LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MNM TEAM

Towards Quantum-Resistant MACSec using EAP-TLS

Abschlussvortrag zur Masterarbeit

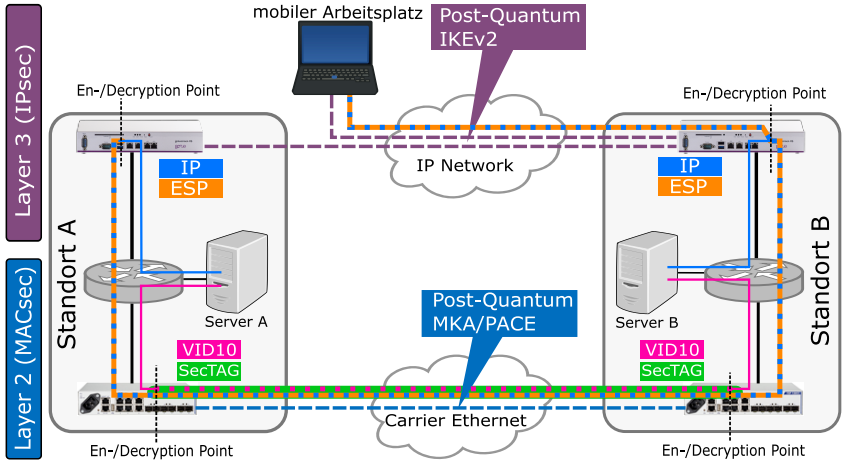
Robin Lösch

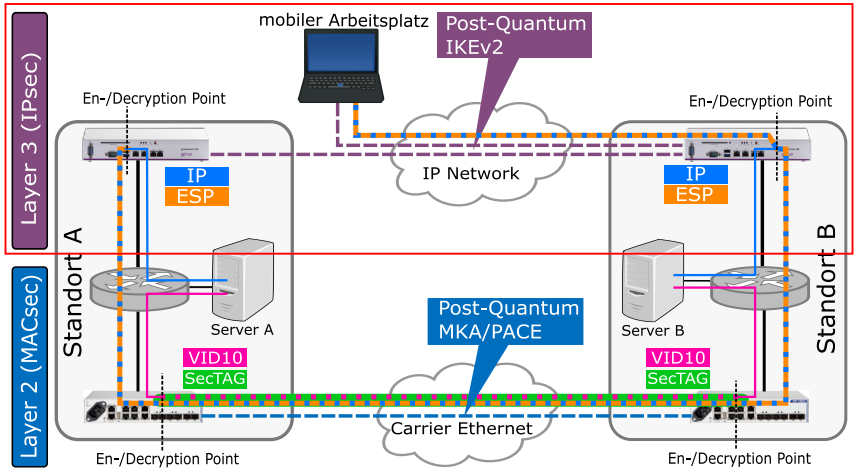
loesch@cip.ifi.lmu.de

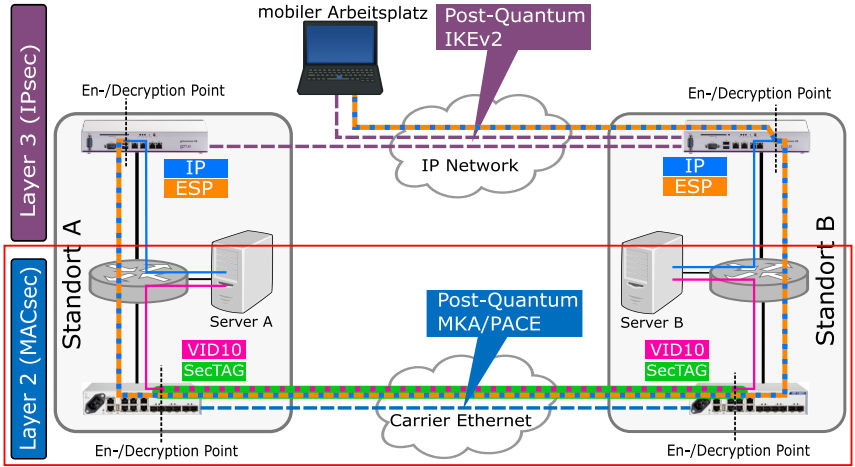
Aufgabensteller: Prof. Dr. Dieter Kranzlmüller
Betreuer: Sophia Grundner-Culemann
Dr. Tobias Guggemos
Dr. Joo Cho, ADVA Optical Networking

