



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

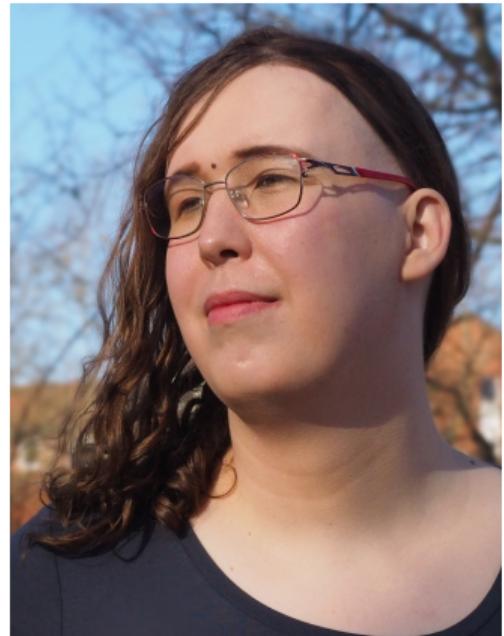


Full Paper

Karolin Varner



- 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 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



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

Die Zerstörung der Kryptografie



WE ARE IN DANGER

Ethical Hacker: "I'll Show You Why Google Has Just Shut Down Their Quantum Chip"

9/20

Die Zerstörung der Kryptografie



IT'S COMING!

0:00 / 20:37 • Intro >

Quantum Computing Explained: What It Means for Bitcoin Security

Coin Bureau • Subscribe

5.5K Share Thanks Clip Save

9/20

Die Zerstörung der Kryptografie



NO SECRET IS SAFE

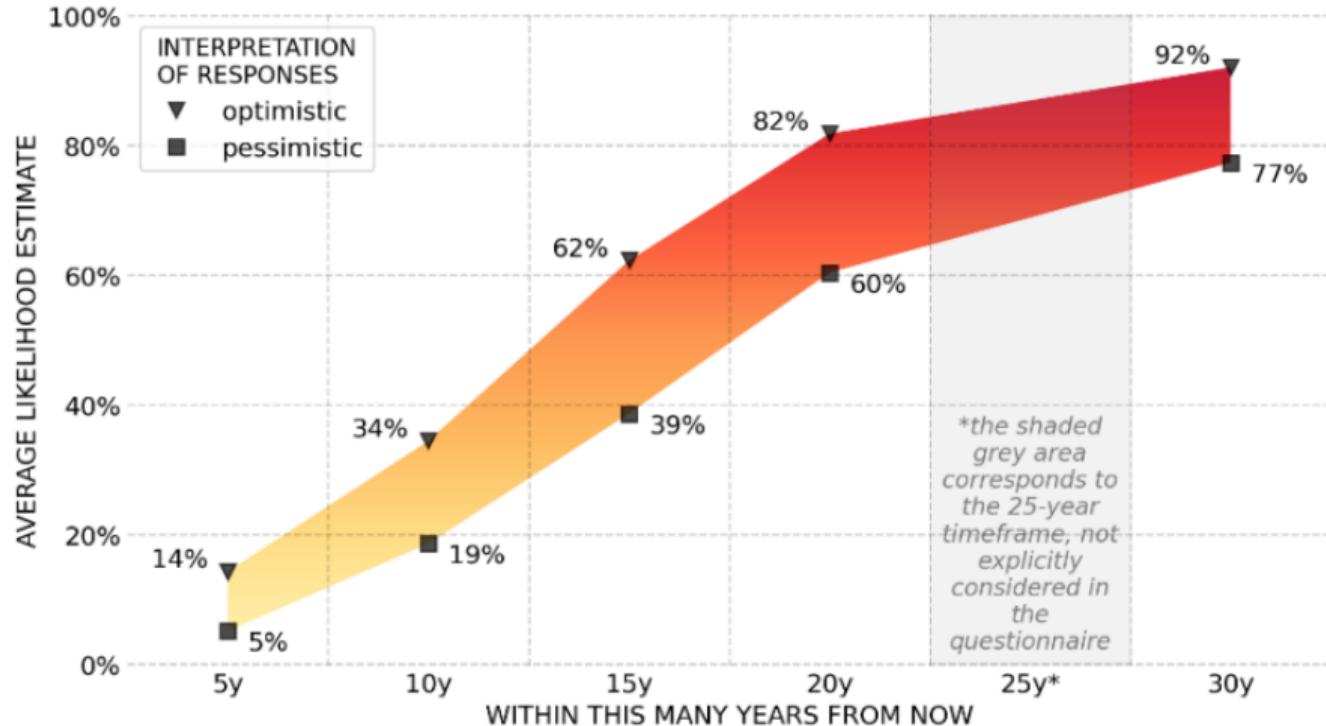
0.00 / 24:28 • Store Now, Decrypt Later (SNDE) ▶

How Quantum Computers Break The Internet... Starting Now

Veritasium Subscribed 333K Share Thanks Clip Save ...

9/20

Quantencomputer – So schnell wie Fusion



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

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: Classic McEliece: 1. PQ-Sichere Chiffre
- 1994: Kritische Quantenangriffe gefunden
- 2016: Wettbewerb angekündigt: PQ-Sichere Standardchiffren
- 2019: Experiment: PQ-Sicherheit auf öffentlichen Websites
- 2022: OpenSSH abgesichert
- 2023: Rosenpass veröffentlicht (WireGuard abgesichert)
- 2023: Signal Messenger abgesichert
- 2024: NIST-Wettbewerb: Erster Standard verabschiedet
- 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

- Rosenpass – VPN



- OpenSSH – Linux Server Administration
- Signal – Messaging
- mullvad.net – Internet Gateway (VPN Provider)



- **wolfSSL** WolfSSL – SSL/TLS, Web (Not standardized)