



Bunny Rose against quantum attacks on cryptography!

Karolin Varner

<https://rosenpass.eu>



## The Plan

- 1. What is cryptography**
- 2. The end is neigh (quantum attacks)**
- 3. Migrating to post-quantum cryptography**
- 4. Advertisement (Migrating your own setup)**

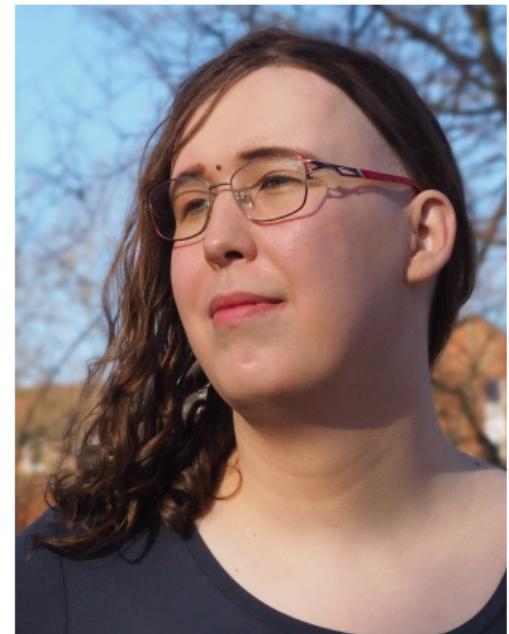


Slides

# Karolin Varner



- Initiator & Lead Scientist off Rosenpass e. V.
- Software-Developer & Cryptographer
- Worked for about 12 years in industry with start ups and large corps
- Working at Max-Planck-Institute for Security and Privacy since 2024
- Worked on Rosenpass & other cryptographic projects, such as teh X-Wing cipher



## Rosenpass e. V.



- Founded in 2023 as a host for the eponymous project
- Security WireGuard VPN against quantum attacks via protocol level hybridization
- Institution for translational research in cryptography
- Communication hub between science, industry, and civil society

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



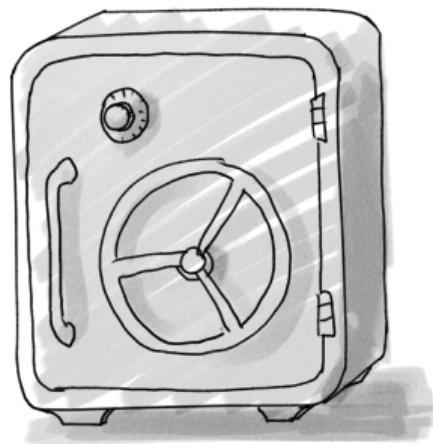
# What is Cryptography?



