QR.N-Workshop II
2025-12-05

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

Karolin Varner, Lisa (mullana) Schmidt
https://rosenpass.eu

Rosenpass e. V., Lisa Schmidt, Karolin Varner

Scientific Illustration:
Lisa (mullana) Schmidt

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

What do we want?

What do we want?

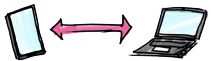
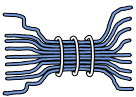
data communication

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

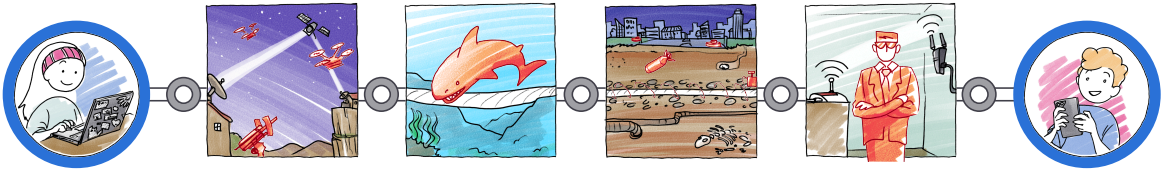
[5]With a suitcase of hard drives containing keys

How to secure the internet against quantum attacks?

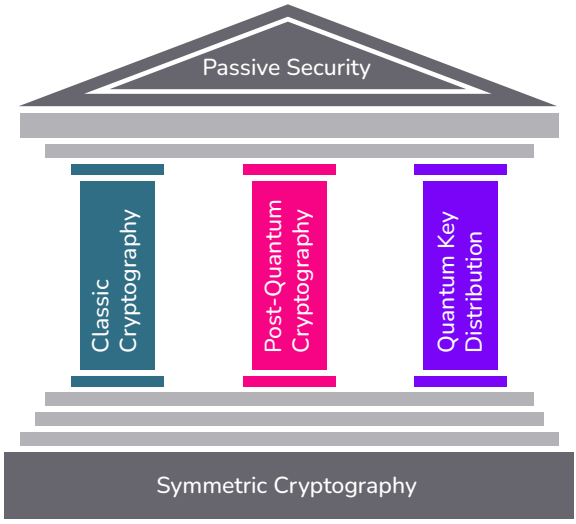
With computational cryptography

How do we think about QKD then?

Conceptualize QKD



QKD as a 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

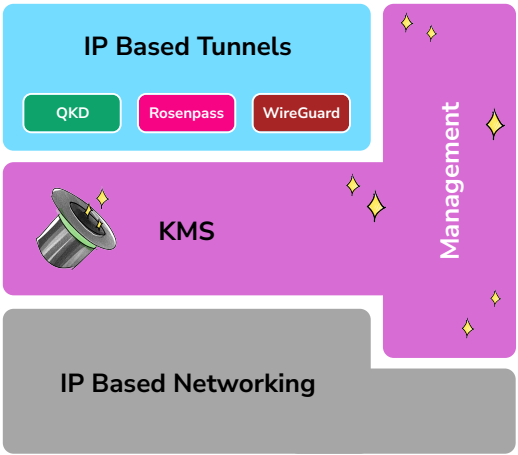
In what particular manner?