MNM-Team, LMU München

January 19, 2021


Layer 3 (IPsec)
Layer 2 (MACsec)
mobiler Arbeitsplatz
Post-Quantum IKEv2
En-/Decryption Point
En-/Decryption Point
IP Network
IP
ESP
IP
ESP
Standort A
Standort B
Server A
Server B
Post-Quantum MKA/PACE
VID10
SecTAG
VID10
SecTAG
Carrier Ethernet
En-/Decryption Point
En-/Decryption Point


Layer 3 (IPsec)
Layer 2 (MACsec)
mobiler Arbeitsplatz
Post-Quantum IKEv2
En-/Decryption Point
En-/Decryption Point
IP
ESP
IP Network
IP
ESP
Standort A
Standort B
Server A
Server B
Post-Quantum MKA/PACE
VID10
SecTAG
VID10
SecTAG
Carrier Ethernet
En-/Decryption Point
En-/Decryption Point


Layer 3 (IPsec)
Layer 2 (MACSec)
mobiler Arbeitsplatz
Post-Quantum IKEv2
En-/Decryption Point
En-/Decryption Point
IP Network
IP
ESP
IP
ESP
Standort A
Standort B
Server A
Server B
Post-Quantum MKA/PACE
VID10
SecTAG
VID10
SecTAG
Carrier Ethernet
En-/Decryption Point
En-/Decryption Point