## Creating trustful communication spaces



Protecting privacy



Protecting belongings & capital



# Digital spaces, as trustful as the analog ones





## Data communication is usually public





## Data streams become gibberish

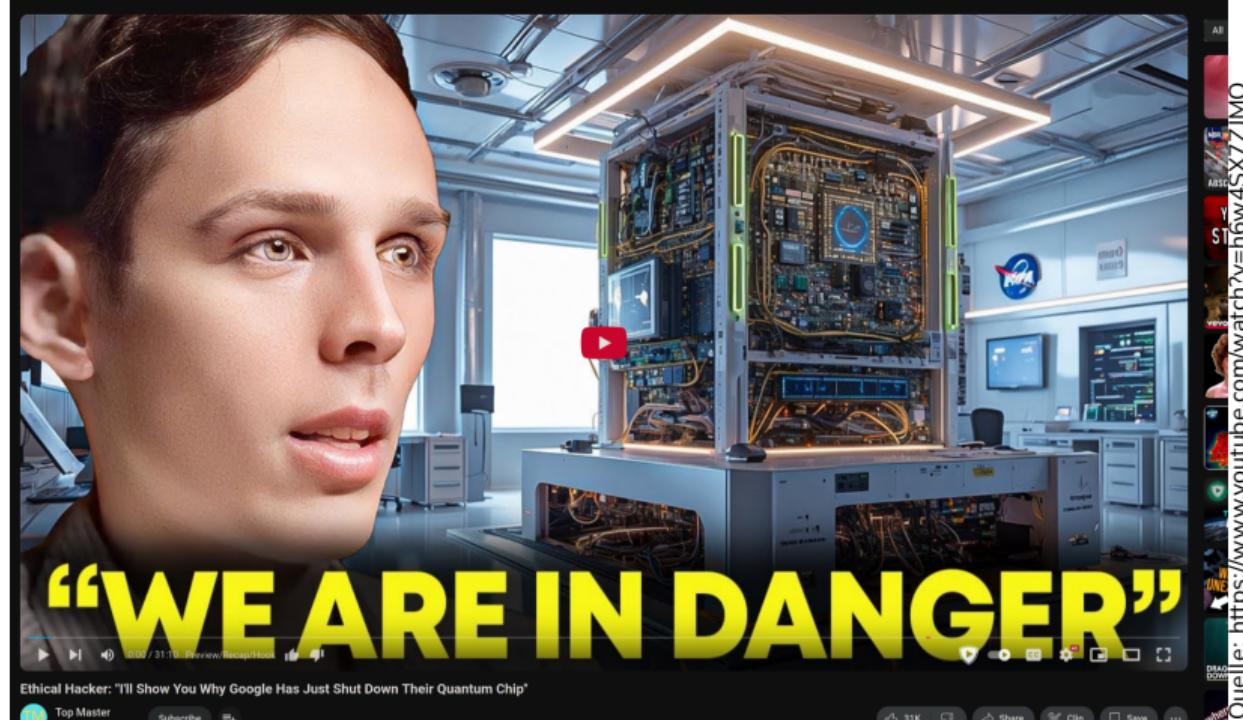


- Patient and doctor exchange a secret number
- Both computer use this number to encrypt & decrypt
- Patient and doctor can understand each other
- For everyone else, the data stream looks like gibberish (random)
- Well-made cryptography even protects info about who is communicating

The end is neigh (quantum attacks)



Doom sayers: “Please Like and Subscribe”





Doom sayers: “Please Like and Subscribe”





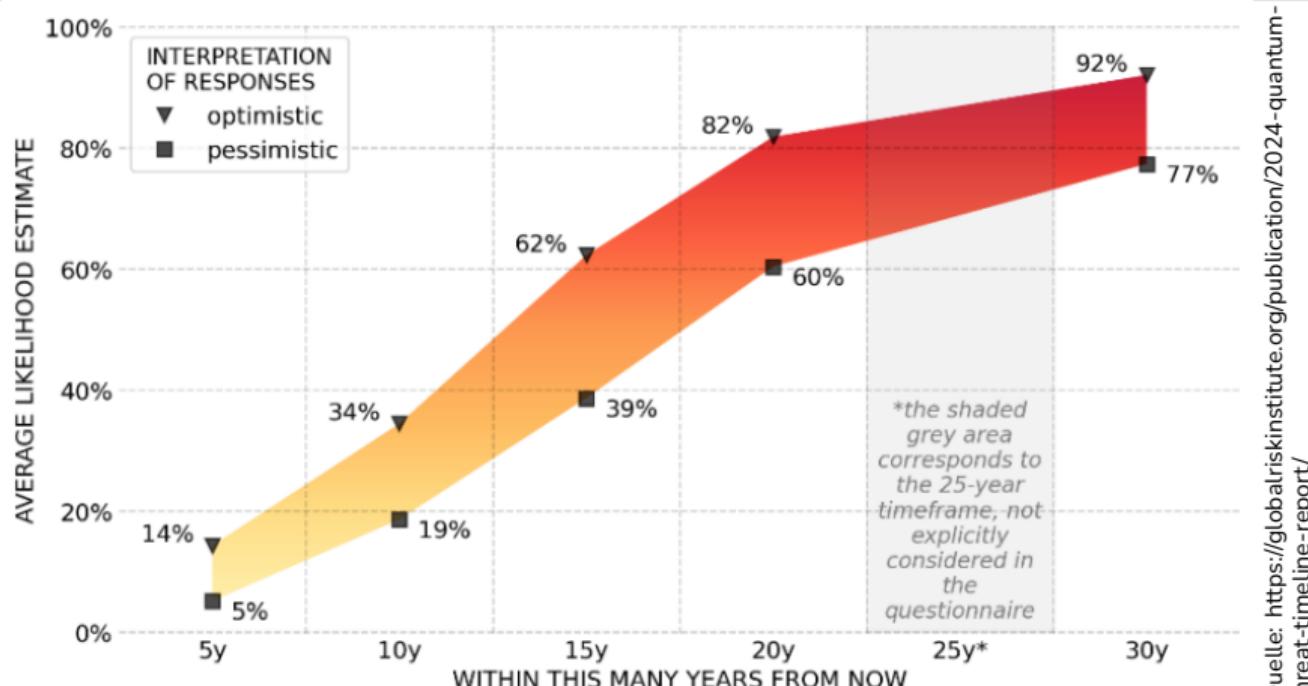
Doom sayers: “Please Like and Subscribe”



