Workshop on Entanglement Assisted Communication Networks

2024-09-20


# Computational, Authenticated Key Distribution

Encryption the old-fashioned way

**Karolin Varner**

with support from Benjamin Lipp, Lisa Schmidt, and Marei Peischl

**https://rosenpass.eu**

# Computational, Authenticated Key Distribution

Software Encryption...

- ...secures communication using modest computational resources.
- ...is deployed on a vast number of devices.

Follow the talk at:
rosenpass.eu/docs/ presentations/eacn-2024/

# Computational, Authenticated Key Distribution

Software Encryption...

- ...is superior to QKD in most respects.
- ...can benefit from the inclusion of QKD.

Follow the talk at:
rosenpass.eu/docs/ presentations/eacn-2024/

# Rosenpass

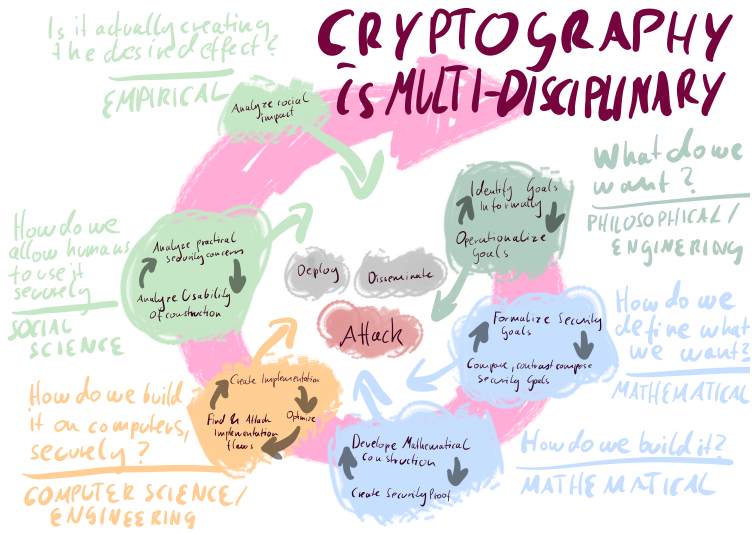
I am the main author of Rosenpass.

- A post-quantum secure key exchange
- A real-world application used to secure WireGuard against quantum attacks
- An organization for doing translation research in cryptography

**rosenpass.eu**

# About cryptology

# To build real-world cryptography solutions



# Proofs of security are fundamental: Reduction proofs


Proof by reduction to a well-known mathematical problem *assumed to be hard* or existing cryptographic construction *assumed to be secure*.

**If** an attack against my cryptosystem exists,
**then** this other cryptosystem can be attacked or this math problem can be solved.

Proof ad-absurdum:

- Assume an attacker against the new cryptosystem exists
- Construct a solution to the underlying math problem using the assumed attacker

# Proofs are fundamental: Using information theory

Showing that each *plain text* is plausible for each *ciphertext*.

Cryptosystem should be formulated as a function:

$$F : K \times D \to C$$

- $K$ Key material; secret information held by the trusted parties
- $D$ Protected information
- $C$ Leaked information; any information known to the attacker after protocol execution

Now it needs to be shown, that for every value of the leaked information, every value of the protected information is equally plausible.

$$\forall c : C, d_1 : D, d_2 : D; |\{k \in K | F(k, d_1) = c\}| = |\{k \in K | F(k, d_2) = c\}|$$

# Proofs are fundamental: Implementation security


## Functional Correctness

Using formal methods from computer science that a cryptographic implementation is functionally equivalent to its specification.

## Efficiency

Using complexity theoretic analysis to ensure that the implementation can not be slowed down by an attacker.

