ETSI/IQC Quantum Safe Cryptography Event

Quantum-safe VPNs

Sophia Grundner-Culemann

LMU Munich

02/14/2023

Project „QuaSiModO“

for Quantum-safe VPNs

Members

genua.

Adva
NETWORK SECURITY

LMU
LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Fraunhofer
AISEC

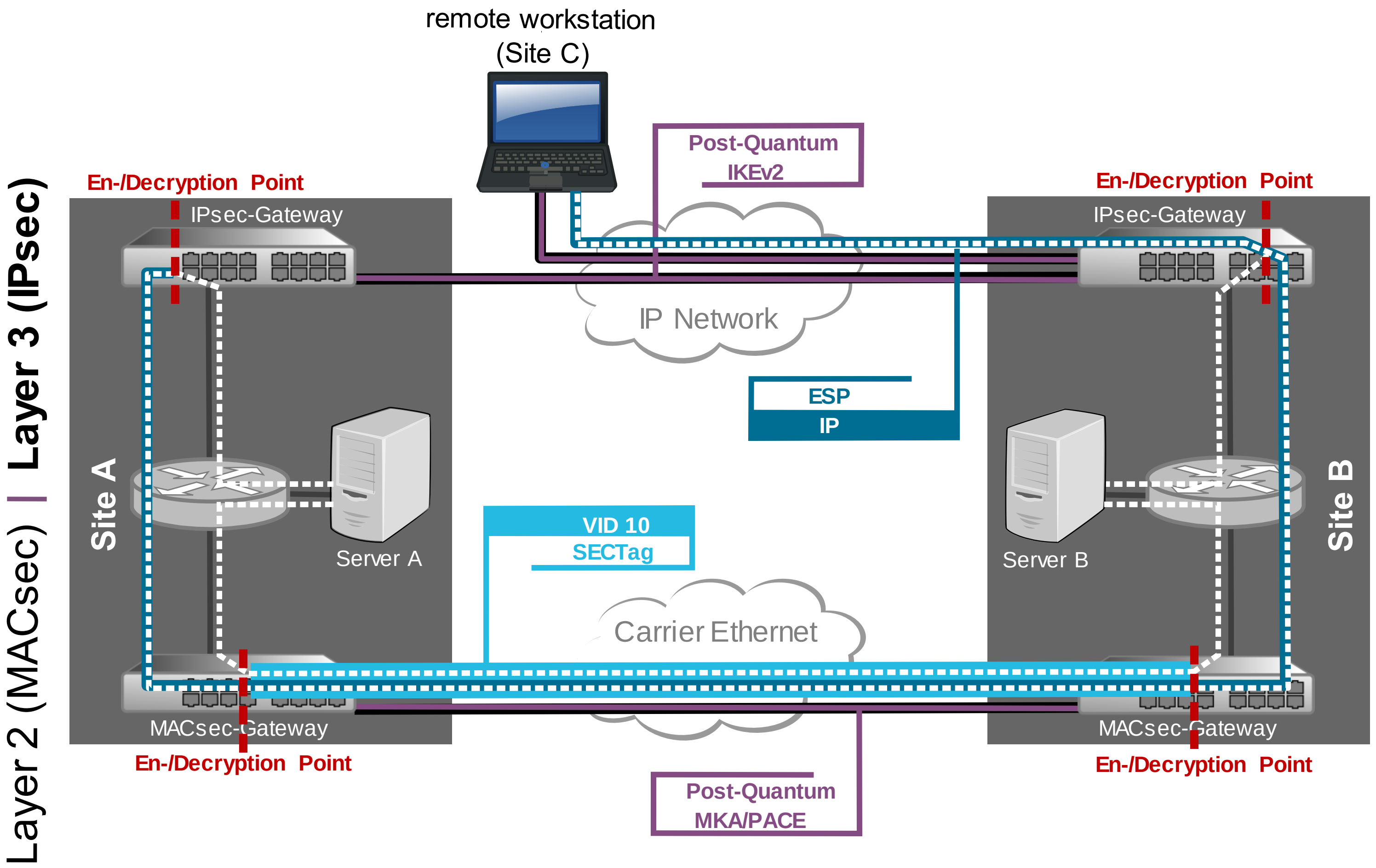
Associates

- Hessen3C
- Bundesamt
für Sicherheit in der
Informationstechnik

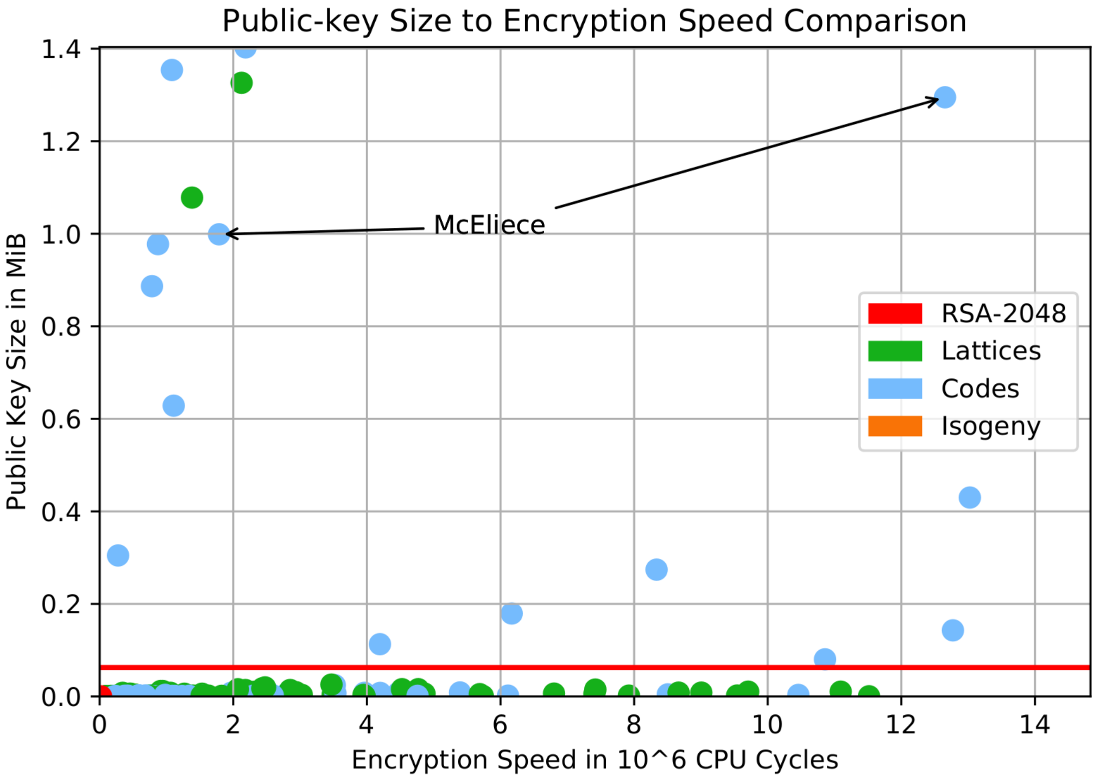
Funding

Bundesministerium
für Bildung
und Forschung

Virtual Private Networks (VPNs)