with hardware security measures

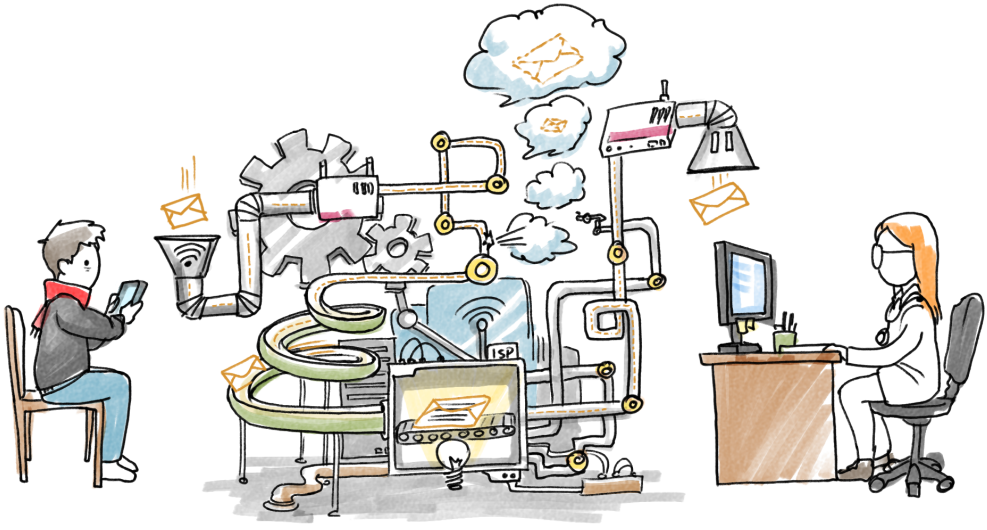
especially QKD

How do we build it?

How about a key management system?

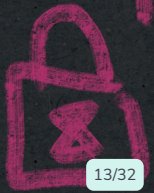


- Pretty expensive
- Pretty complicated
- Still requires IP-based networking
- One compromised node compromises the entire network
- Does not address how to create data channels

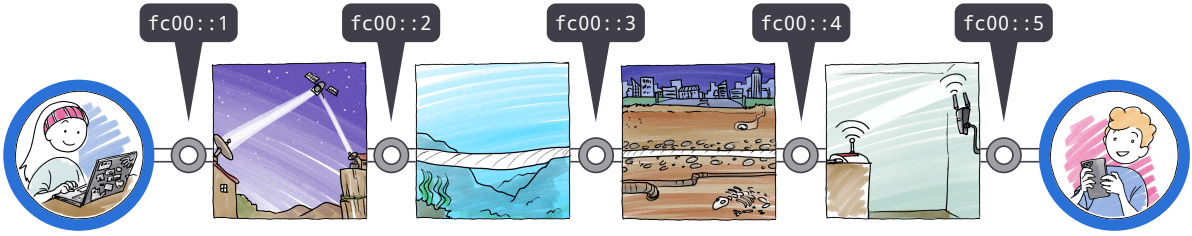


Key management systems evoke the image of a Rube Goldberg machine.

Back to the basics: What was the internet again?

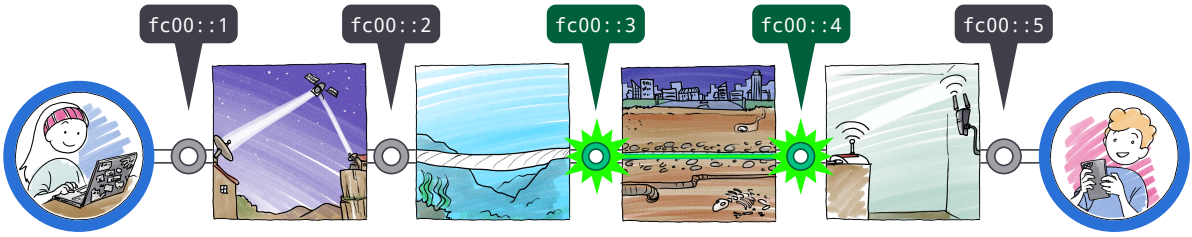


The internet is **packet-routed** and **stateless**.



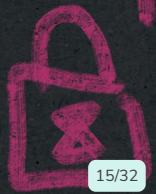
The internet is an architecture for **transport-agnostic** networking.

