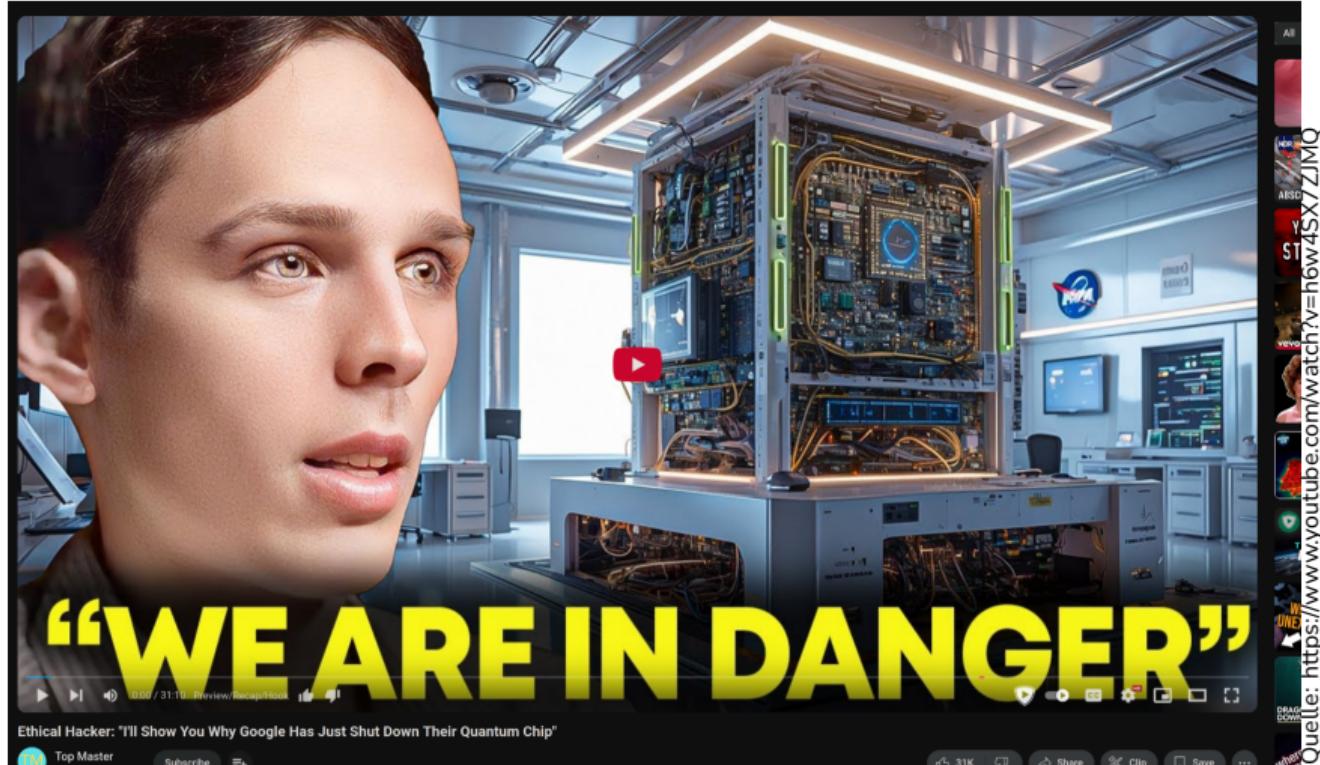
# Datenströme wie Kauderwelsch



- Patient und Doktor tauschen geheime Zahlen aus
- Beide Computer verschlüsseln
- Patient und Doktor verstehen sich
- Für alle anderen ist der Datenstrom Kauderwelsch
- Ordentlich umgesetzt sehen sie nicht mal, wer mit wem spricht