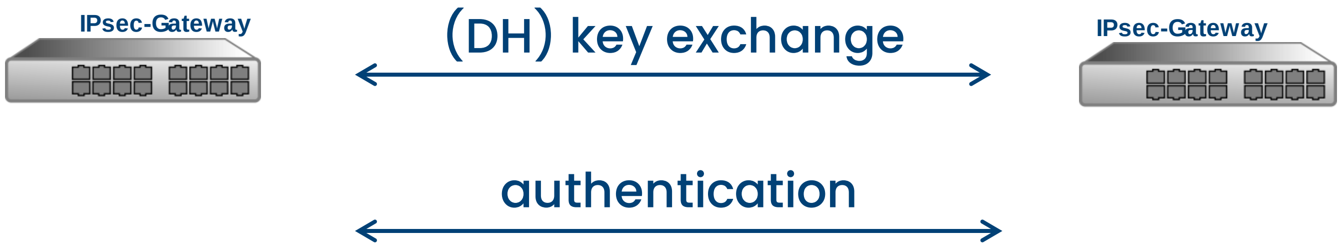
Challenge 1:
Key size (of the most trusted crypto)



Maximum transmission unit (1500 B)

Challenge 2:
Optimised (=Inflexible) design

IKEv2 (Layer 3 key exchange)