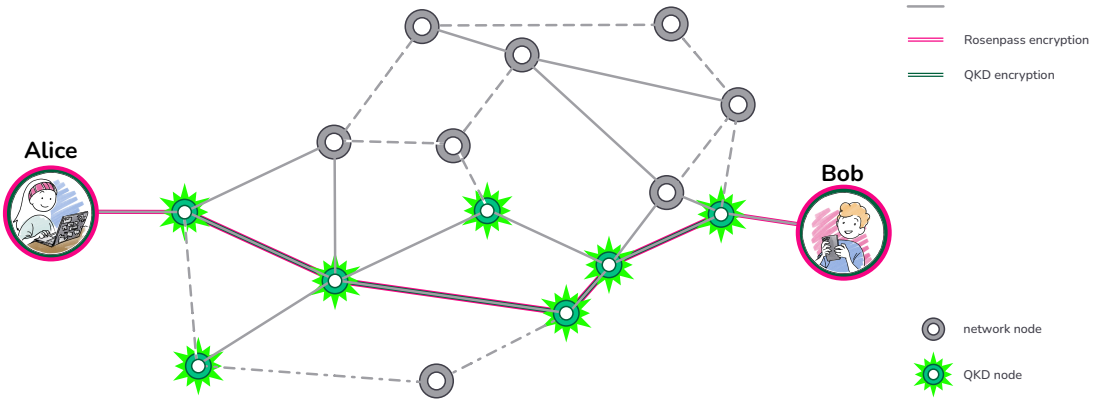
The internet is **packet-routed** and **stateless**.



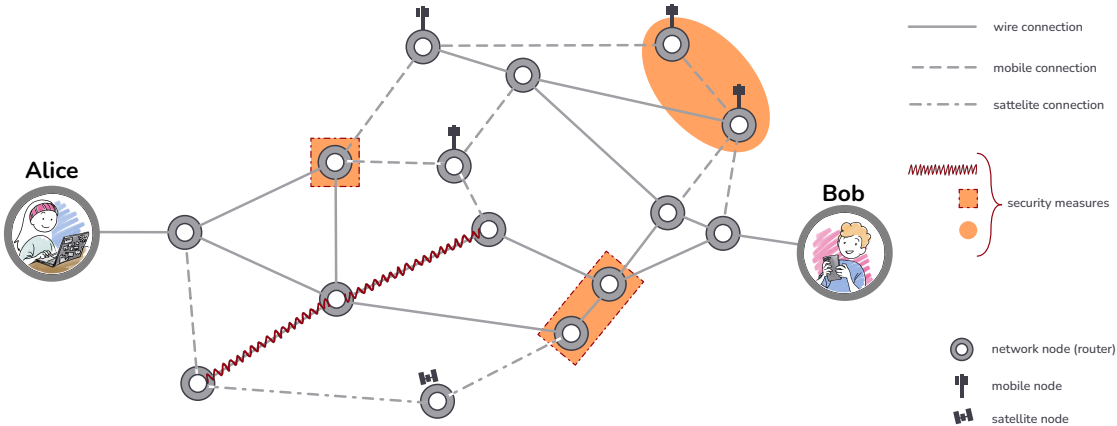
Then QKD is just another transport technology, with extra security features.

That’s a wrap, problem solved!





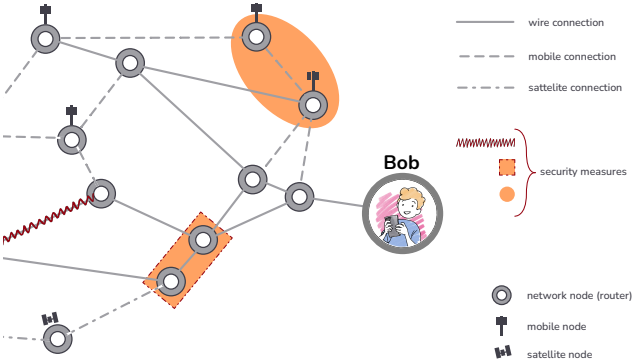
To do this safely and securely, we need **secure routing** (for safety) and **E2E**-encryption (for security).



