QR.N-Workshop II
2025-12-05

Plug and Play – How to enter the Quantum Internet without Fuzz, Buzz, or KMS

Karolin Varner
https://rosenpass.eu

Rosenpass e. V. (and me, Karolin Varner)

- Initiator & Lead Scientist of Rosenpass e. V.
- We are at intersection of science, business and infrastructure
- **Research**: Cryptography, protocol design, key exchanges
- **Product**: Rosenpass, which upgrades the WireGuard VPN to post-quantum security
- **Specialty**: Explaining cryptography. How to think about the technology?

rosenpass.eu

What do we want?

What do we want?

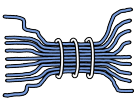
data communication

How do we want it?

securely

Specifically?

post-quantum secure



	QKD	Guards	Crypto.
E2E-Security	✗	✓[1]	✓
Auth.	✓[2]	✓[1]	✓
Commodity Hardware	✗	✗	✓
Data Rates	kb	Any	Any
Everlasting Secrecy[3]	(✗)[4]	(✓)[1]	(✓)[5]

[1] Assuming resistance against sneak attacks

[2] Through Wegman-Carter

[3] Information-Theoretic Security, the lack of algorithmic hardness assumptions

[4] Not at these data rates

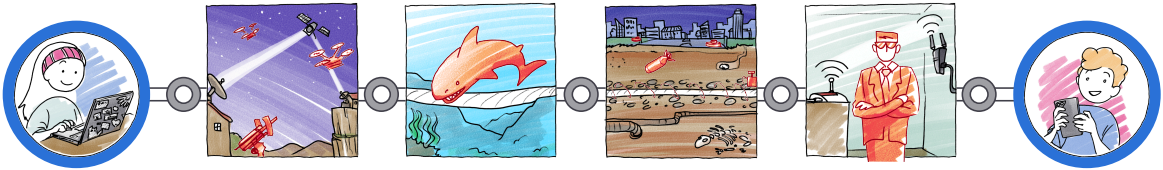
[5] With a suitcase of hard drives containing keys

How to secure the internet against quantum attacks?

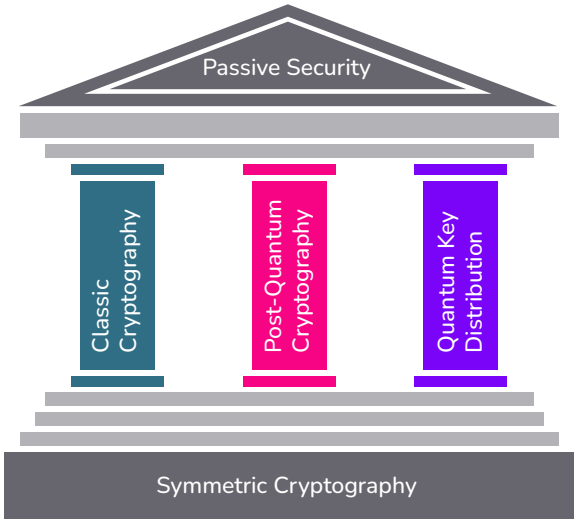
With computational cryptography

How do we think about QKD then?

Conceptualize QKD



QKD as measure of hardware security.



QKD: A fail-over in case Post-Quantum Cryptography fails.

What do we want?

secure data communication

Where do we want it?

on highly secure institutional networks

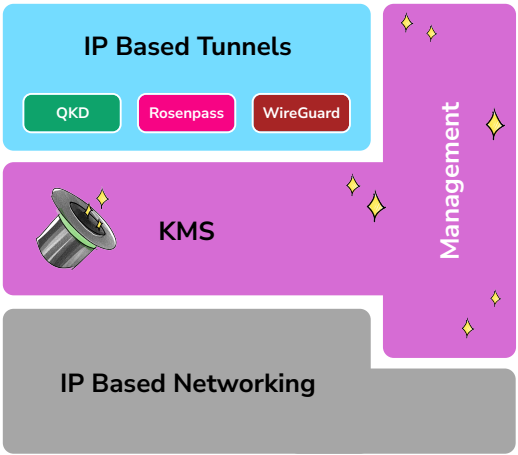
In what particular manner?

