



Quantencomputer gefährden IT-Systeme? Nicht mit uns.

Karolin Varner

<https://rosenpass.eu>



## Der Plan

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



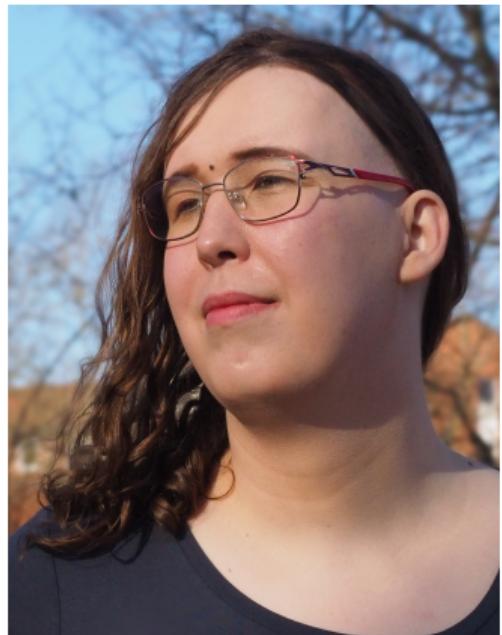
Folien



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



## Rosenpass e.V.



- 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



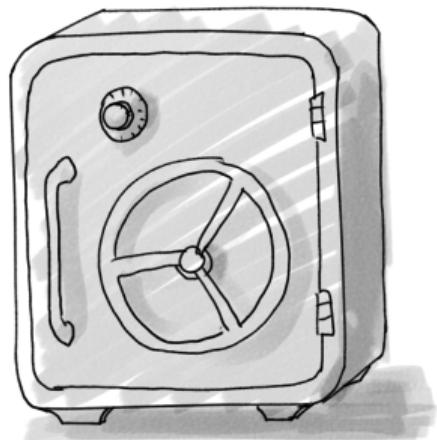
[rosenpass.eu](http://rosenpass.eu)

# 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



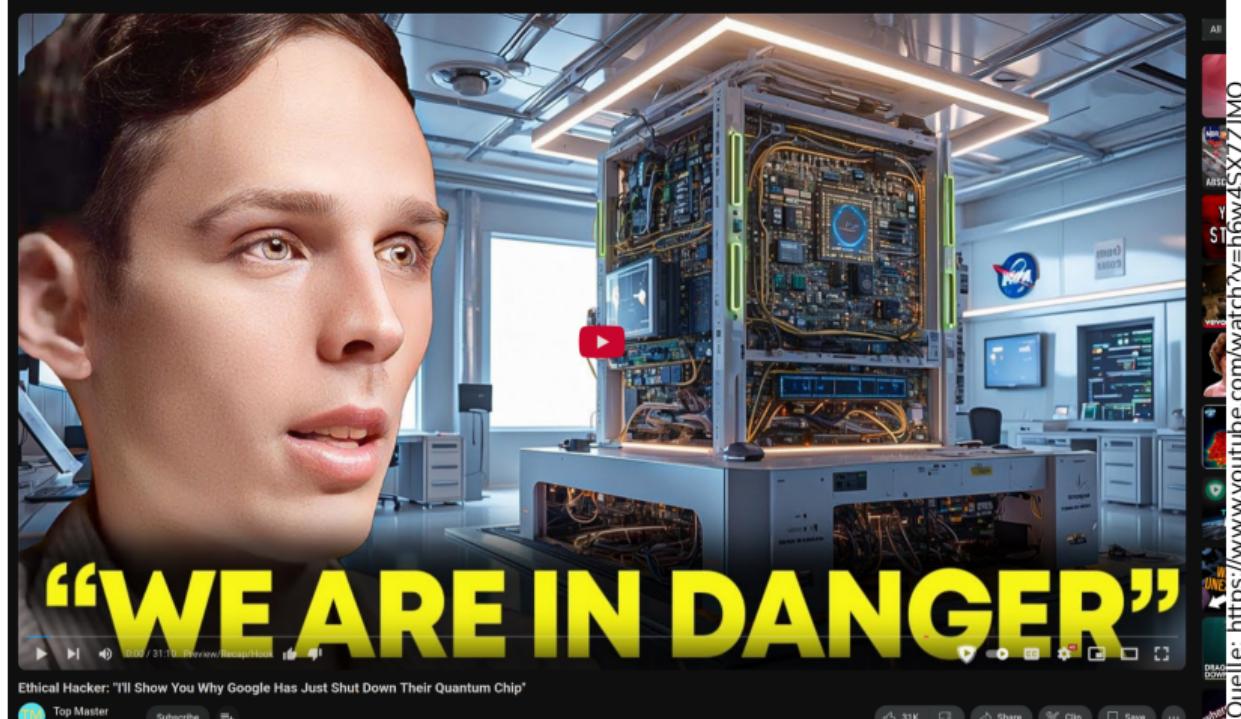
- Patient und Doktor tauschen geheime Zahlen aus
- Beide Computer verschlüsseln
- Patient und Doktor verstehen sich
- Für alle anderen ist der Datenstrom Kauderwelsch
- Ordentlich umgesetzt sehen sie nicht mal, wer mit wem spricht