## Implementation security

Ensuring cryptographic implementation fulfill various extra security properties. For example:

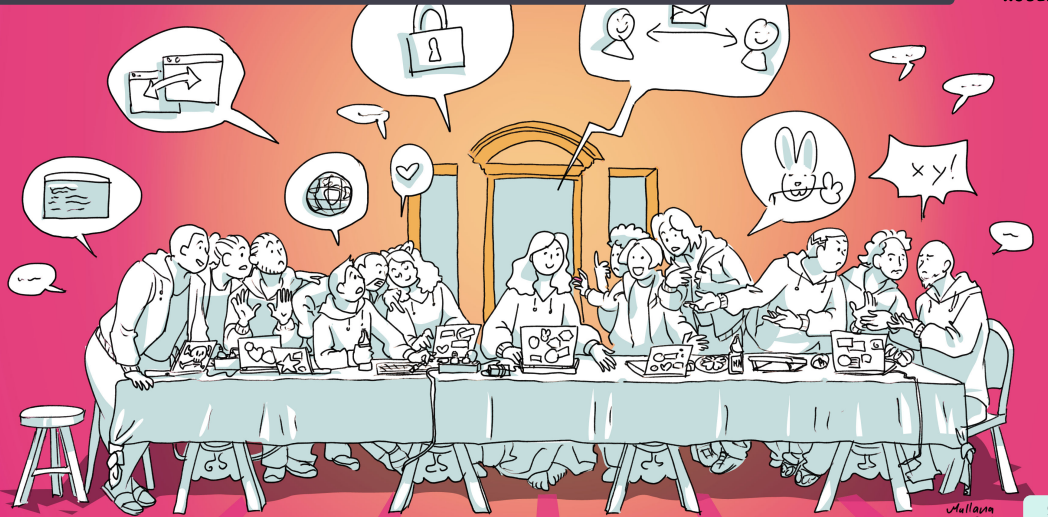
- Timing side-channel resistance
  certain assembly operations are forbidden
- Memory-safety
  advanced programming languages such as Rust to avoid bugs such as buffer-overflows

# Practical security is essential


It is not enough to build a system that is secure in theory but vulnerable on real hardware. Some dangers include:

- Timing side-channels
- Power side-channels
- Hardware bugs in the CPU (Rowhammer, Spectre, or Meltdown)
- Lack of usability (Implementations that are easy to misuse)

# Implementations and specifications must be open

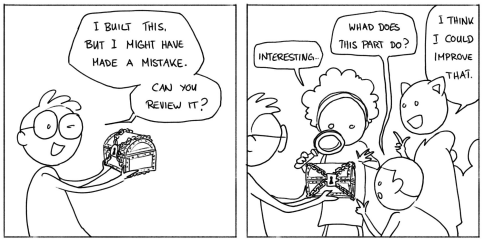


# Open-Source & Open-Science are mandatory


Keeping details about a security system secret creates mistrust and risks obscuring obvious security flaws

# Open-Source & Open-Science are mandatory

Cryptography is about creating trust; so peer review and open processes are a crucial part of the process.



# More than encryption


Key-exchanges are a subfield in cryptography, not the whole thing!

**Censorship circumvention** to ensure all people can use encryption

Multi-Party Computation Arbitrary computation on encrypted data without cheating by consortium

Homomorphic Encryption Arbitrary computation on asymmetrically encrypted data

Robust Combiners Redundancy in cryptographic systems

Private Information Retrieval Databases without leakage about user activity

# To integrate QKD in cryptology

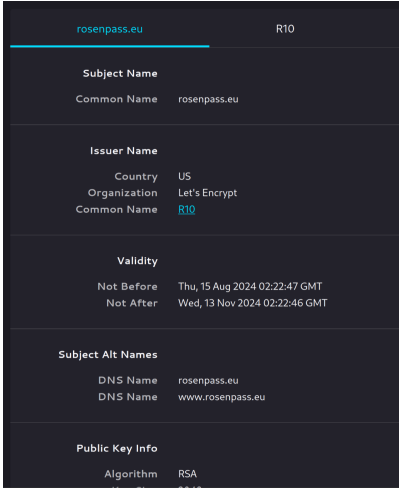

- Integrate with community of cryptography researchers
- Use open-source/open-science approach
- Define security properties in cryptographic terms to be comparable
- **Use QKD within cryptographic systems**