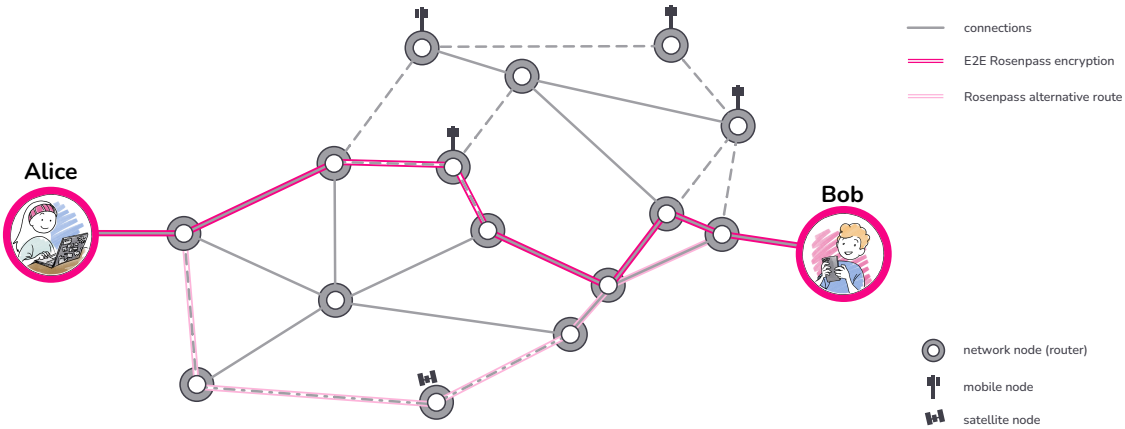
Secure routing detects and avoids *accidentally insecure* routes.

With internet standard technologies:

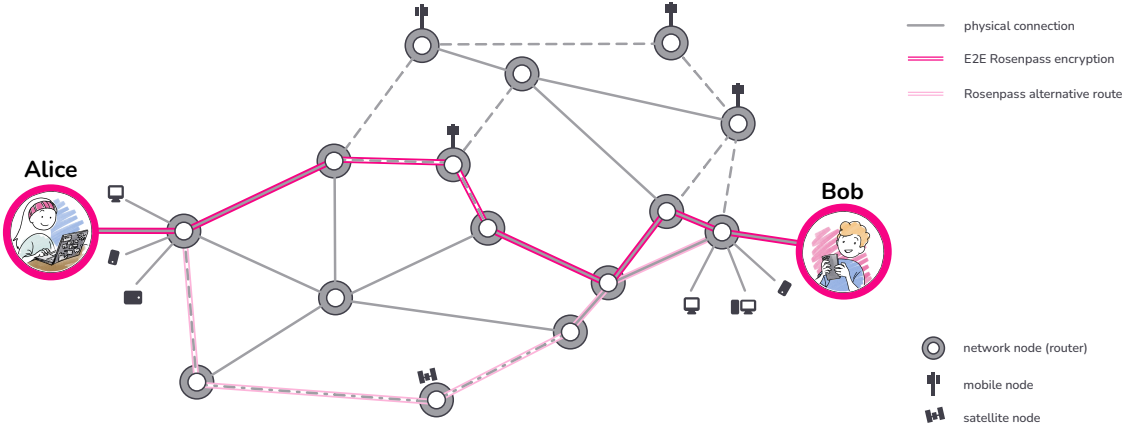
- **SRv6** to fully control the routes packages take
  … even if nodes not on the path are compromised.
- **HNCP** to learn the network topology
  … and to automatically deploy networks in the first place.



Secure routing detects and avoids *accidentally insecure* routes.