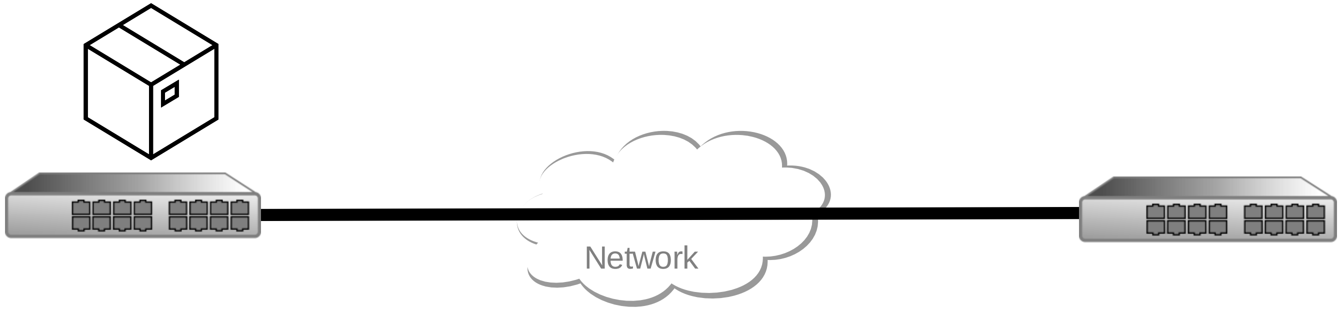
IPsec-Gateway

(DH) key exchange

IPsec-Gateway

authentication

Challenge 3:
Lossy networks



An ideal solution would be …

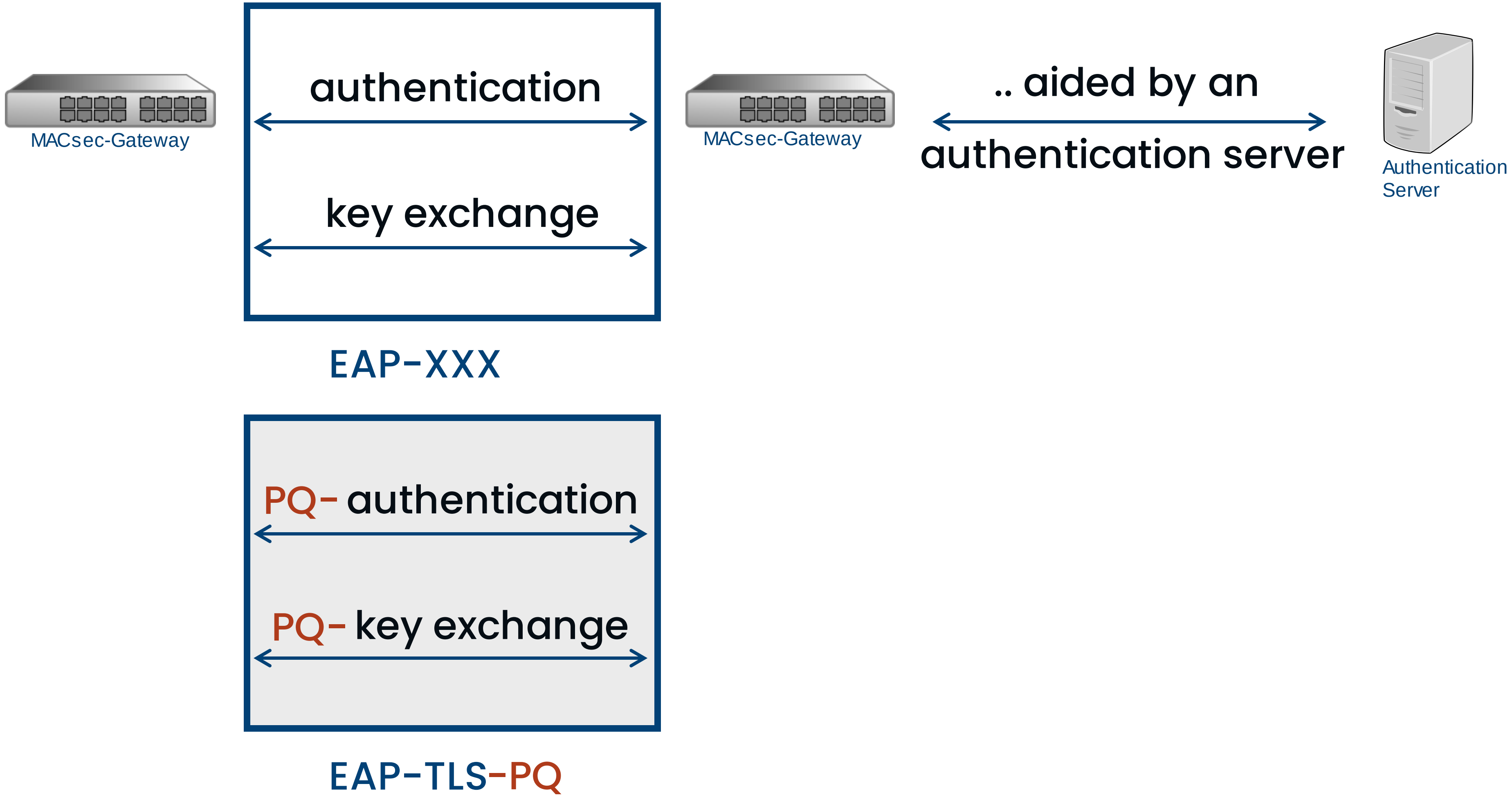
Flexible

- hybrid
- manage large keys
- crypto-agile
- KEX-friendly

Error resistantC

- fast initial connection
- minimal design
- cipher suites

MACsec / MKA



MACsec-Gateway

authentication

key exchange

MACsec-Gateway

.. aided by an

authentication server

Authentication Server

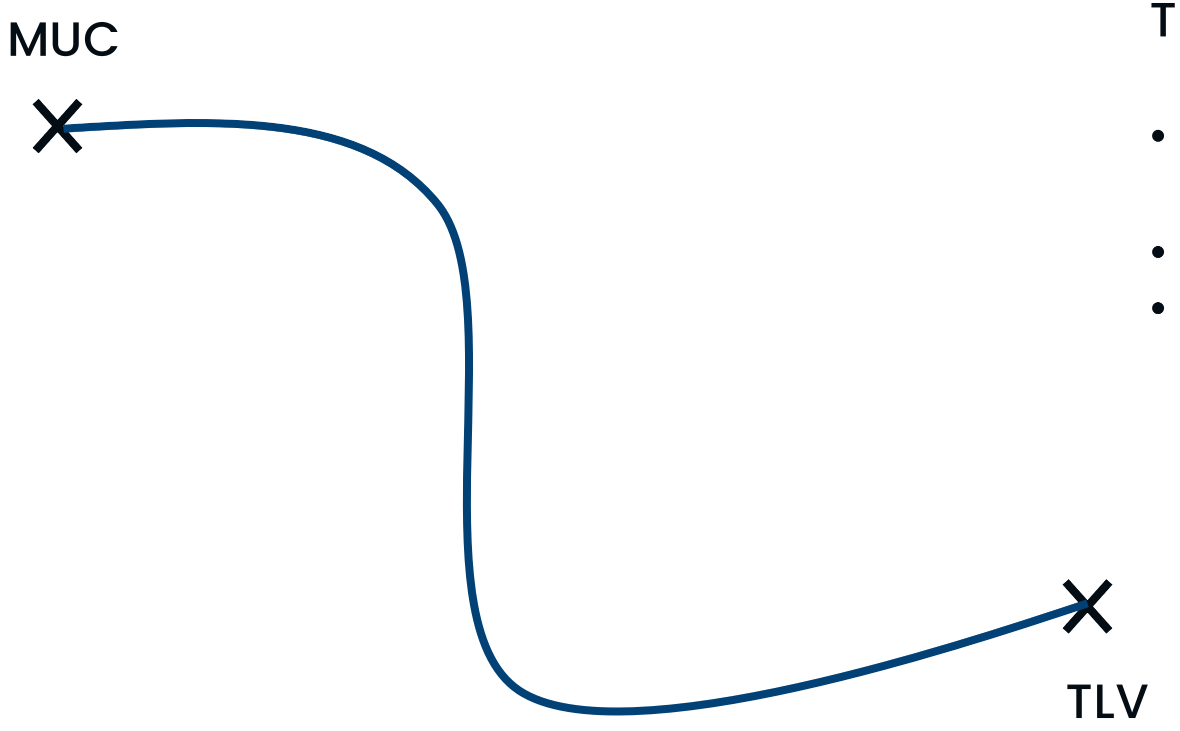
EAP-XXX

PQ- authentication

PQ- key exchange

EAP-TLS-PQ

MACsec / MKA Testing

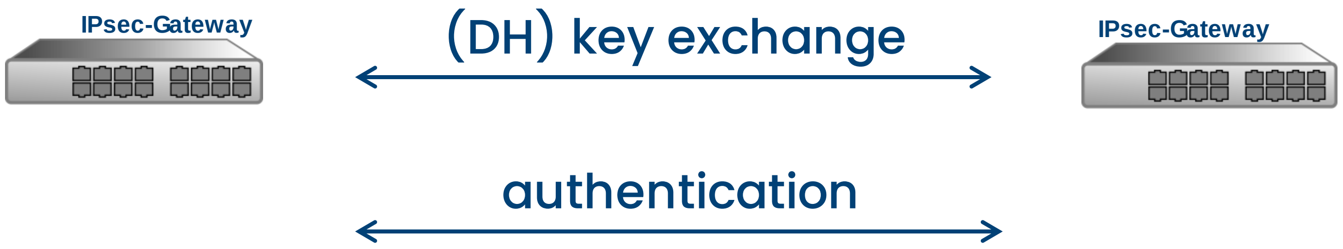


Throughput:

