Co-funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

LINUX ENCRYPTOR OF NETWORK TRAFFIC

CA5: Post-Quantum Cryptography

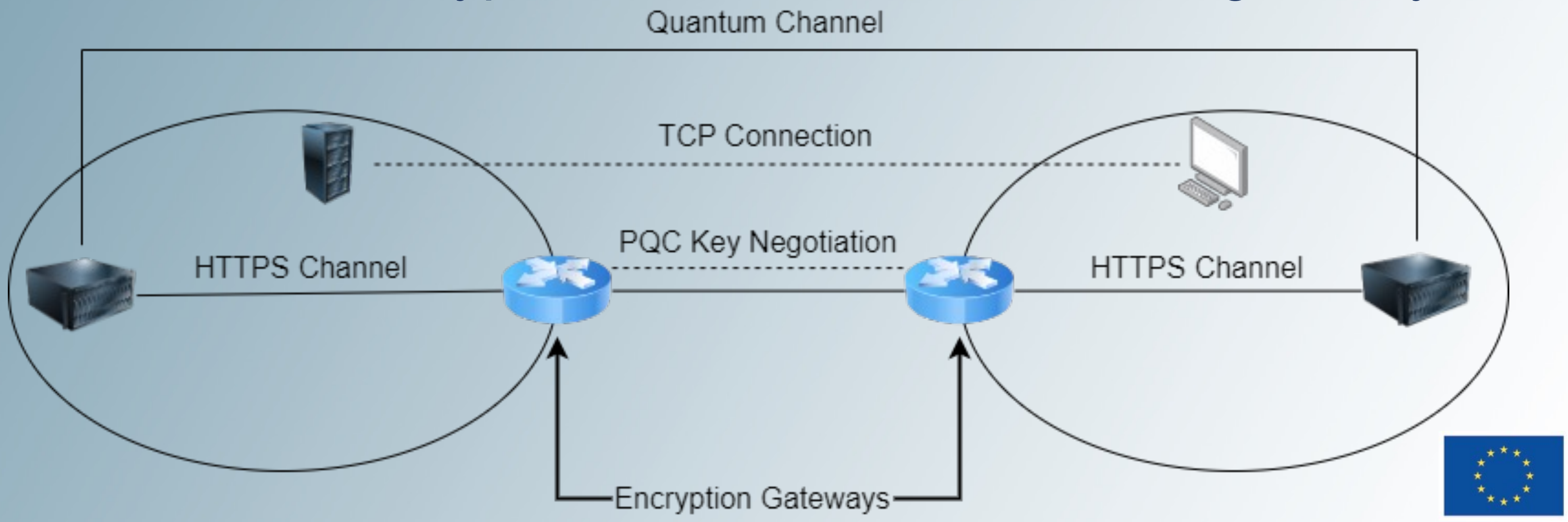
Jan Hajny, hajny@vut.cz

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Overview

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Originally a student project at Brno University of Technology, CZ
- Goal of this subproject is to create Linux implementation of IPv4 network traffic encryptor using quantum resistant algorithms.
- Network encryptors serve as inter-network gateways.



Co-funded by the European Union

Gateway Properties

- Network traffic routed using virtual interfaces
- Packet-by-packet encryption in tunnel mode
- 60 bytes packet expansion – MTU decrease needed
- Encrypted traffic is wrapped in UDP and sent to port number 62 000
- Other traffic is considered to be unencrypted

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Used Algorithms

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

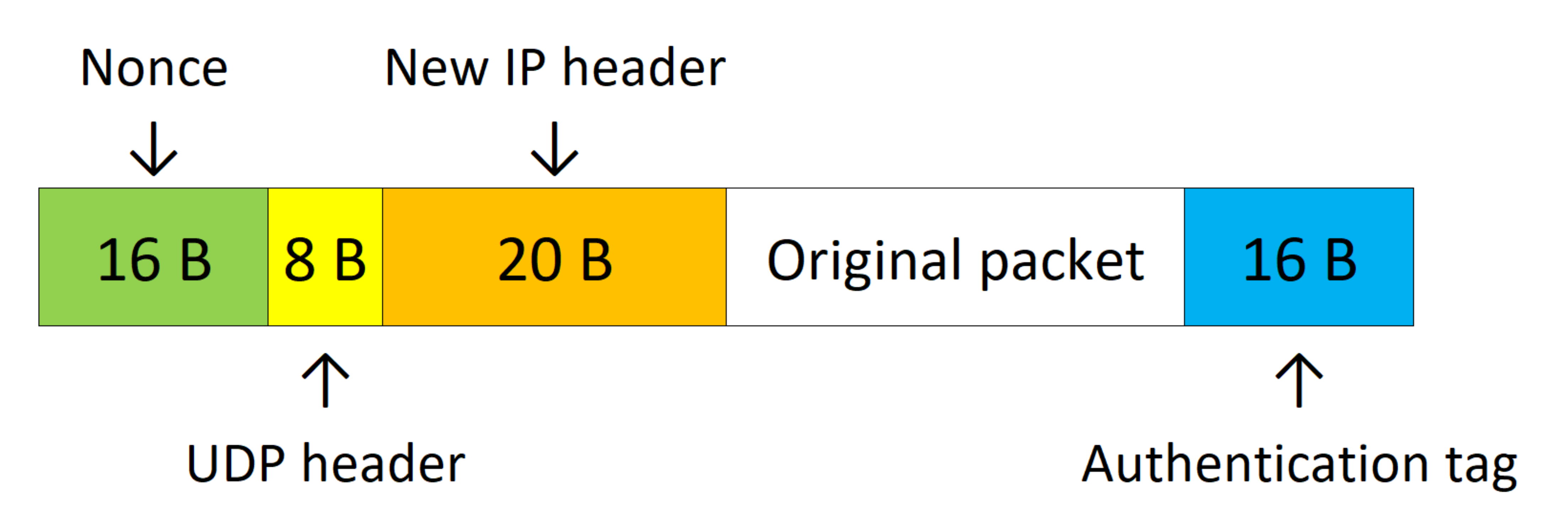
- Hybrid key establishment – 2 parts:
  - Post-Quantum Cryptography: Crystals Kyber 512
  - Quantum Key Distribution: COW Protocol in IDQ Clavis
  - Key combination: SHA3-256