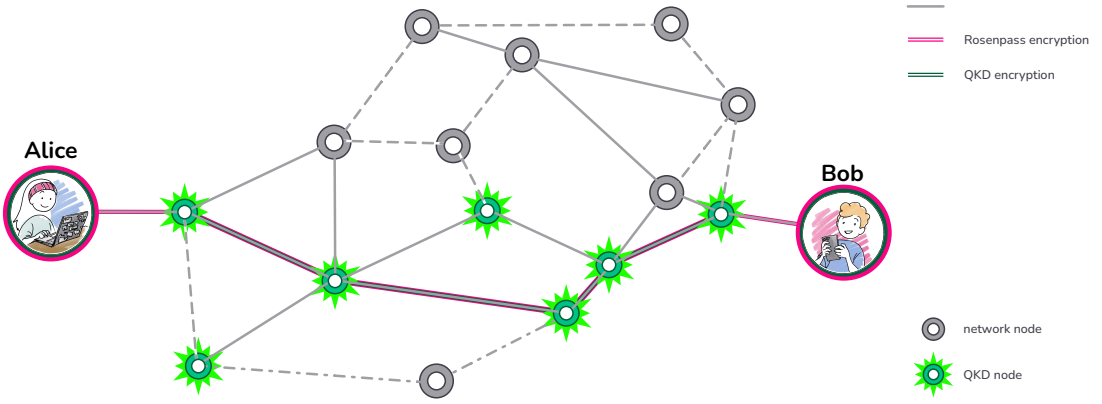


And we need end-to-end cryptography for security.
For instance, using Rosenpass for post-quantum security and WireGuard for classical security.



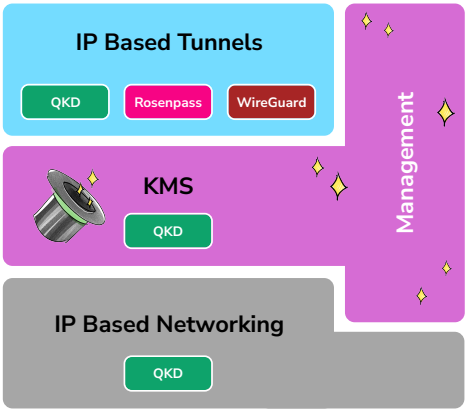
Ingress-to-egress security can substitute for end-to-end security in corporate environments

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

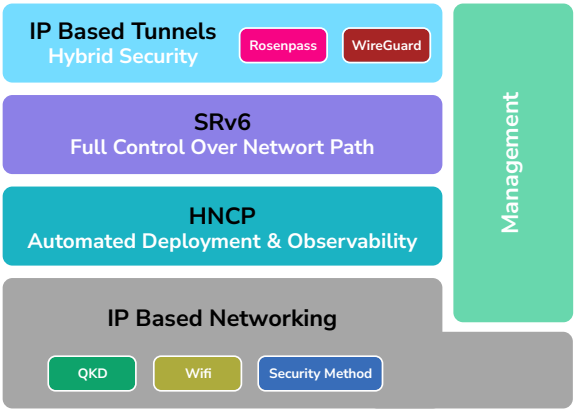


Here is what it might look like if a properly secure connection is established.
Note how secure routing invalidates the backup route, because it's not QKD secured all the way.

KMS-Based Architecture



Networking-oriented architecture

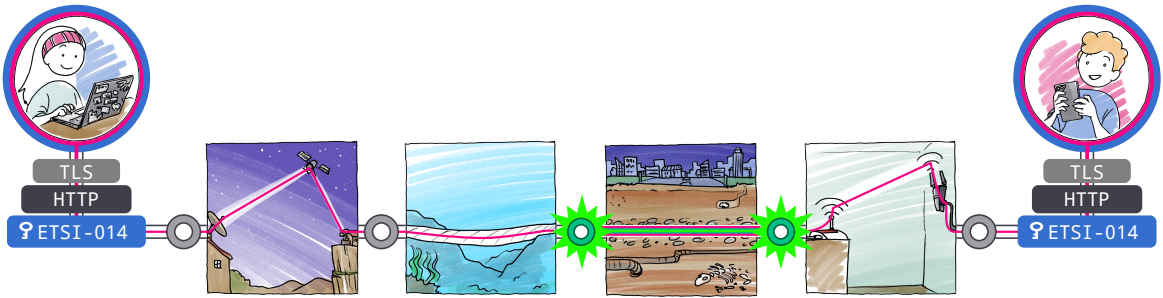


QKD becomes just another transport: SRv6, HNCP, and tunnels for added safety & security.