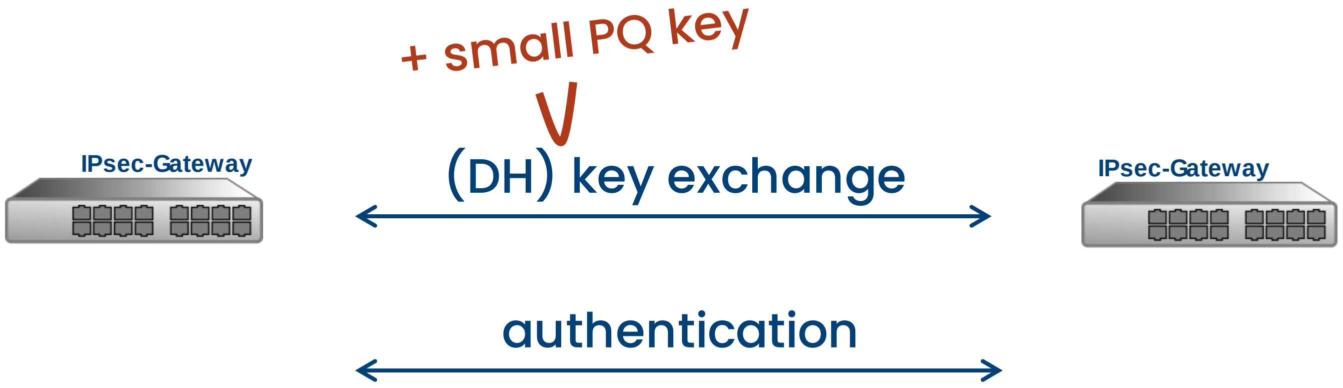
- MUC regional: 575 Mbit/s

- MUC → TLV: ~ 90 Mbit/s
- TLV → MUC: ~ 6 Mbit/s

Ipsec / IKEv2


IPsec-Gateway
(DH) key exchange
IPsec-Gateway
authentication

Ipsec / IKEv2

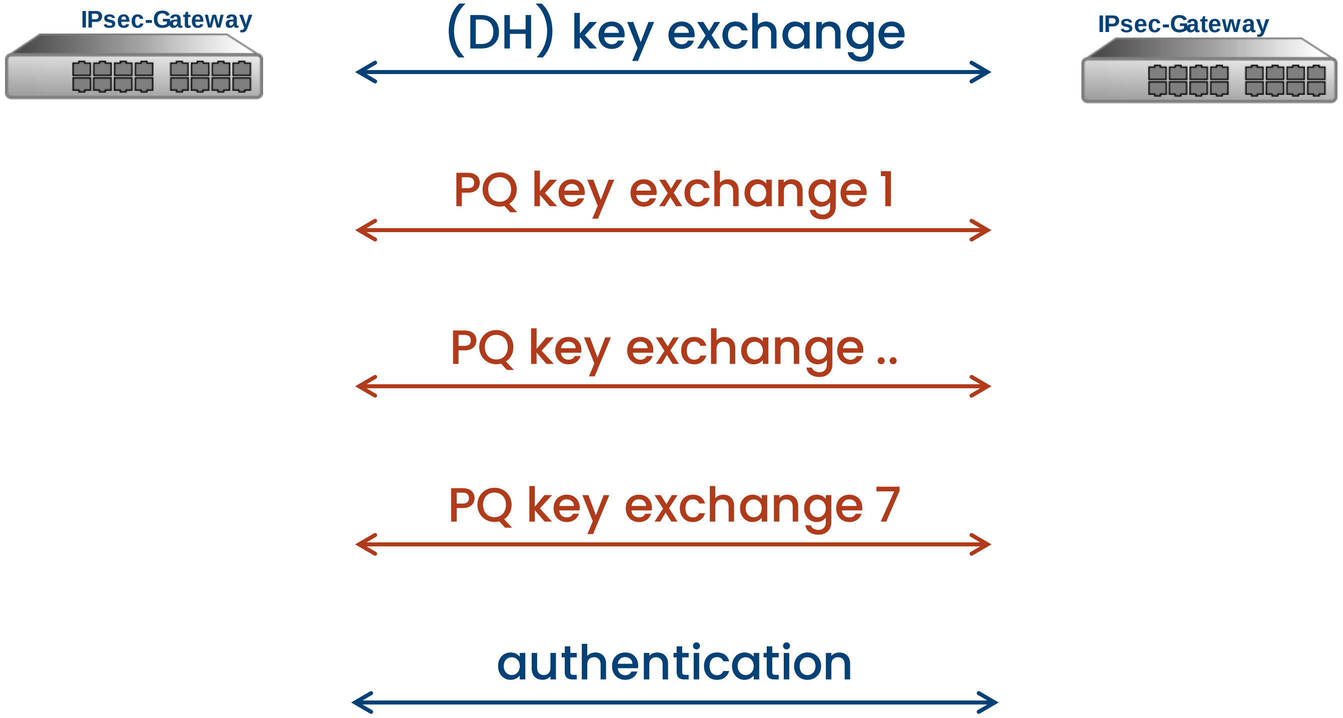


+ small PQ key

(DH) key exchange

authentication

Ipsec / IKEv2



(DH) key exchange

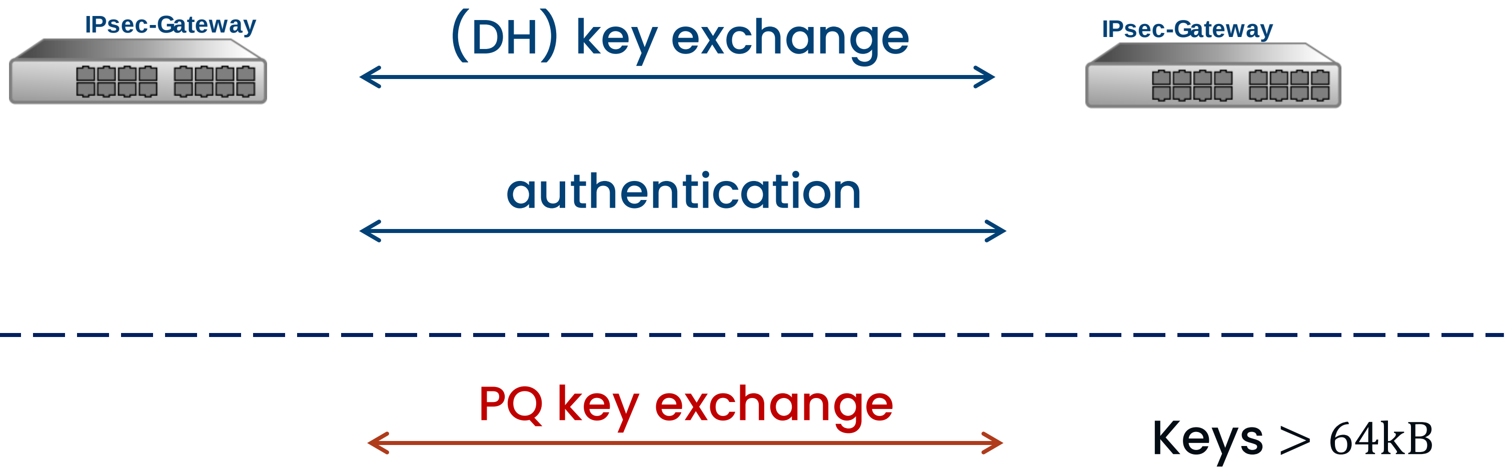
PQ key exchange 1

PQ key exchange ..