Quantencomputer gefährden IT-Systeme? Nicht mit uns.

# Endzeitstimmung



# Die Zerstörung der Kryptografie



Quelle:



## Die Zerstörung der Kryptografie



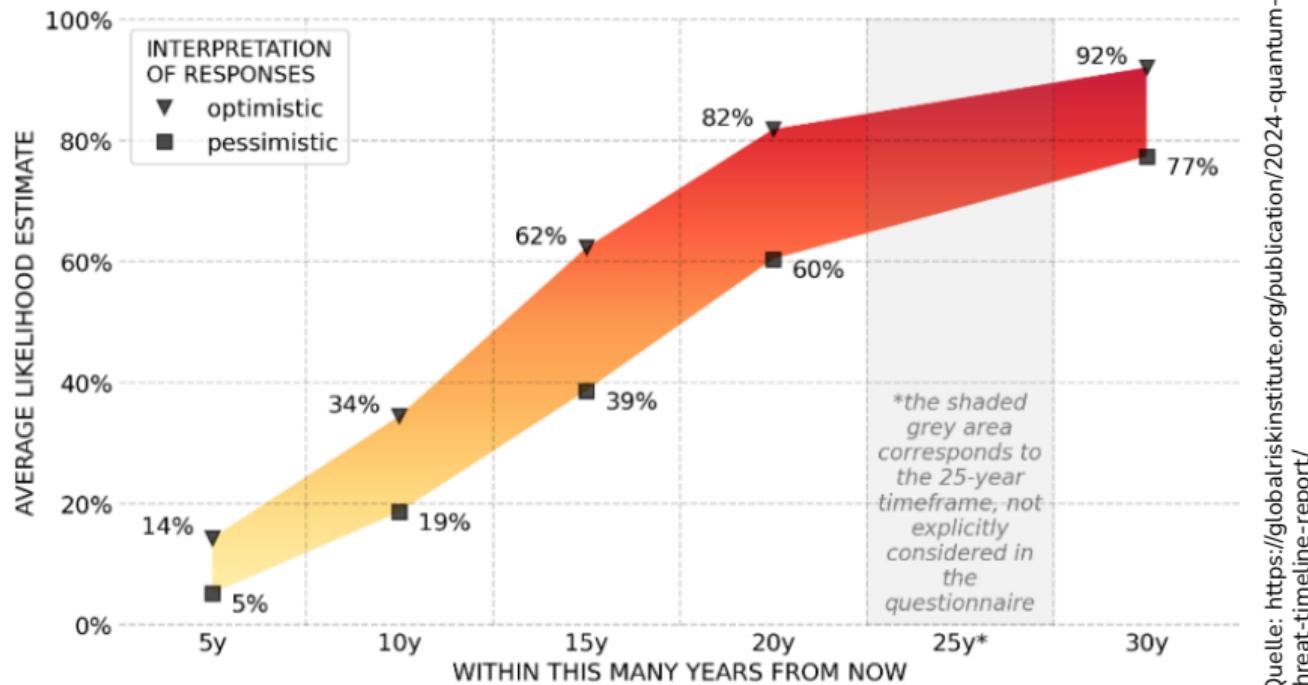


## Die Zerstörung der Kryptografie





## Quantencomputer – So schnell wie Fusion



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