We now support: automatic network deployment; hardware security other than QKD supported; interoperability with the internet.

This is in fact a Key Management System

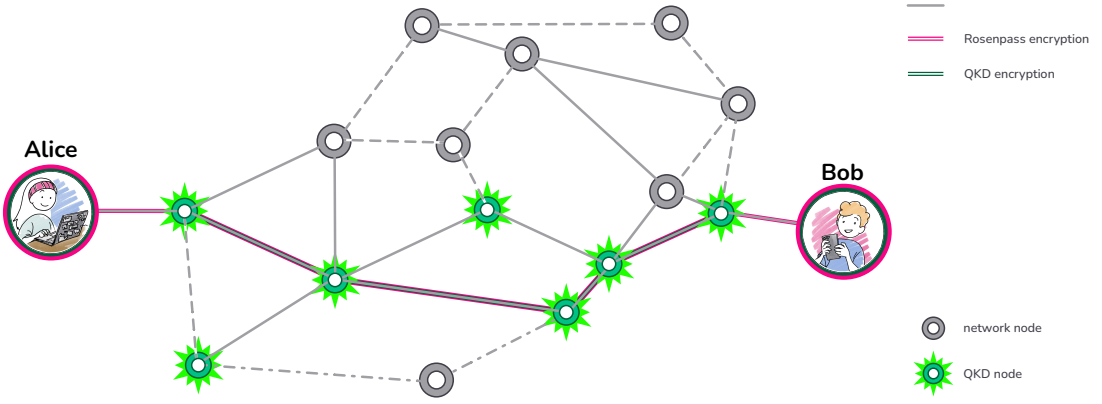
KMS by API adapter



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

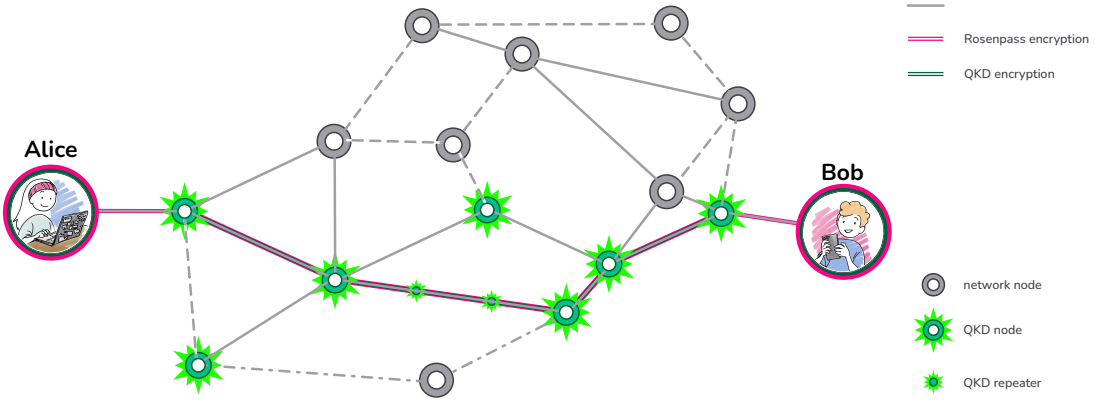
We can implement a KMS by exposing an API that chooses a random key, then transmits it.

The plan data path is almost always more useful.