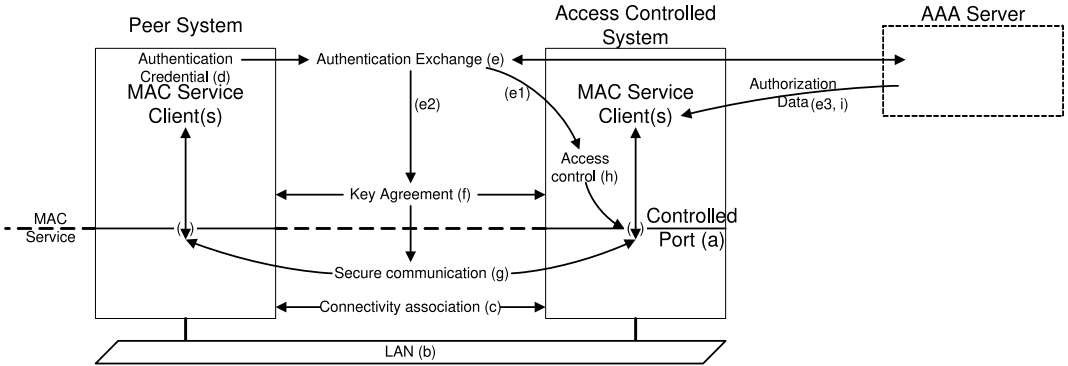
MACSec

- IEEE Standard
- Layer 2 encryption & integrity protection

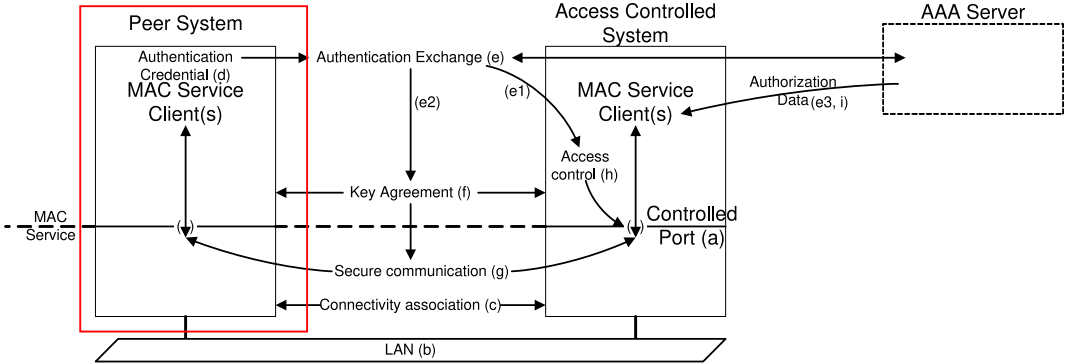
MACSec

- IEEE Standard
- Layer 2 encryption & integrity protection
- Two important standards:
  - IEEE 802.1X: Port-Based Network Access Control[1]
  - IEEE 802.1AE: Media Access Control (MAC) Security[2]

