**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**

# Karolin Varner

- Initiator & Lead Scientist of Rosenpass e. V.
- We are at intersection of science, business and infrastructure
- **Expertise**: Cryptography and internet engineering
- **Research**: Cryptography, protocol design, key exchanges
- **Product**: Rosenpass, which upgrades the WireGuard VPN to post-quantum security
- **Collaborate**: With businesses and other institutions towards deployment of cutting-edge cryptography
- **Specialty**: Explaining cryptography. How to think about the technology?

**rosenpass.eu**

# What do we want?

What do we want?

What do we want?
Data communication

What do we want?
Data communication
Securely

What do we want?
Data communication
Securely
Something something quantum

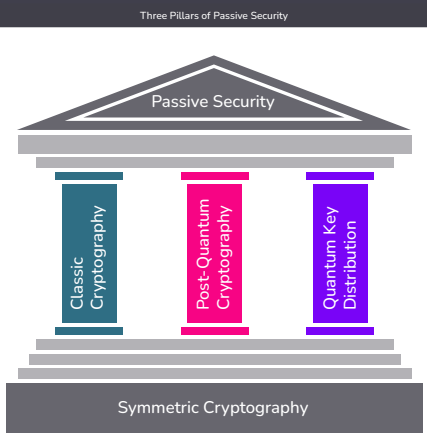
| | QKD | Computational Cryptography |
|---|---|---|
| End to End Security | No | Yes |
| Authentication | Yes[1] | Yes |
| Commodity Hardware | No | Yes |
| Data rates | kilobits | Arbitrary |
| Information-theoretic security[2] | (No)[3] | (Yes)[4] |

[1] Through Wegman-Carter
[2] Everlasting Secrecy, the lack of algorithmic hardness assumptions
[3] Not with these data rates
[4] With a suitcase of hard drives containing keys

# How to secure the internet against quantum attacks


With computational cryptography!

# How to think about quantum key distribution?




As a fail-over in case Post-Quantum Cryptography fails.

# Data streams become gibberish


PLACEHOLDER
As a hardware-security measure.

What do we want?

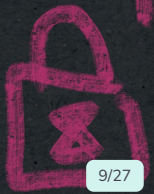
What do we want?
Data communication

What do we want?
Data communication
on highly secure institutional networks

What do we want?
Data communication
on highly secure institutional networks
with hardware security measures
especially QKD

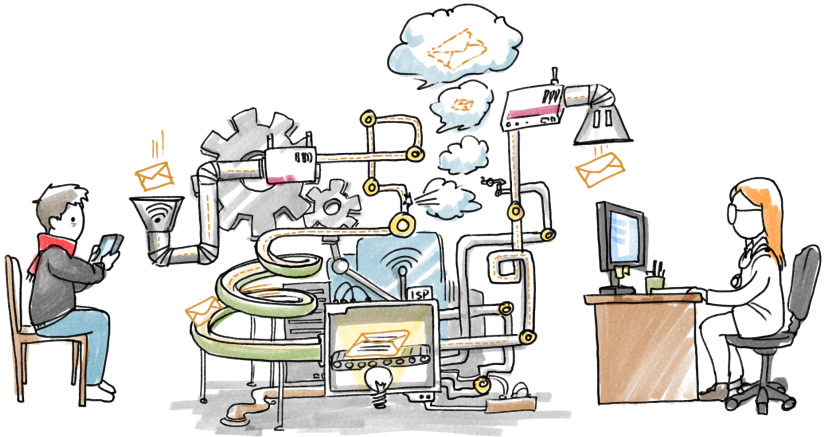
What do we want?
Data communication
on highly secure institutional networks
with hardware security measures
especially QKD
interoperable with the internet

# 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.

PLACEHOLDER

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

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

# The end!

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
- Key management systems are overcomplicated and not actually needed
- We can use or extend standard internet technologies, to build the quantum internet