with hardware security measures

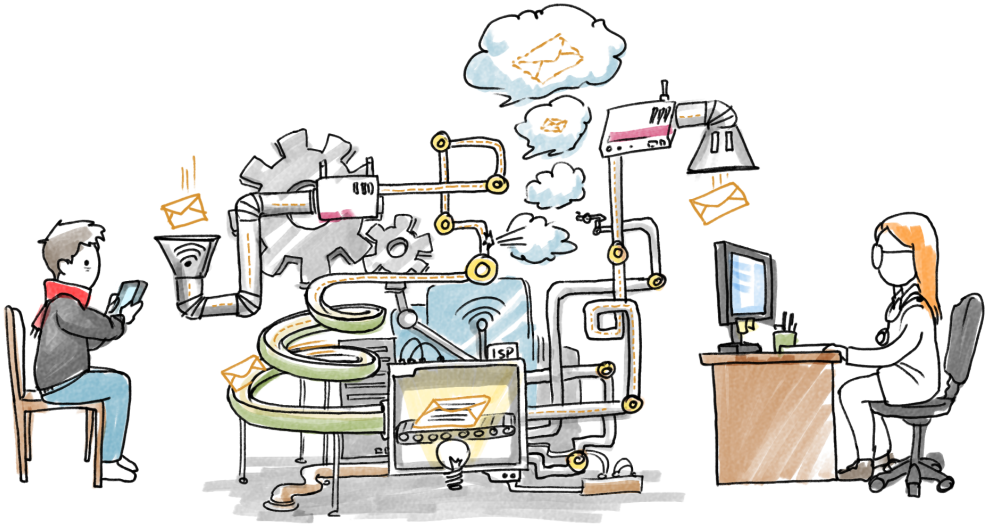
especially QKD

How do we build it?

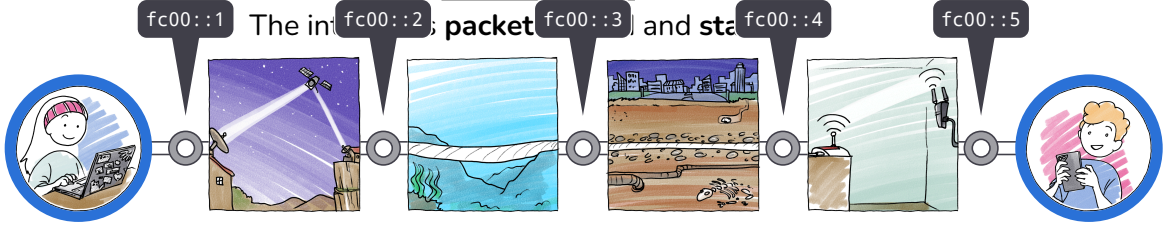
How about a key management system?



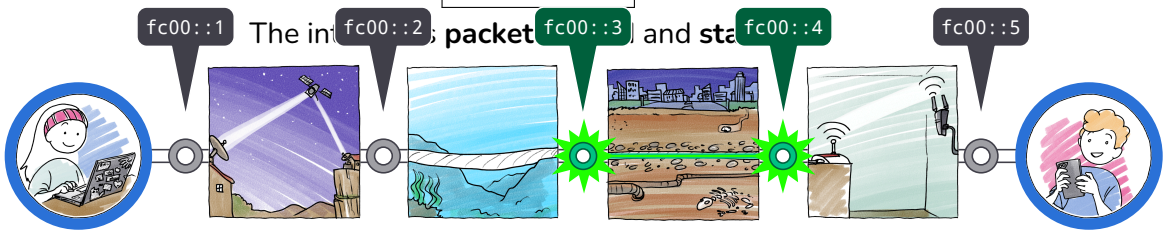
- Pretty expensive
- Pretty complicated
- Still requires IP-based networking
- One compromised node compromises the entire network
- Does not address how to create data channels



Key management systems evoke the image of a rube-goldberg machine.



The internet is an architecture for **transport-agnostic** networking.



Then QKD is just another transport technology, with extra security features.

That’s a wrap, problem solved!

With internet standard technologies:

- **SRv6** to fully control the routes packages take
  ...even if nodes not on the path are compromised.
- **HNCP** to learn the network topology
  ...and to automatically deploy networks in the first place.

Doing this securely means we need secure routing.

And we need end-to-end hybrid computational security.
For instance using Rosenpass for post-quantum security and WireGuard for classical security.

Ingress to egress security can substitute for end to end security in corporate environments

...so the technology does not have to be installed on every old windows laptop.

Comparing the architectures

With internet standard technologies:

- QKD becomes just another transport
- KMS replaced with HNCP (observability) and SRv6 (secure routing)
- Management application package ties this into a neat bundle

Additional features:

- Interoperability with the normal internet
- Hardware security measures other than QKD supported

This is in fact a Key Management System

Keys sent on a secured path, gain the security properties of the secured path.

So we can implement a KMS, if we really want to, by exposing an API that chooses a random key, then transmits it.

Information theoretic security: supported if the transports do support it.

Quantum repeaters: Just a special type of transport, no distinction for the network.

What about a proper QKD-enabled internet?

Do not reinvent the wheel, use established routing protocols: Build an extension to IPv6, that can transmit QKD keys alongside packages.

We are collaborating with Quantum Optics Jena to realize this

Key takeaways

Key takeaways:

- QKD is a hardware security measure, not a replacement for cryptography
- Focus on secure data paths, not on key forwarding in complex networks
- We can use or extend standard internet technologies, to build the quantum internet