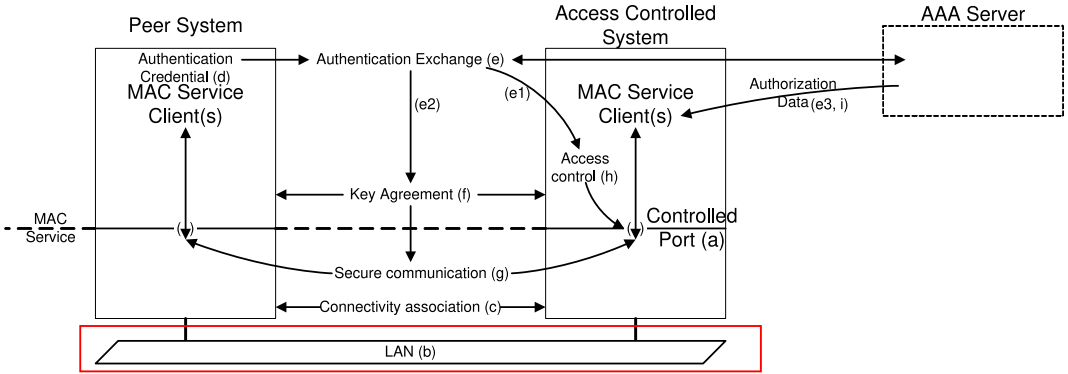
Background & Motivation



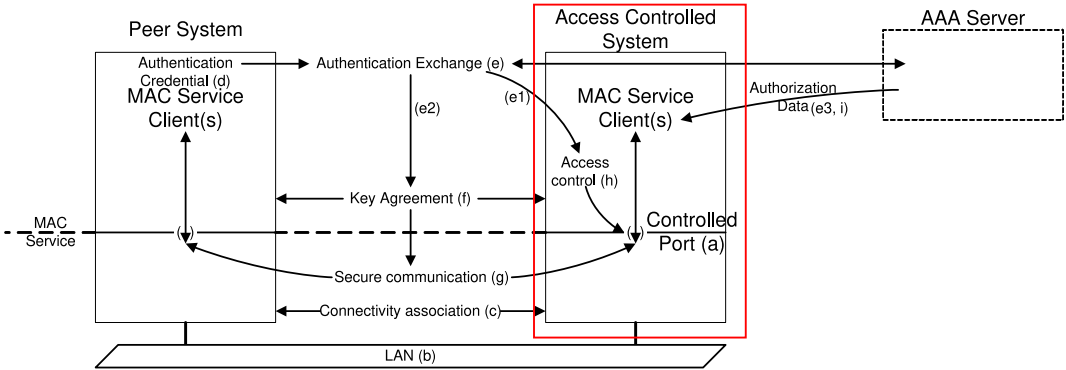
Background & Motivation



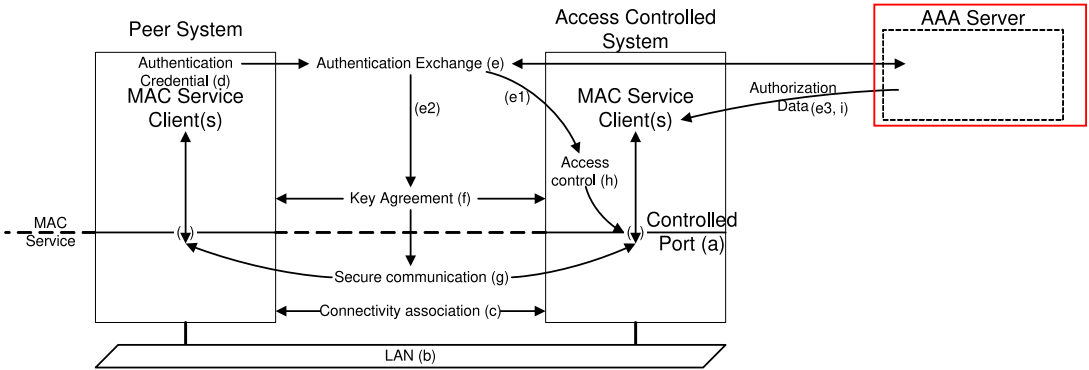
Background & Motivation

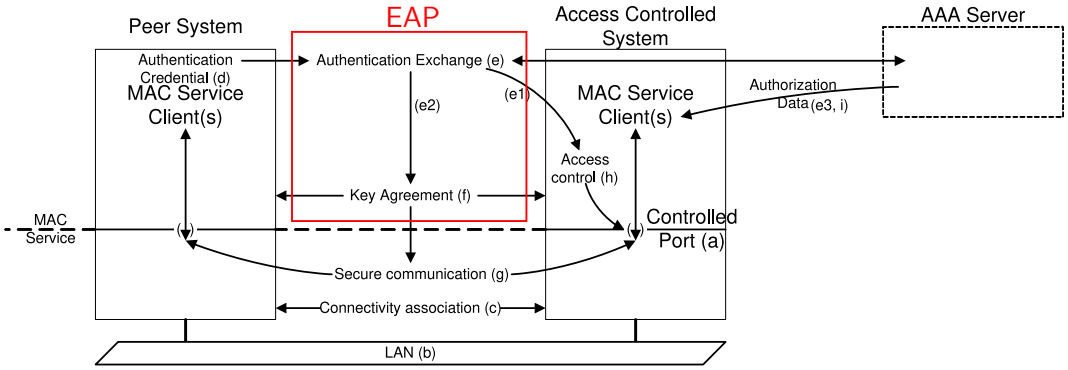


Background & Motivation



Background & Motivation




Peer System
EAP
Access Controlled System
AAA Server
Authentication Credential (d)
MAC Service Client(s)
Authentication Exchange (e)
(e1)
(e2)
MAC Service Client(s)
Authorization Data (e3, i)
Access control (h)
Key Agreement (f)
MAC Service
Controlled Port (a)
Secure communication (g)
Connectivity association (c)
LAN (b)

Extensible Authentication Protocol[3]

- Framework for arbitrary authentication methods
- Request-Response based protocol

Extensible Authentication Protocol[3]

- Framework for arbitrary authentication methods
- Request-Response based protocol
- IEEE 802.1X uses EAP-TLS
  - TLS encapsulated in EAP
  - (EC)DH and RSA for authentication and key exchange

Extensible Authentication Protocol[3]

- Framework for arbitrary authentication methods
- Request-Response based protocol
- IEEE 802.1X uses EAP-TLS
  - TLS encapsulated in EAP
  - (EC)DH and RSA for authentication and key exchange
- Result:
  - Mutual authentication (Access control)
  - Shared symmetric key (MACSec encryption)