# Secure Channels

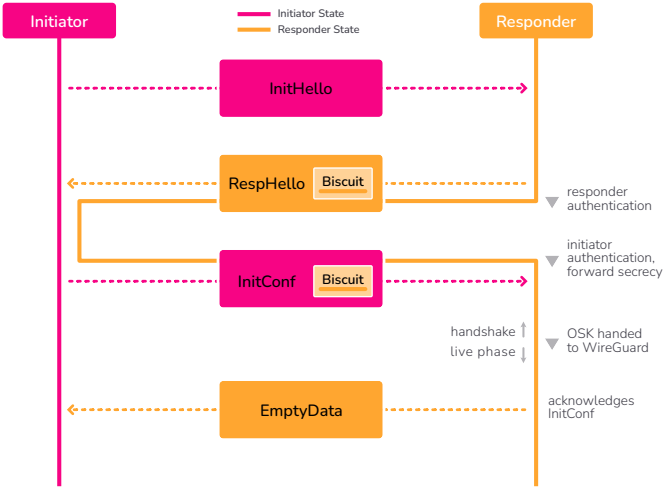
# Secure Channel Protocols

Secure channel protocols like TLS, OpenSSH, or the Noise Protocol Framework [NOISE] are used everywhere on the internet. They are

- Cheap
- Fast
- Secure
- Well analyzed
- Authenticated
- Usually not secure against quantum attacks



# Security against quantum attacks




- Migration to post-quantum security is possible
- Rosenpass (pictured) is an example
- Some deployed systems are already doing partial migration (e.g. OpenSSH, Signal Messenger)

# Secure channels: Security Properties

# Passive attacker are eavesdropping

# Active attackers are intercepting

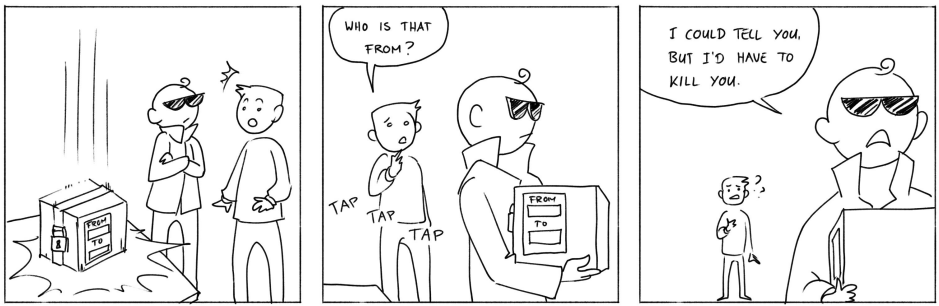
# Secrecy


The data being transmitted must never be leaked.

# Authenticity

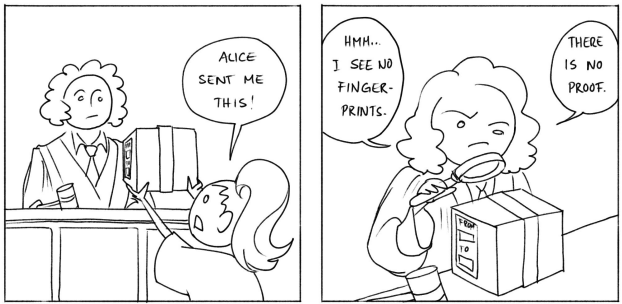

Sender and receiver must be certain about each others identity.

# Identity hiding



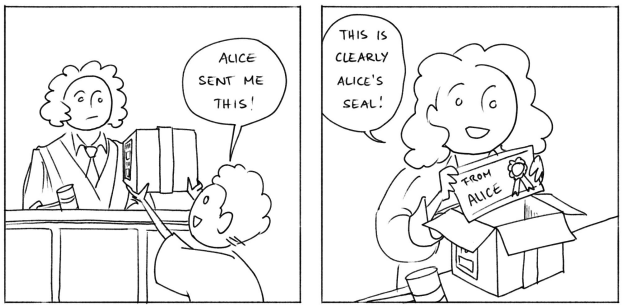

The data being transmitted must not leak sender and recipient identities (although the metadata may).