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



# Quantum computing – As soon as we have fusion power



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



## When networked world stops turning



- We work on the internet
- We manage critical infrastructure
- Our supply chains depend on it



## Hoarding hamster attacker

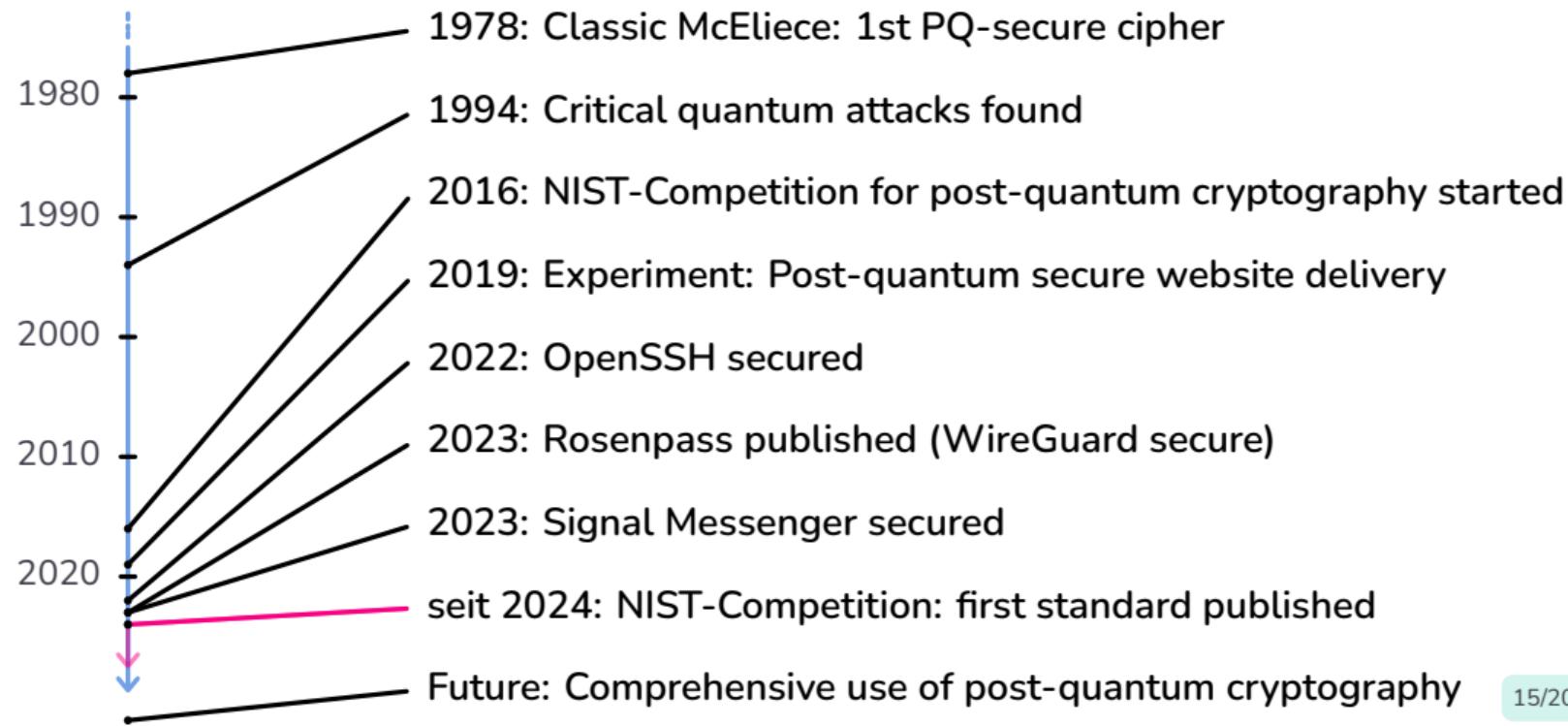
- Angreifer hoard encrypted communication
- This enables attacking past communication
- “Store now, decrypt later Attack”