Post-Quantum Cryptography

- Quantum computers are an inherent problem for asymmetric cryptography

Post-Quantum Cryptography

- Quantum computers are an inherent problem for asymmetric cryptography
- Alternative cryptosystems have been researched for years:
  - McEliece (1978): Code-based cryptosystems[4]
  - Lamport (1979): Hash-based signatures[5]
  - Imai, Matsumoto (1988): Multivariate cryptography[6]
  - Ajtai (1996): Lattice-based cryptosystems[7]
  - De Feo, Jao, and Plût (2011): (Supersingular) Isogeny-based DH[8]

Post-Quantum Cryptography

- Quantum computers are an inherent problem for asymmetric cryptography
- Alternative cryptosystems have been researched for years:
  - McEliece (1978): Code-based cryptosystems[4]
  - Lamport (1979): Hash-based signatures[5]
  - Imai, Matsumoto (1988): Multivariate cryptography[6]
  - Ajtai (1996): Lattice-based cryptosystems[7]
  - De Feo, Jao, and Plût (2011): (Supersingular) Isogeny-based DH[8]
- NIST standardization project: One or more PQ cryptosystems

Post-Quantum Cryptography

- Quantum computers are an inherent problem for asymmetric cryptography
- Alternative cryptosystems have been researched for years:
  - McEliece (1978): Code-based cryptosystems[4]
  - Lamport (1979): Hash-based signatures[5]
  - Imai, Matsumoto (1988): Multivariate cryptography[6]
  - Ajtai (1996): Lattice-based cryptosystems[7]
  - De Feo, Jao, and Plût (2011): (Supersingular) Isogeny-based DH[8]
- NIST standardization project: One or more PQ cryptosystems
- Which cryptosystem is a good replacement for DH, RSA...?

Finding a good replacement

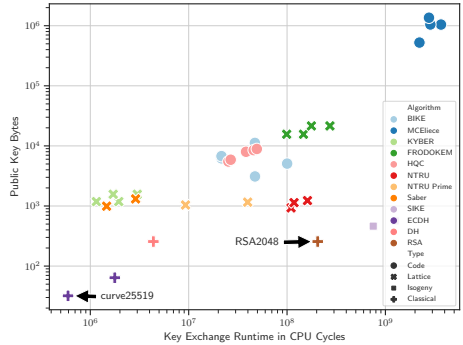
- Main focus of this work

Finding a good replacement

- Main focus of this work
- There is no clear "winner"

Finding a good replacement

- Main focus of this work
- There is no clear "winner"
- Different requirements/different trade-offs
  - Small key sizes (traffic footprints)
  - Fast algorithms (latency)
  - “Maturity”



Requirements for a PQ MACSec

- Main Goals:
  - Quantum-resistant design
  - Keep existing security properties

Requirements for a PQ MACSec

- Main Goals:
  - Quantum-resistant design
  - Keep existing security properties
- Key Exchange Algorithm / Signature Algorithms:
  - Latency > Traffic
  - Forward-secrecy for Key Exchange

Requirements for a PQ MACSec

- Main Goals:
  - Quantum-resistant design
  - Keep existing security properties
- Key Exchange Algorithm / Signature Algorithms:
  - Latency > Traffic
  - Forward-secrecy for Key Exchange
- Need to evaluate different algorithms

Methodology

Methodology

- Implement PQ MACSec:
  - hostapd (Peer/Access Controlled System)
  - FreeRADIUS (Authentication Server)
  - OpenSSL fork by Open Quantum Safe

Methodology

- Implement PQ MACSec:
  - hostapd (Peer/Access Controlled System)
  - FreeRADIUS (Authentication Server)
  - OpenSSL fork by Open Quantum Safe
- Experimental evaluation of all NIST Round 3 candidates

Methodology

- Implement PQ MACSec:
  - hostapd (Peer/Access Controlled System)
  - FreeRADIUS (Authentication Server)
  - OpenSSL fork by Open Quantum Safe
- Experimental evaluation of all NIST Round 3 candidates
- Practical proof-of-concept