# Deniability




The receiver must be unable to prove (mathematically) what data the sender had transmitted to allow for informal communication.

# Non-Repudiation



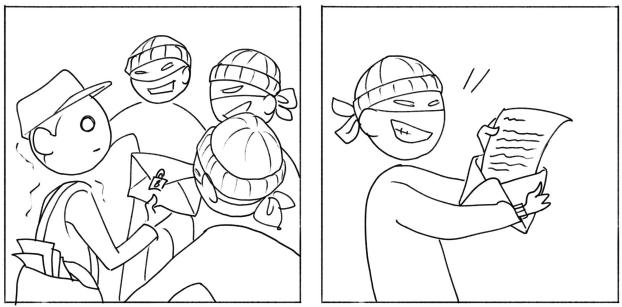

Sometimes it is appropriate instead to ensure that the recipient can prove what the sender had sent them.

# Forward secrecy

An attacker must not be able to decrypt past communication by breaking into the server:

An extra asymmetric keypair is generated on the fly and immediately shredded after the key exchange.

# Forward secrecy

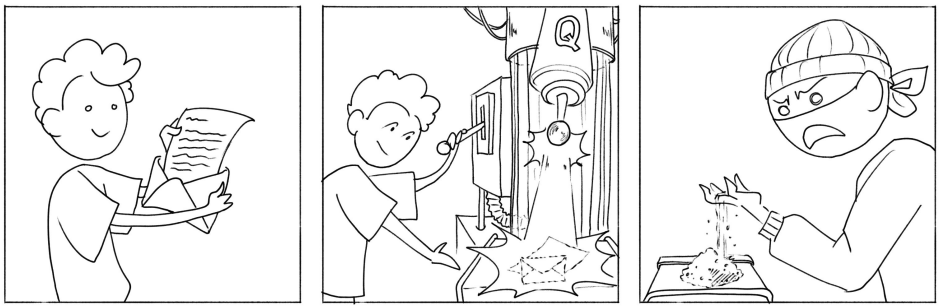


Which is no help against active attackers – interception – though.

# Forward secrecy

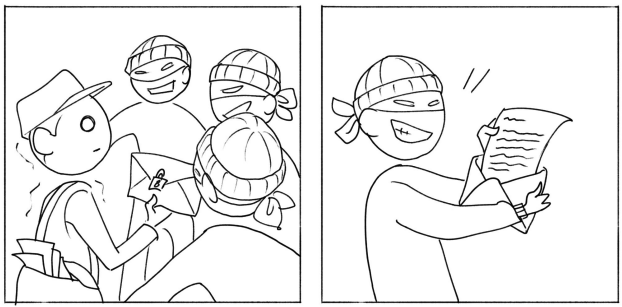
Nor against future attacks against the cryptographic schemes themselves.

# Everlasting secrecy (QKD)




It would be great to be able to defend even against future attacks against cryptography.

# Everlasting secrecy (QKD)



Though even QKD can not help against interception, which is why we will always need cryptography.

# QKD is impractical and insufficient

| Security property | QKD | Software encryption |
|---|---|---|
| Post-Quantum | ✓ | ✓ |
| Forward-secrecy | ✓ | ✓ |
| Everlasting-Secrecy | Impractical | ✗ |
| End-2-End | Impractical | ✓ |
| Active Attackers | ✗ | ✓ |
| Authenticity | ✗ | ✓ |
| Deniability | ✗ | ✓ |
| Non-repudiation | ✗ | ✓ |
| Identity hiding | ✗ | ✓ |

QKD is...