## Unsere Welt im Internet

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



## Jetzt speichern, später angreifen

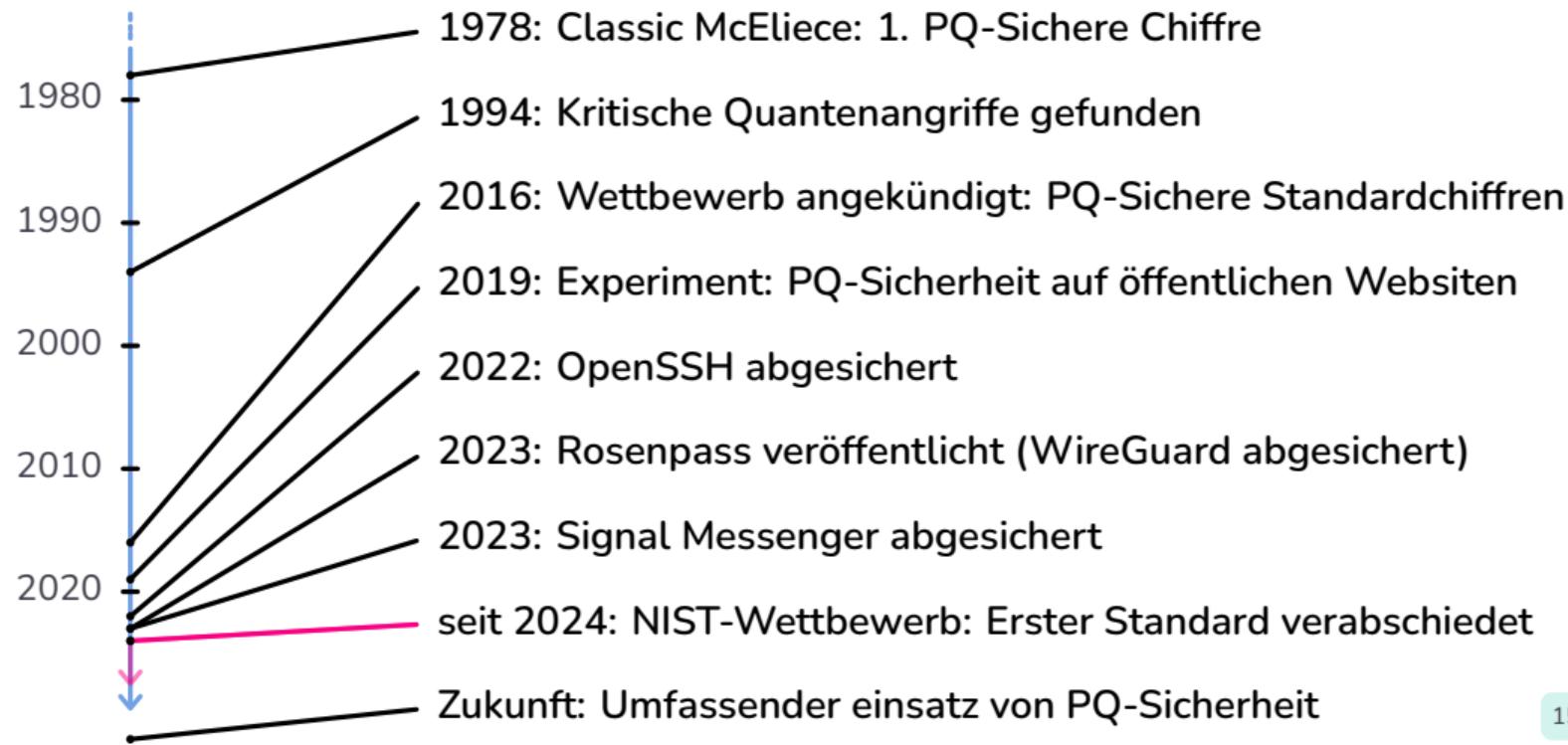
- Angreifer können verschlüsselte Daten auf Vorrat speichern
- So werden Angriffe auf vergangene Kommunikation möglich
- “Store now, decrypt later Attack”