PQ key exchange 7

authentication

Ipsec / IKEv2



(DH) key exchange

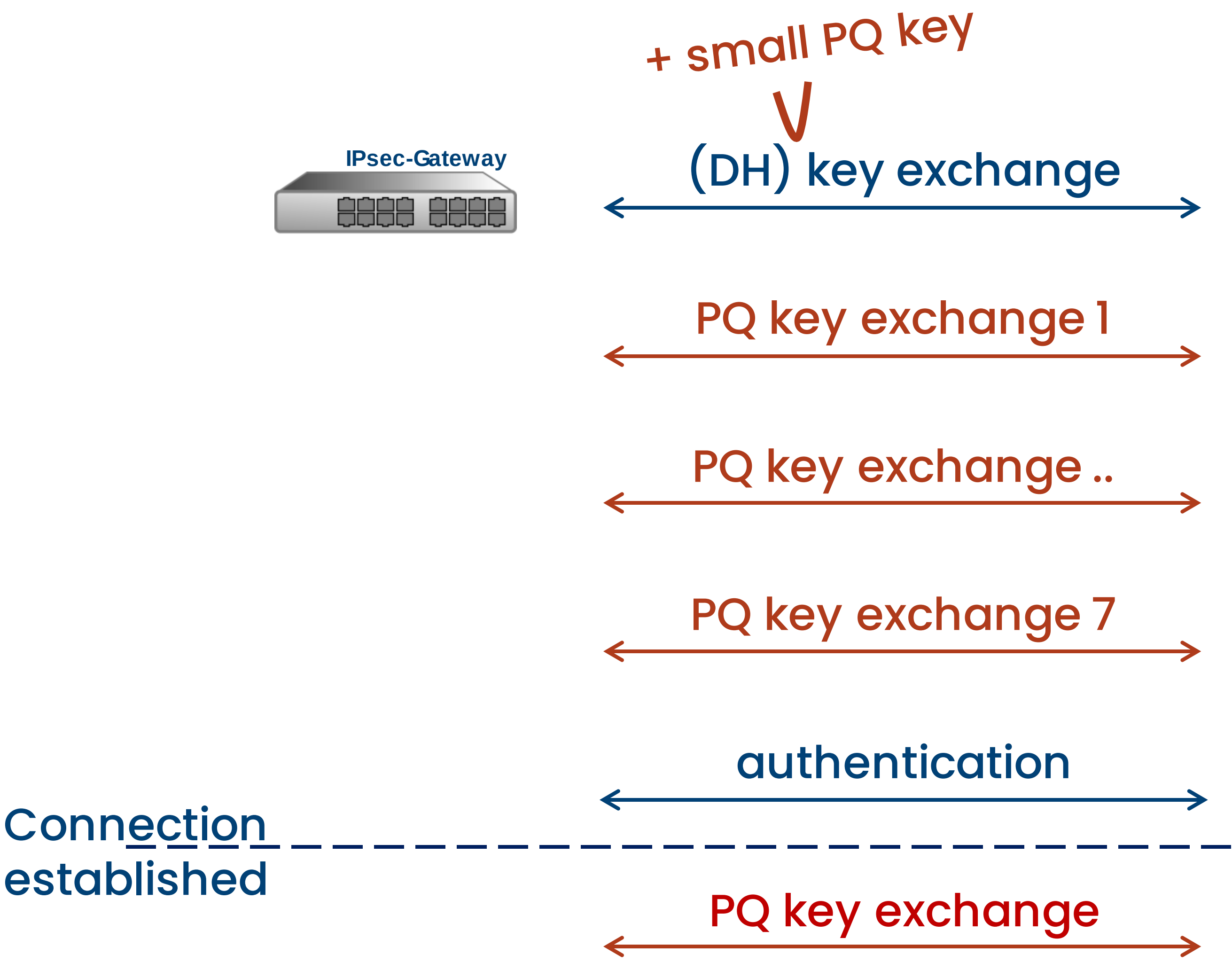
authentication

Connection established

PQ key exchange

Keys $> 64\text{kB}$

Ipsec / IKEv2



+ small PQ key

V

(DH) key exchange

IPsec-Gateway

IPsec-Gateway

PQ key exchange 1

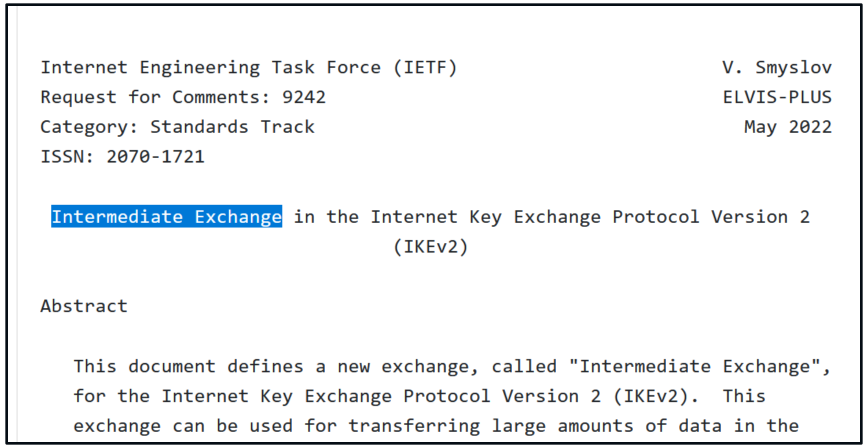
PQ key exchange ..

PQ key exchange 7

authentication

Connection established

PQ key exchange

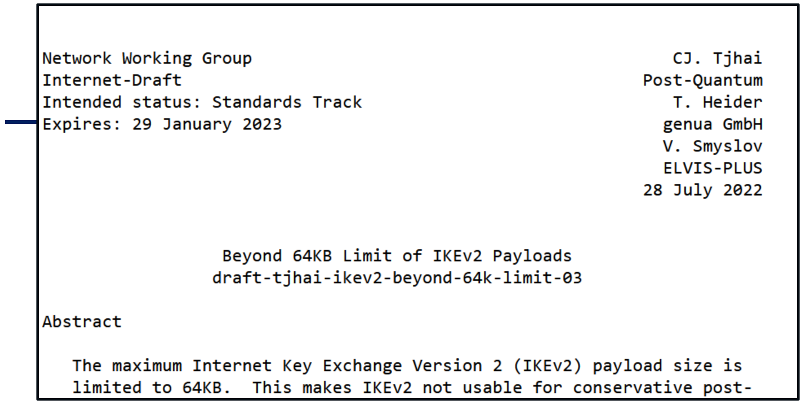


```
Internet Engineering Task Force (IETF)                        V. Smyslov
Request for Comments: 9242                                    ELVIS-PLUS
Category: Standards Track                                       May 2022
ISSN: 2070-1721

 Intermediate Exchange in the Internet Key Exchange Protocol Version 2
                                 (IKEv2)

Abstract

   This document defines a new exchange, called "Intermediate Exchange",
   for the Internet Key Exchange Protocol Version 2 (IKEv2).  This
   exchange can be used for transferring large amounts of data in the
```