# Migrating to post-quantum security



## Migrating to post-quantum security



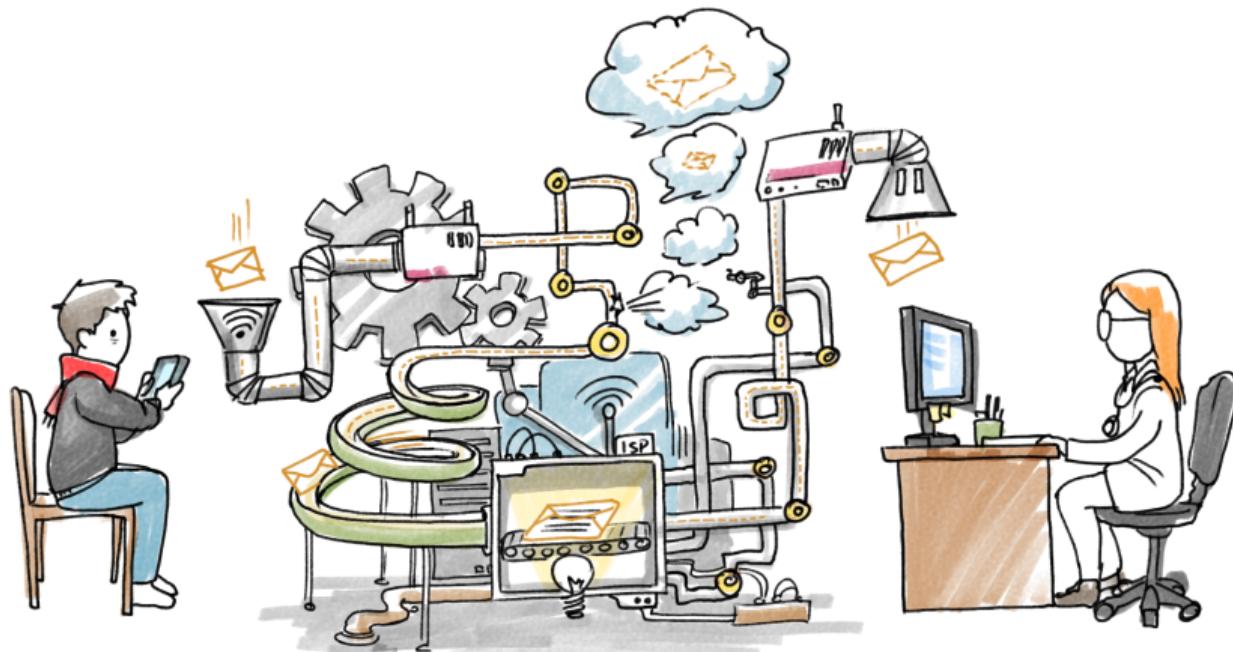


## System complexity is a major challenge





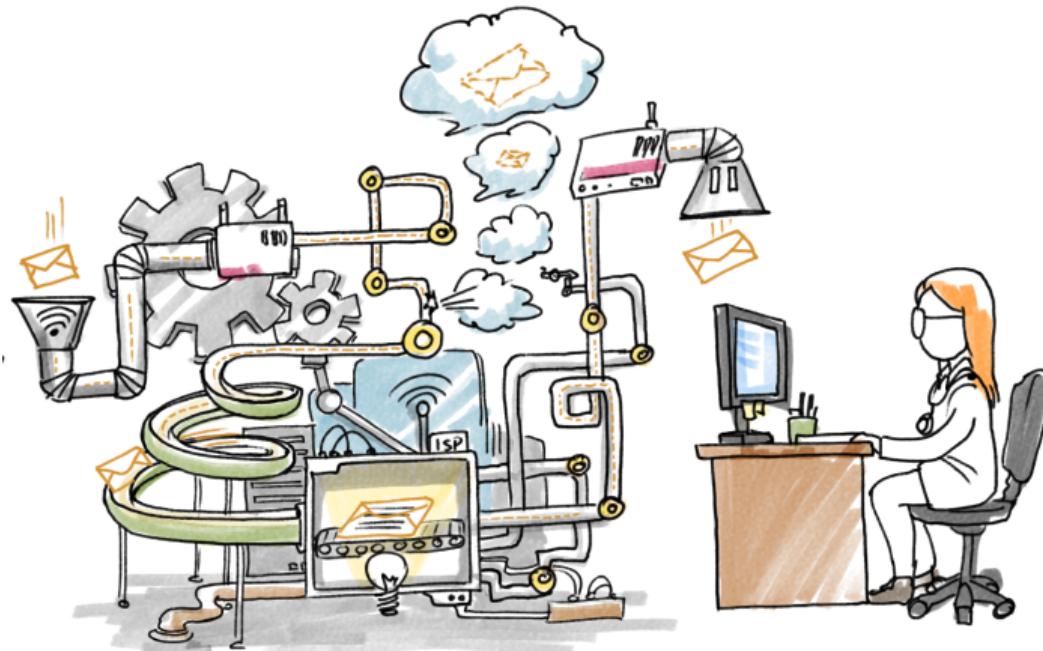
## System complexity is a major challenge