- Symmetric encryption: AES-256-GCM
  - 16 B nonce
  - 16 B authentication tag

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by
the European Union

Encrypted Packet Structure



Nonce

New IP header

16 B

8 B

20 B

Original packet

16 B

UDP header

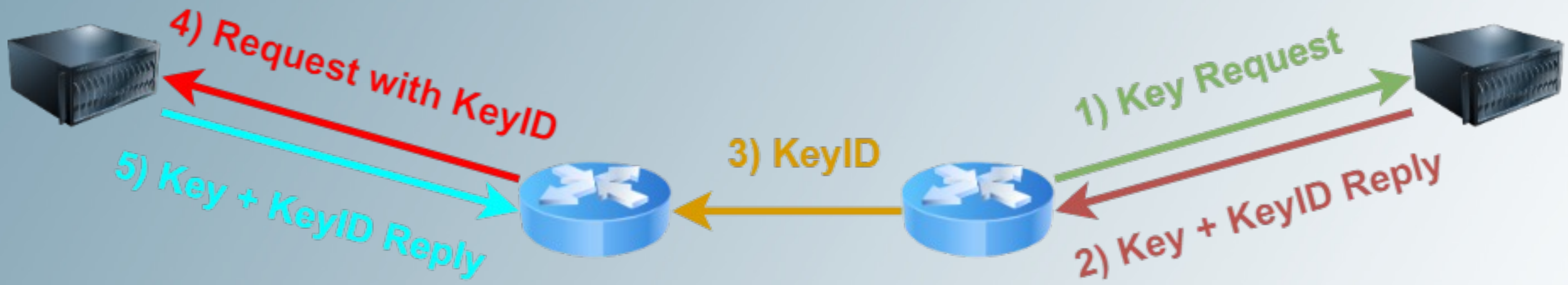
Authentication tag

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by
the European Union

Rekeying

- Occurs every 200 000 encrypted packets
  - Hybrid key recalculated with new QKD part



- TCP port 61000 is used to transfer key ID
- Rekey causes packet loss
  - Packets transferred during steps 1-3 fail integrity check

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Performance

- Average speed of file transfer measured using wget utility

Encryption	1 MB [mbps]	500 MB [mbps]	1 GB [mbps]	5 GB [mbps]
No encryption	435,4	499,8	476	458,6
Rekeying	162,7	142,6	140,3	140,6
No rekeying	162,7	144	145,3	145,8

- CPU: Intel Core i7 1065G7 Ice Lake

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Installation and Usage

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

- Requirements:
  - Debian or Debian-based Linux distribution + root privileges
- Installation:

```
git clone https://github.com/gabsssq/Linux-network-traffic-encryptor.git
cd Linux-network-traffic-encryptor
chmod +x install.sh
./install.sh [IP address of other gateway network {x.x.x.x/y}]
```

- Usage:
  - 1st Gateway – server: `./encryptor_server [QKD system IP]`
  - 2nd Gateway – client: `./encryptor_client [QKD system IP] [Server gateway IP]`

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by
the European Union

Summary

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Encryptor is used to create encryption gateways
- Quantum and post-quantum algorithms are used for key establishment
- AES-256-GCM is used to encrypt network traffic on virtual interfaces
- Gateways can serve as physical or virtual devices, with either physical or virtual interfaces. VPN clients are supported.

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

References

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

- Brno University of Technology: https://www.vut.cz/en
- Github: https://github.com/gabsssq/Linux-network-traffic-encryptor
- Crystals Kyber: https://pq-crystals.org/kyber/
- hajny@vut.cz

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union