- Expensive
- Inefficient
- Everlasting secrecy would be nice, but is impractical for real-world setups
- Multi-hop security is impractical
- End-2-end security is missing entirely (no QKD on my end-user device fiesable for now)

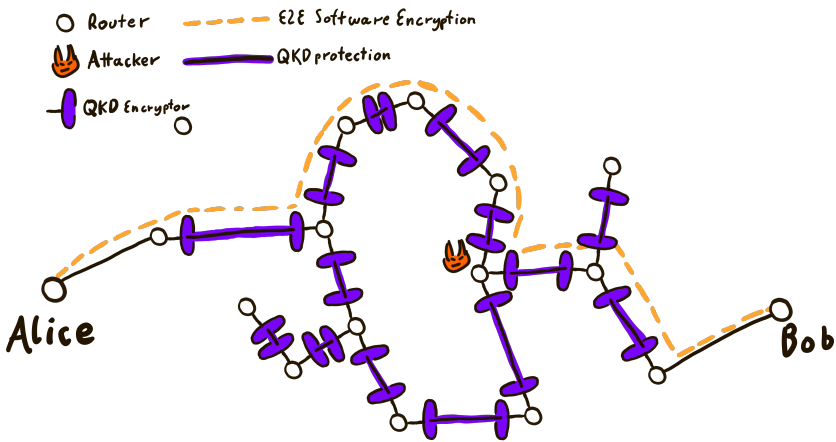
# Redefining QKD Success

# Three Pillars of passive Security

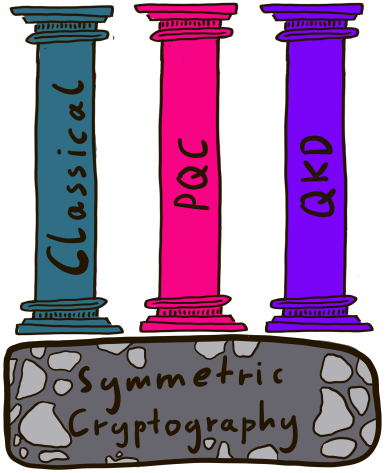

- As a measure of redundancy against future flaws in asymmetric cryptography.
- As a method of improving hardware security.

If you would build a wall around your fiber, you might as well use QKD which could be cheaper.

# Hybrid setups using QKD and end to end connections



# Three Pillars of passive Security




- As a measure of redundancy against future flaws in asymmetric cryptography.
- As a method of improving hardware security.

If you would build a wall around your fiber, you might as well use QKD which could be cheaper.

# Appendix — Here Be Dragons

# Bibliography


[PQWG]: https://eprint.iacr.org/2020/379

[GHP]: https://eprint.iacr.org/2018/024

[HPKE]: https://eprint.iacr.org/2020/1499 (analysis) &
https://www.rfc-editor.org/rfc/rfc9180.html (RFC)

[XWING]: https://eprint.iacr.org/2024/039

[NOISE]: https://noiseprotocol.org/noise.html

[BR06]: https://eprint.iacr.org/2004/331

[Hal05]: https://eprint.iacr.org/2005/181

[MK-KEM]: https://csrc.nist.gov/pubs/fips/203/final

# Graphics attribution


- https://unsplash.com/photos/brown-rabbit-Efj0HGPdPKs
- https://unsplash.com/photos/barista-in-apron-with-hands-in-the-pockets-standing-near-the-roaster-machine-Y5qjv6Dj4w4
- https://unsplash.com/photos/a-small-rabbit-is-sitting-in-the-grass-1_YMm4pVeSg
- https://unsplash.com/photos/yellow-blue-and-black-coated-wires-iOLHAIaxpDA
- https://foto.wuestenigel.com/gray-hamster-eating-sunflower-seed/
- https://unsplash.com/photos/gray-rabbit-XG06d9Hd2YA
- https://unsplash.com/photos/big-ben-london-MdJq0zFUwrw
- https://unsplash.com/photos/white-rabbit-on-green-grass-u_kMWN-BWyU
- https://unsplash.com/photos/3-brown-bread-on-white-and-black-textile-WJDsVFwPjRk
- https://unsplash.com/photos/a-pretzel-on-a-bun-with-a-blue-ribbon-ymr0s7z6Ykk
- https://unsplash.com/photos/white-and-brown-rabbit-on-white-ceramic-bowl-rcfp7YEnJrA