## System complexity is a major challenge

- Our cryptographic infrastructure is a massive mess of components
- We don't even precisely know which components are used
- Almost all must be migrated





# Kryptoagilität

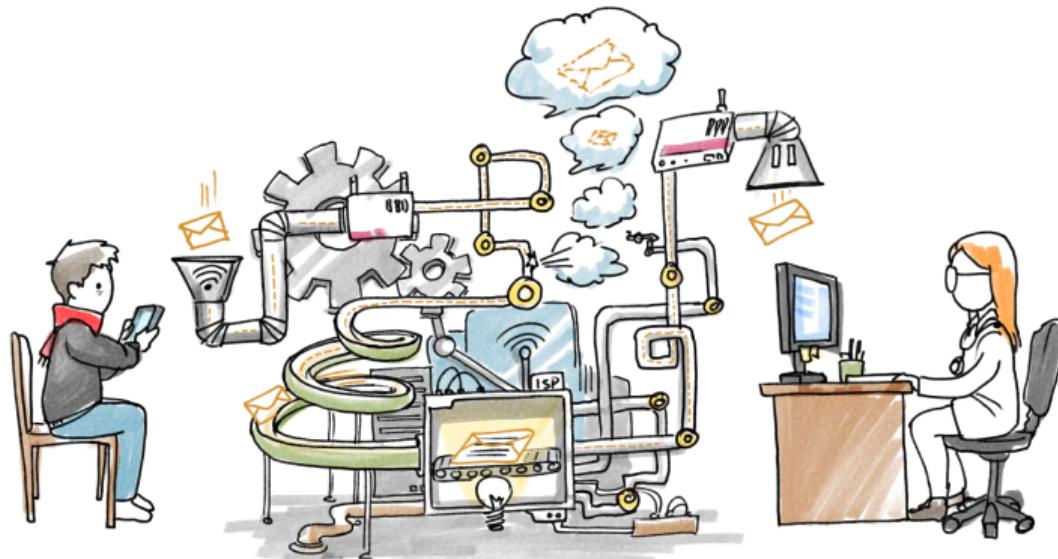


- Document existing cryptographic infrastructure
- Introduce procedures for rapid upgrades
- Sustainable & enduring

# Advertisement!

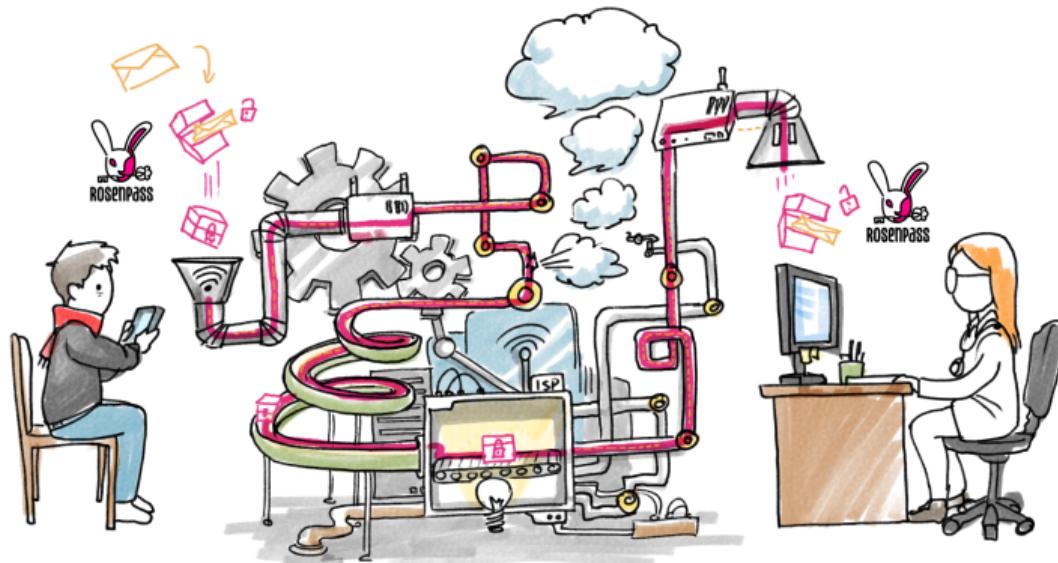


# PQ-Security without replacing infrastructure





# PQ-Security without replacing infrastructure



The VPN-advantage: Adding post-quantum-security on top

Bunny Rose against quantum attacks on cryptography!



OpenSSH  
Linux Server  
Administration



mullvad.net  
Internet Gateway  
(VPN Provider)



Signal  
Messaging



wolfSSL  
SSL/TLS, Web  
(Not standardized)