



Plug and Play – How to enter the Quan-  
tum 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](http://rosenpass.eu)

# What do we want?

What do we want?

**data communication**

How do we want it?

**securely**

Specifically?

**post-quantum secure**

	<b>QKD</b>	<b>Bricks</b>	<b>Crypto.</b>
End to End Security	No	Yes	Yes
Authentication	Yes <sup>1</sup>	Yes	Yes
Commodity Hardware	No	No	Yes
Data rates	kilobits	Arbitrary	Arbitrary
Information-theoretic security <sup>2</sup>	(No) <sup>3</sup>	(Yes) <sup>4</sup>	(Yes) <sup>5</sup>

<sup>1</sup> Through Wegman-Carter

<sup>2</sup> Everlasting Secrecy, the lack of algorithmic hardness assumptions

<sup>3</sup> Not with these data rates

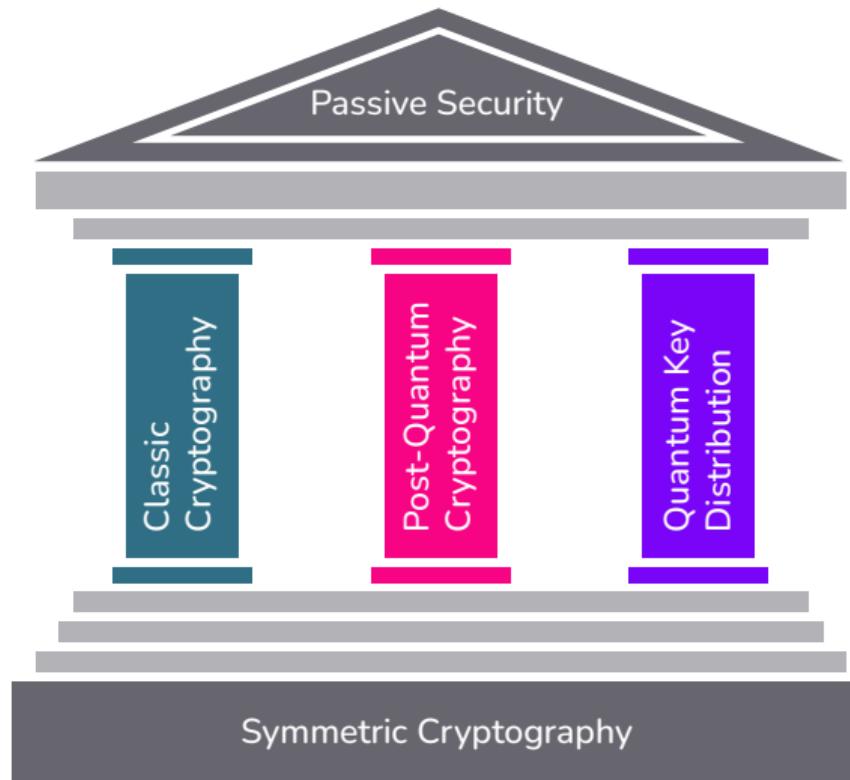
<sup>4</sup> Assuming pressure hammer attacks are detected

<sup>5</sup> 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?



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

PLACEHOLDER

**QKD:** A measure of hardware security.

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**

Anything else else?

**interoperability with the internet**

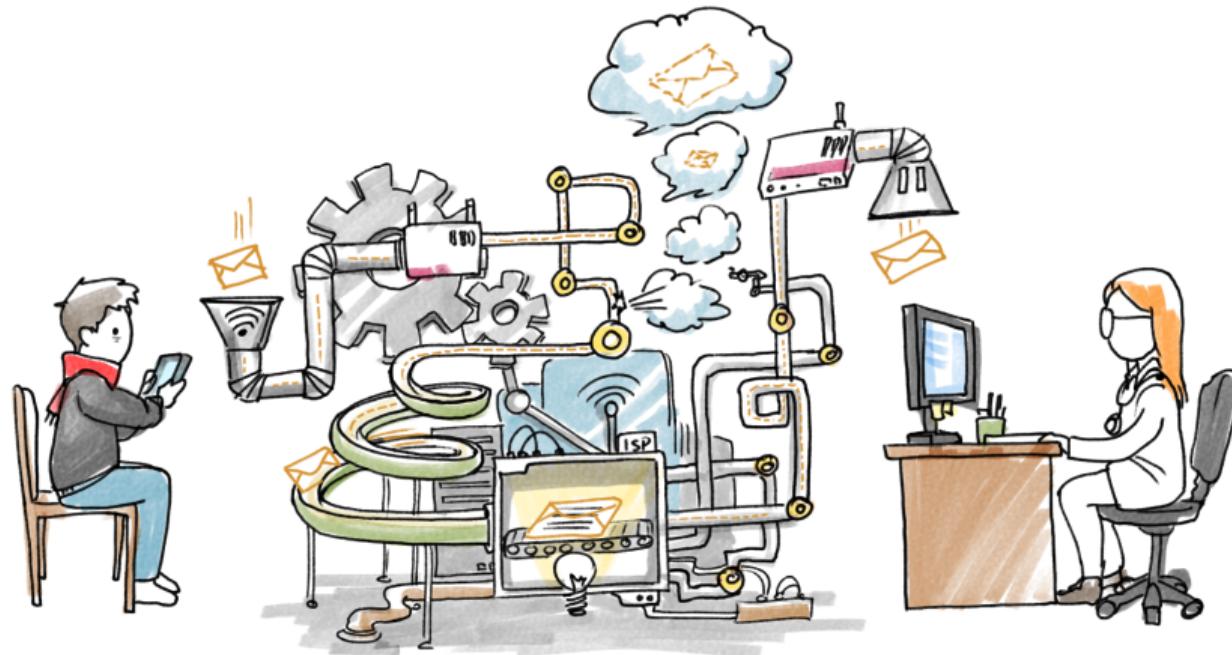
# How do we build it?



## 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.

That's a wrap, problem solved!



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
- Open Source, Open Source, Open Source
- We can use or extend standard internet technologies, to build the quantum internet