



Rosenpass

VPN & Struktur für Translationsforschung in der Kryptografie

Wanja Zaeske, Stephan Ajuvo, Marei Peischl,
Benjamin Lipp, Lisa Schmidt, Karolin Varner

<https://rosenpass.eu>



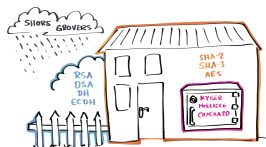
Das Rosenpass-Projekt

- Quantencomputer-sichere Kryptografie
- Forschung
- Ergebnisse in die Anwendung bringen
- Zusammenarbeit mit Industrie



Warum sind Quantencomputer (k)eine Bedrohung?

- Grovers Algorithmus **schwächt** symmetrische Kryptografie
 - AES, SHA-2, SHA-3, Chacha20
 - Lösung: größere Keys
- Shors Algorithmus **bricht** asymmetrische Kryptografie
 - RSA, DSA, DH, ECDH
 - Lösung: alternative Kryptografie
- Nur auf großen Quantencomputern
 - Die existieren noch nicht
 - Problem: Store now, decrypt later



Quantencomputer überschatten Kryptografieverfahren.

Sichere Kommunikation durch VPN

- Ermöglicht Sicherheit ohne Anpassung von Applikationen
- Protokoll: WireGuard



- Schnell
- Effizient
- Open Source
- Kompatibel
- Etabliert
- Problem: nutzt ECDH, also angreifbar!



Quantencomputer überschatten Kryptografieverfahren.



Wie löst Rosenpass das Problem?

- Basiert auf PQ-sicherer asymmetrischer Kryptografie
 - Classic McEliece
 - Kyber
- Benötigt: Public Key von anderen Peers
- Erzeugt: Shared Secrets zwischen Peers
- Angriff mit Quantencomputer nicht effizient
- Rosenpass, das Protokoll
 - Nutzt 3-Way Handshake
 - Secret wird alle 2 Minuten rotiert
 - Authentication, Secrecy und Integrity



PQ-sichere Kommunikation: WireGuard + Rosenpass

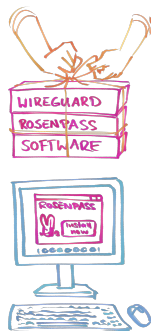
- Hybride Sicherheit
 - Bricht nur, wenn Rosenpass **und** WireGuard versagen
- Überall nutzbar, wo WireGuard schon läuft
- Ohne Anpassung vom WireGuard Source Code
 - Shared Secret aus Rosenpass = PSK für WireGuard
- Aber:
 - Ein Prozess mehr
 - Handshake alle 2 Minuten





Rosenpass Struktur

- Zusammenkunft von Kryptografie, Dev und SciComm Experten
- Idee: Team festigen
- Mittel: Rosenpass e. V.
 - Zusammenarbeit mit Industrie
 - Ansprechpartner für Integratoren
- Rosenpass Roadmap
 - Rosenpass in Embedded
 - Rosenpass in Datacenter
 - Integration in andere Apps
- Kryptografie + Safety Forschung
 - Decryption Despite Error



Anwendungsfälle.