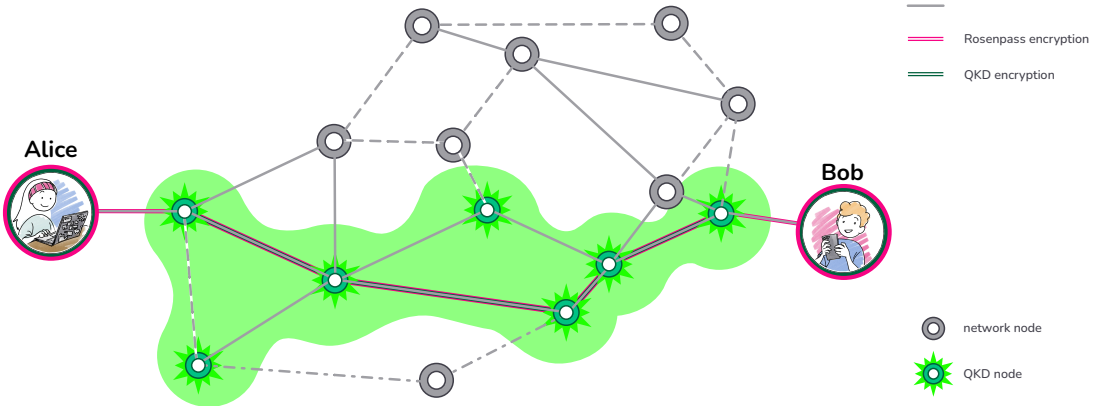
Information theoretic security: No distinction; supported if the transports do support it.

(All transports must use One-Time-Pad with Wegman-Carter auth based on QKD-Keys).



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.

Advertisement

Collaborating with Quantum Optics Jena

WireGuard: For classical security

Rosenpass: For post-quantum security

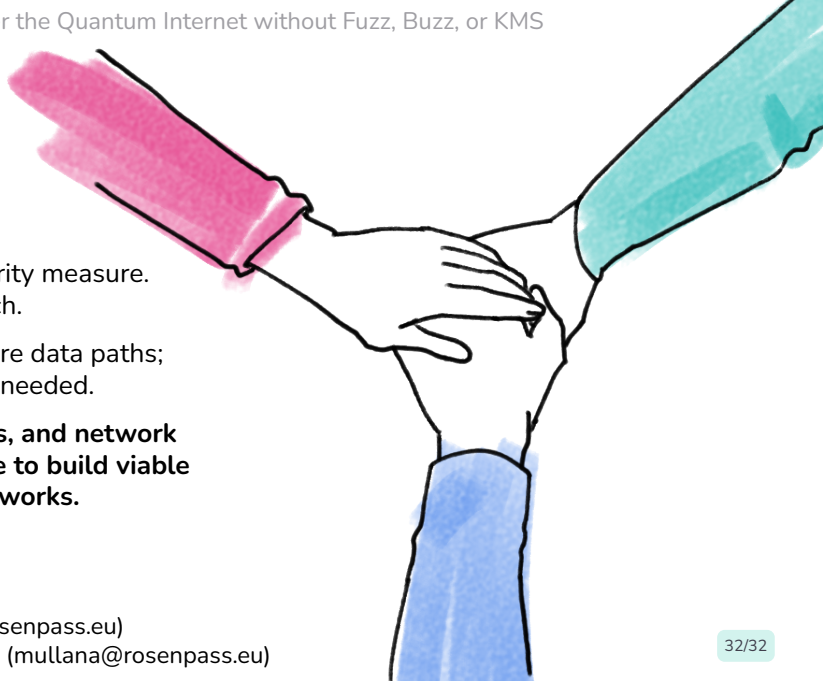
QOJ QKD devices: For QKD support

HNCP: For network observability and automatic network deployment.

SRv6: For secure routing support

QUANTUM OPTICS
JENA

Key takeaways



QKD is a hardware security measure.
Treat it as such.

Focus on connecting secure data paths;
build KMS on top if needed.

Physicists, cryptographers, and network engineers must collaborate to build viable QKD-enabled networks.

Rosenpass e. V. ~ rosenpass.eu
Speaker: Karolin Varner (karo@rosenpass.eu)
Scientific Illustration: Lisa Schmid (mullana@rosenpass.eu)