# Endzeitstimmung

# Die Zerstörung der Kryptografie



# Die Zerstörung der Kryptografie

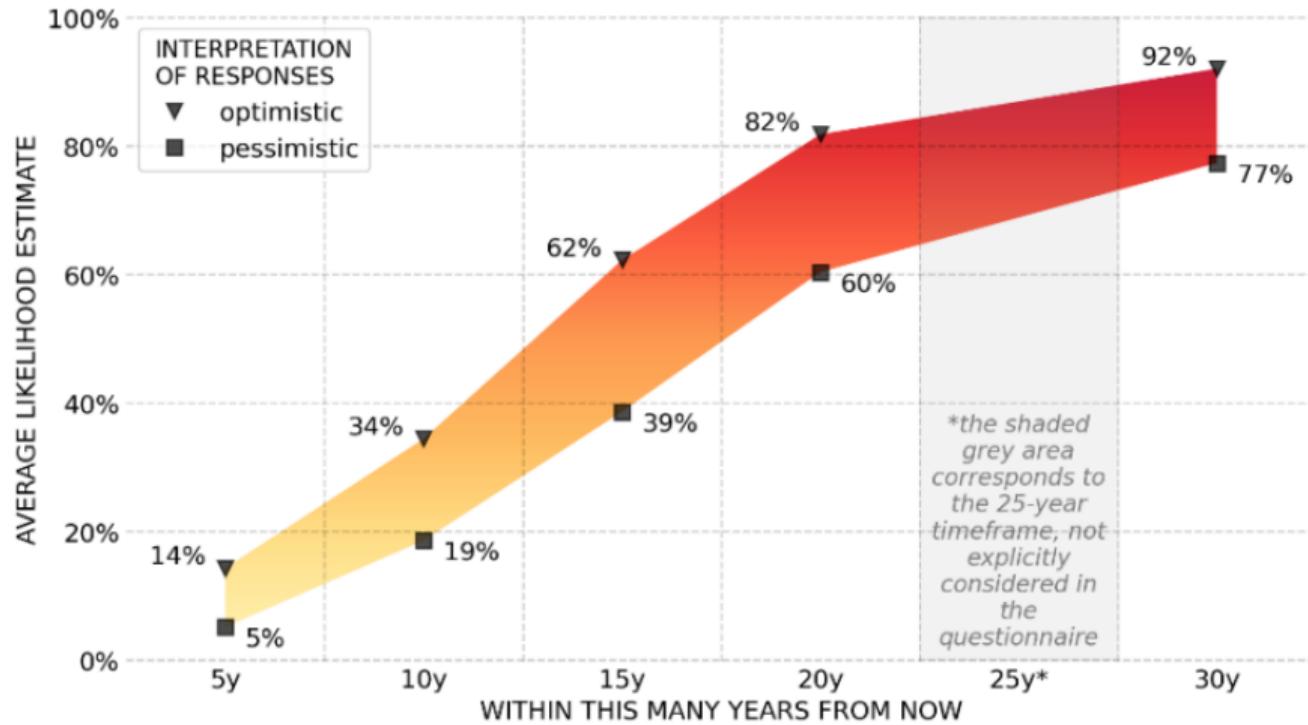


# Die Zerstörung der Kryptografie



Quelle: <https://www.youtube.com/watch?v=-UrdExQW0cs>

# Quantencomputer – So schnell wie Fusion



Quelle: <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>

- Wir arbeiten im Internet
- Wir steuern kritische Infrastruktur via Internet
- Unsere Lieferketten brauchen das Internet
- ⇒ Ein Ausfall wäre Verheerend