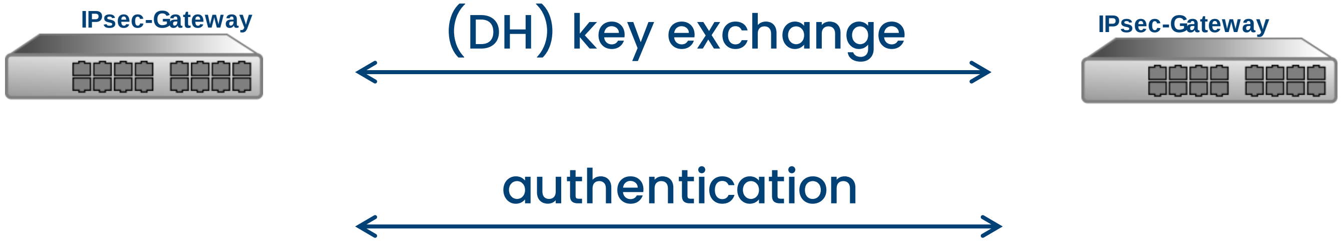
```
Network Working Group                                           CJ. Tjhai
Internet-Draft                                               Post-Quantum
Intended status: Standards Track                                T. Heider
Expires: 29 January 2023                                       genua GmbH
                                                               V. Smyslov
                                                               ELVIS-PLUS
                                                             28 July 2022


                   Beyond 64KB Limit of IKEv2 Payloads
                  draft-tjhai-ikev2-beyond-64k-limit-03

Abstract

   The maximum Internet Key Exchange Version 2 (IKEv2) payload size is
   limited to 64KB.  This makes IKEv2 not usable for conservative post-
```

Testing PQ-IKEv2



IPsec-Gateway

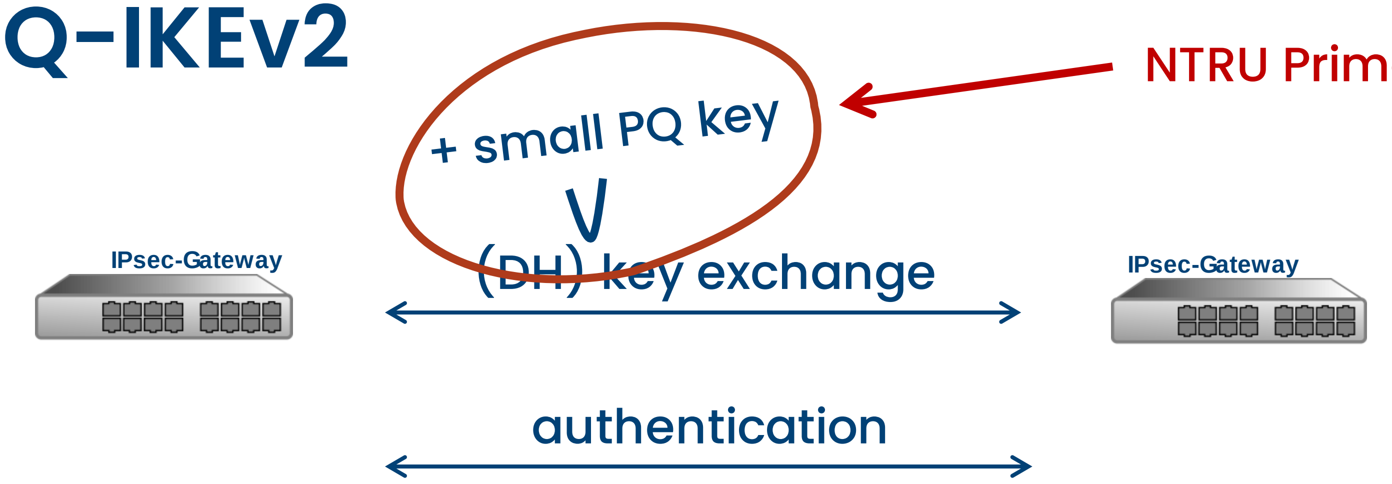
(DH) key exchange

IPsec-Gateway

authentication

Baseline:
~ 18-20 ms

Testing PQ-IKEv2



IPsec-Gateway

+ small PQ key

∨

(DH) key exchange

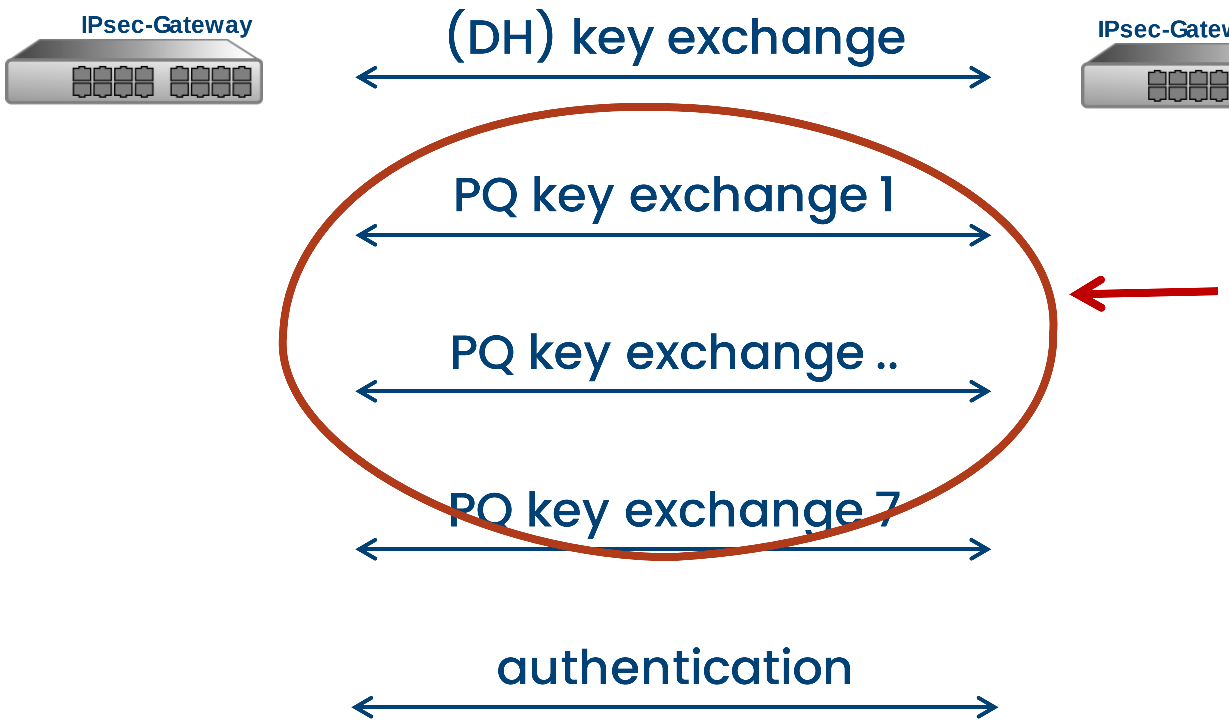
authentication

IPsec-Gateway

NTRU Prime adds 2-3 ms

Baseline:
~ 18-20 ms

Testing PQ-IKEv2



IPsec-Gateway

IPsec-Gateway

(DH) key exchange

PQ key exchange 1

PQ key exchange ..