Quantencomputer gefährden IT-Systeme? Nicht mit uns.

# Migration zur Post-Quanten Sicherheit

# Migration zur Post-Quantum-Sicherheit

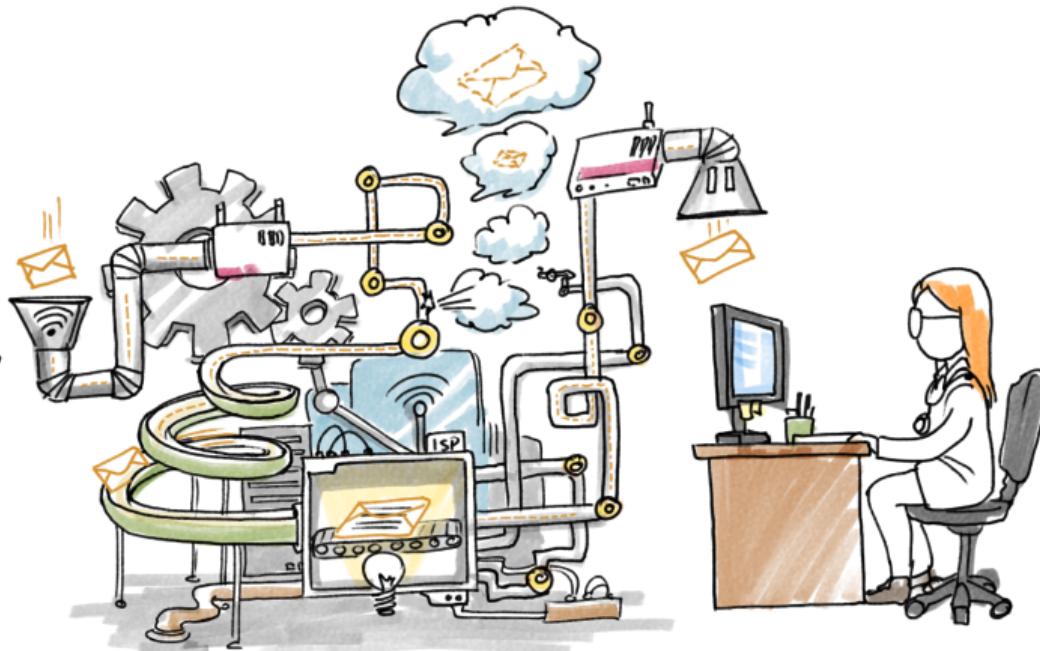


## Systemkomplexität ist eine Herausforderung



## Systemkomplexität ist eine Herausforderung

- Unsere Kryptografische Infrastruktur besteht aus vielen Einzelkomponenten
- Wir wissen nicht genau welche
- Fast alle müssen Migriert werden