# Jetzt speichern, später angreifen

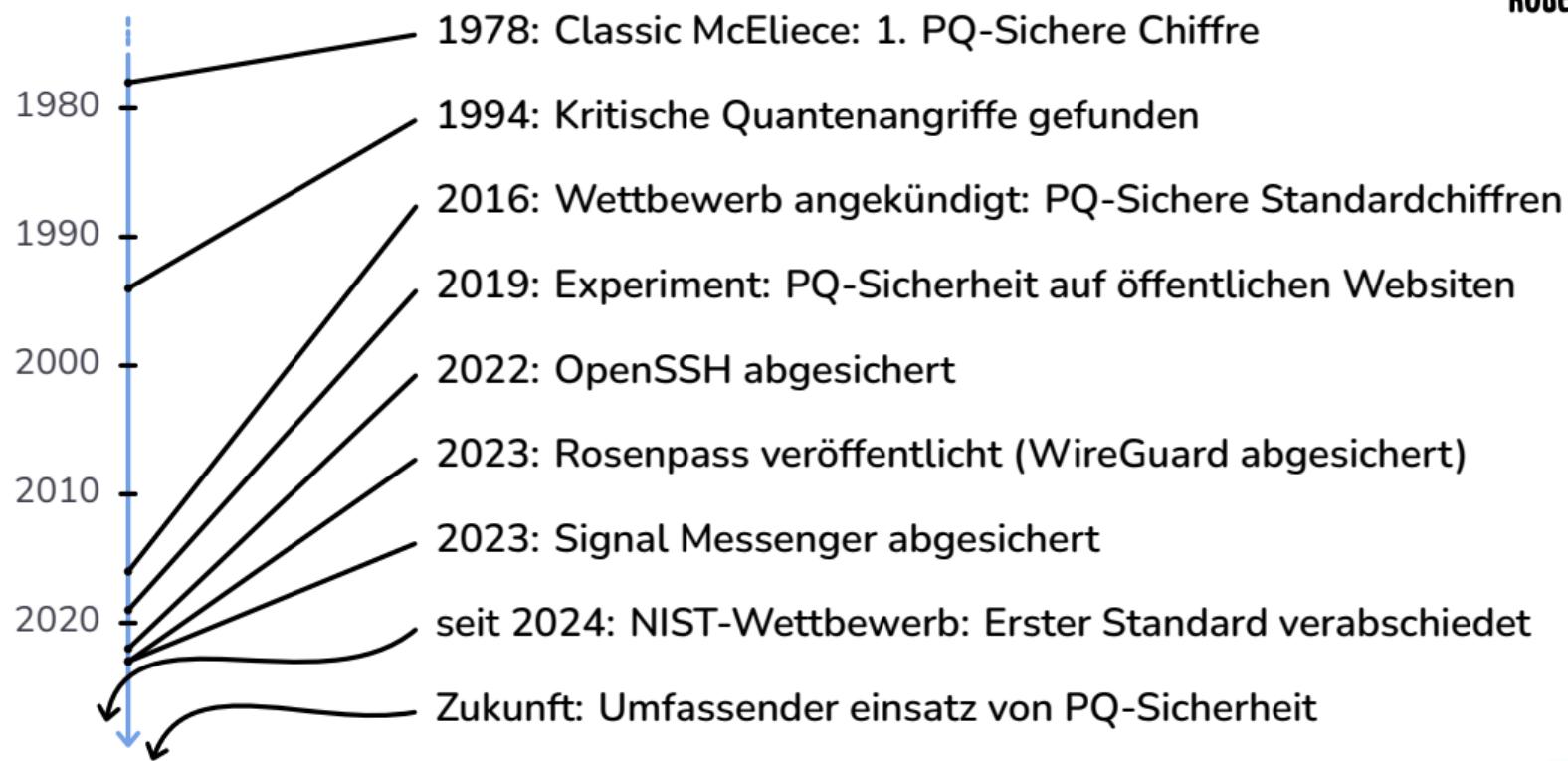


- Angreifer können verschlüsselte Daten auf Vorrat speichern
- So werden Angriffe auf vergangene Kommunikation möglich
- “Store now, decrypt later Attack”



# Migration zur Post-Quanten Sicherheit

# Migration zur Post-Quantum-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



OpenSSH  
Linux Server Administration



Signal  
Messaging



VPN



mullvad.net  
Internet Gateway (VPN  
Provider)



wolfSSL

SSL/TLS, Web  
(Not standardized)