PQ key exchange 7

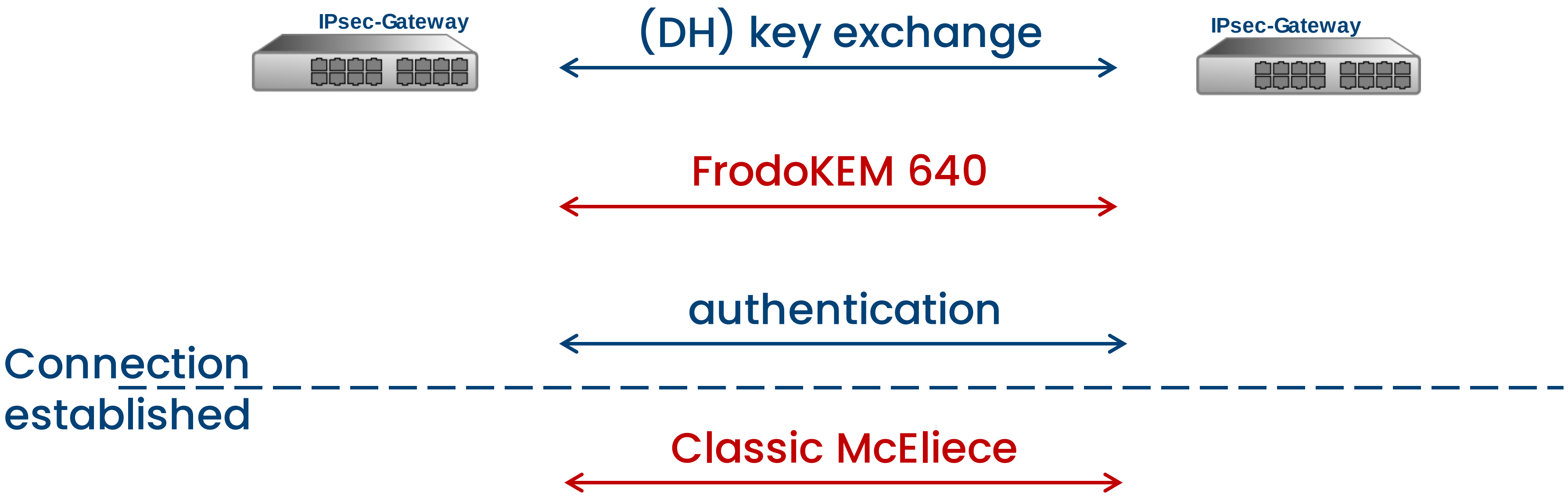
authentication

Baseline:
~ 18-20 ms

with 2 rounds
(CRYSTALSKyber 1024,
FrodoKEM 640)
< 25ms

(SIKE: ~1s)

Testing PQ-IKEv2



IPsec-Gateway

(DH) key exchange

IPsec-Gateway

FrodoKEM 640

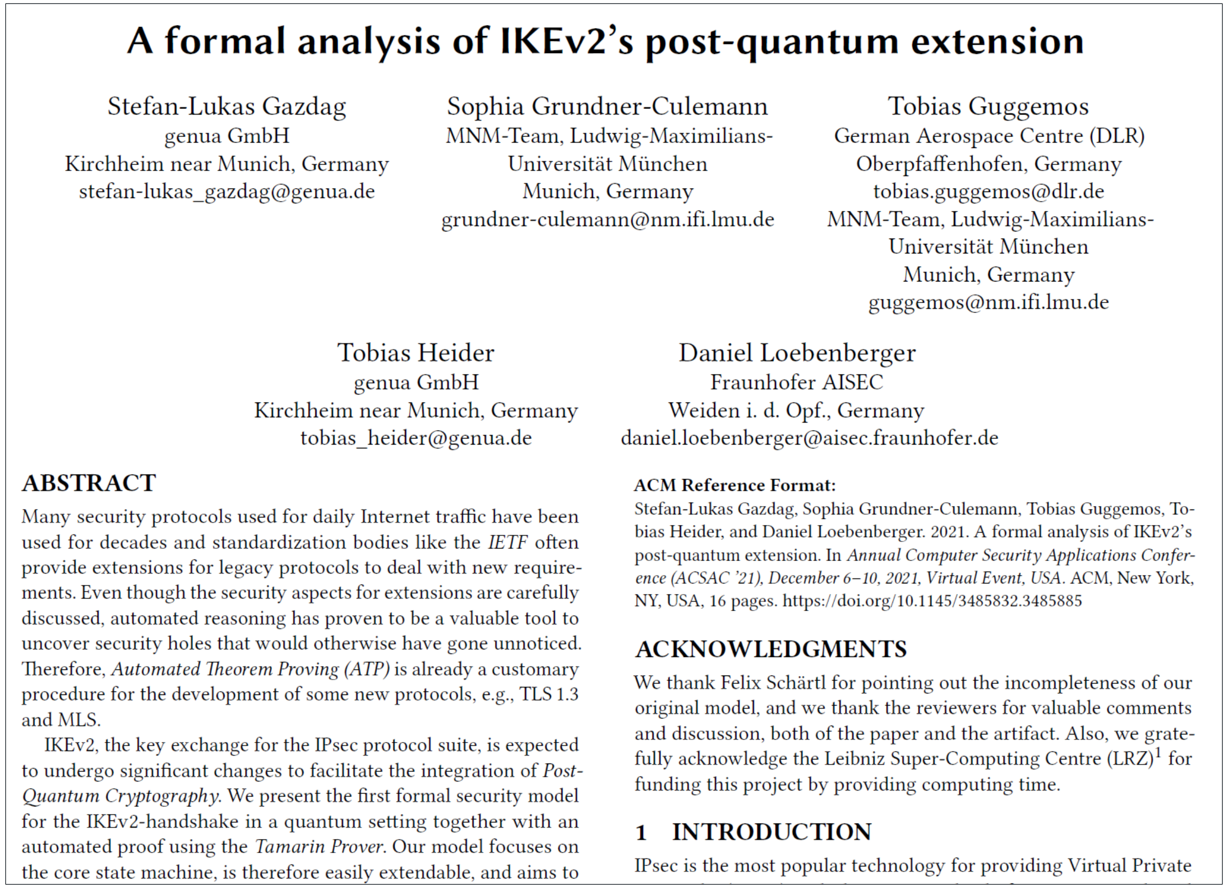
authentication

Connection established

Classic McEliece

~ 2.5 s
(in error-free network)