## Kryptoagilität

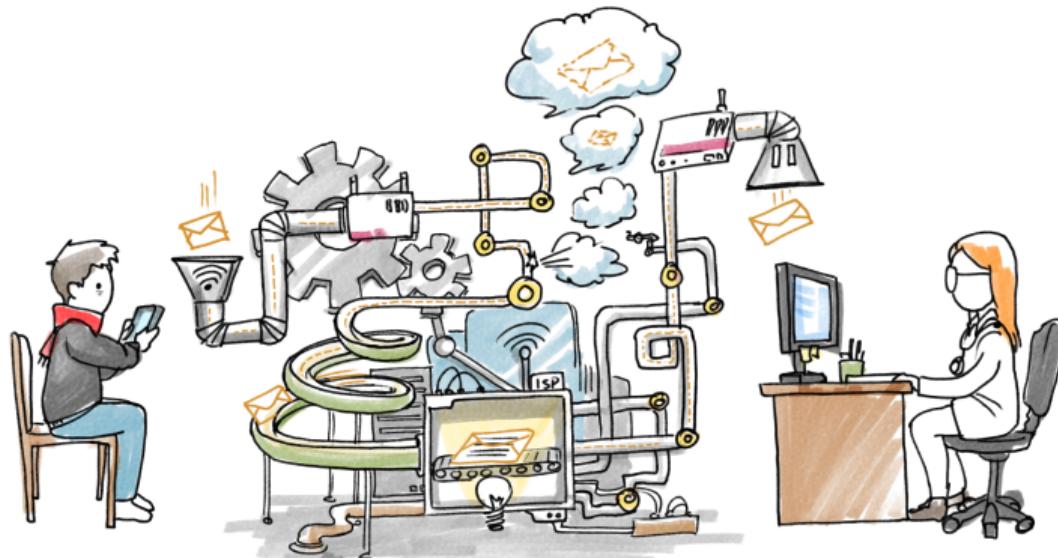


- Dokumentieren welche Kryptografische Infrastruktur vorliegt
- Prozesse für einen schnellen Austausch etablieren
- Nachhaltig und Dauerhaft

Quantencomputer gefährden IT-Systeme? Nicht mit uns.

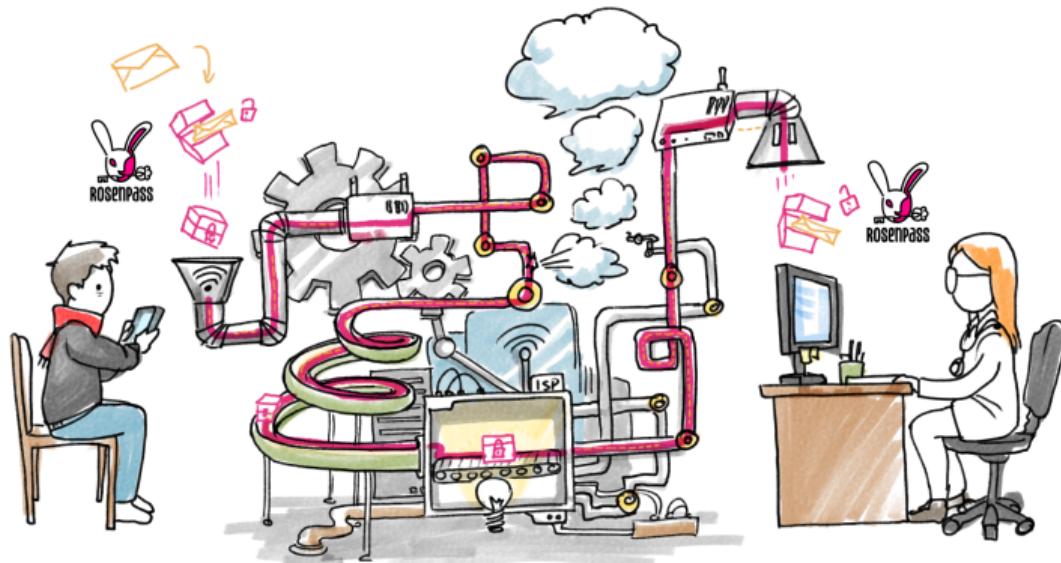
# Werbung

## PQ-Sicherheit ohne Infrastrukturaustausch





## PQ-Sicherheit ohne Infrastrukturaustausch



Der VPN-Vorteil: Post-Quanten-Sicherheit als Zusatzkomponente

Quantencomputer gefährden IT-Systeme? Nicht mit uns.



OpenSSH  
Linux Server  
Administration



mullvad.net  
Internet Gateway  
(VPN Provider)



Signal  
Messaging



VPN



wolfSSL  
SSL/TLS, Web  
(Not standardized)