Security evaluations



A formal analysis of IKEv2's post-quantum extension

Stefan-Lukas Gazdag
genua GmbH
Kirchheim near Munich, Germany
stefan-lukas_gazdag@genua.de

Sophia Grundner-Culemann
MNM-Team, Ludwig-Maximilians-Universität München
Munich, Germany
grundner-culemann@nm.ifi.lmu.de

Tobias Guggemos
German Aerospace Centre (DLR)
Oberpfaffenhofen, Germany
tobias.guggemos@dlr.de
MNM-Team, Ludwig-Maximilians-Universität München
Munich, Germany
guggemos@nm.ifi.lmu.de

Tobias Heider
genua GmbH
Kirchheim near Munich, Germany
tobias_heider@genua.de

Daniel Loebenberger
Fraunhofer AISEC
Weiden i. d. Opf., Germany
daniel.loebenberger@aisec.fraunhofer.de

ABSTRACT

Many security protocols used for daily Internet traffic have been used for decades and standardization bodies like the *IETF* often provide extensions for legacy protocols to deal with new requirements. Even though the security aspects for extensions are carefully discussed, automated reasoning has proven to be a valuable tool to uncover security holes that would otherwise have gone unnoticed. Therefore, *Automated Theorem Proving (ATP)* is already a customary procedure for the development of some new protocols, e.g., TLS 1.3 and MLS.

IKEv2, the key exchange for the IPsec protocol suite, is expected to undergo significant changes to facilitate the integration of *Post-Quantum Cryptography*. We present the first formal security model for the IKEv2-handshake in a quantum setting together with an automated proof using the *Tamarin Prover*. Our model focuses on the core state machine, is therefore easily extendable, and aims to

ACM Reference Format:
Stefan-Lukas Gazdag, Sophia Grundner-Culemann, Tobias Guggemos, Tobias Heider, and Daniel Loebenberger. 2021. A formal analysis of IKEv2's post-quantum extension. In *Annual Computer Security Applications Conference (ACSAC '21), December 6–10, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3485832.3485885

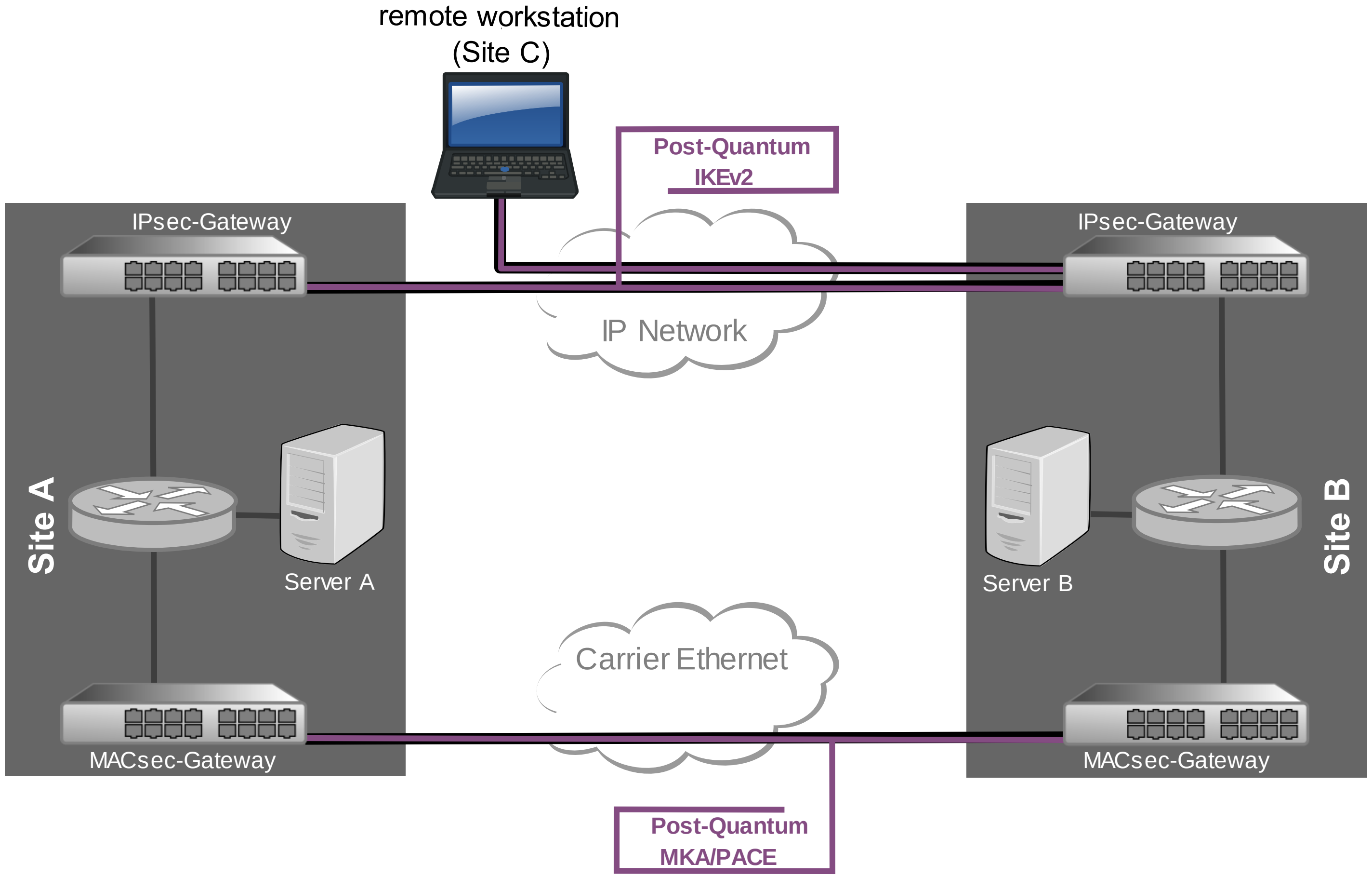
ACKNOWLEDGMENTS

We thank Felix Schärtl for pointing out the incompleteness of our original model, and we thank the reviewers for valuable comments and discussion, both of the paper and the artifact. Also, we gratefully acknowledge the Leibniz Super-Computing Centre (LRZ)[1] for funding this project by providing computing time.

1 INTRODUCTION

IPsec is the most popular technology for providing Virtual Private

To be continued



- Testing MACsec + Ipsec together
- More automated proofs
- Consider authentication (more)
- Many more real-world tests

  → with you?
- Get in contact: **pqc@genua.de**