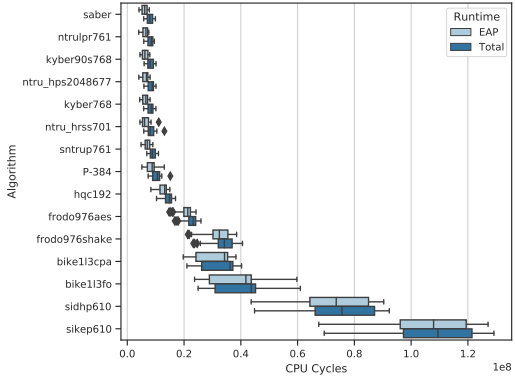
Performance Evaluation

- Strongly depends on foundation

Performance Evaluation

- Strongly depends on foundation
- Performance often similar to ECDH

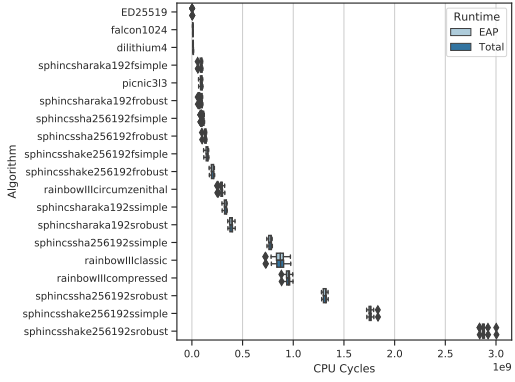
Foundation	Scheme
Code-Based	BIKE
	Classic McEliece
	HQC
Lattice-Based	SABER
	CRYSTALS-KYBER
	NTRU
	NTRU Prime
	FrodoKEM
Isogeny-Based	SIKE



Performance Evaluation

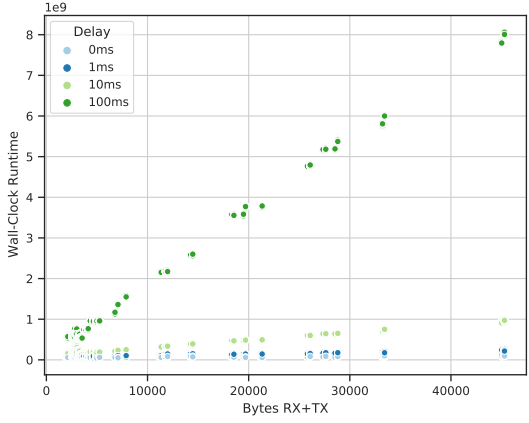
- Strongly depends on foundation
- Performance often similar to ECDH

Foundation	Scheme
Lattice-Based	CRYSTALS-DILITHIUM FALCON
Multivariate	GeMSS Rainbow
Zero-Knowledge Proof	Picnic
Hash-Based	SPHINCS+



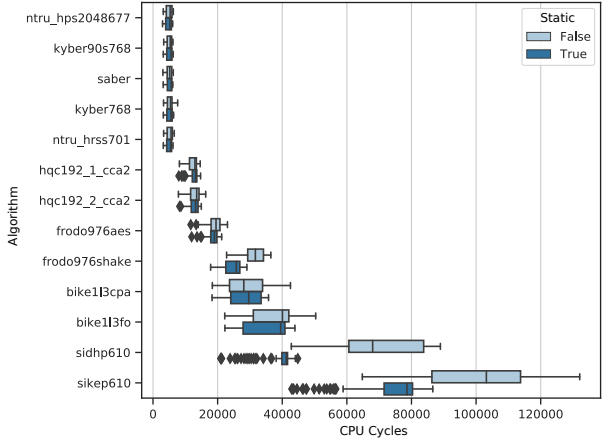
Impact of Latency

- Large number of frames
- EAP Packets need to be acknowledged
- Wall-Clock Runtime strongly depends on latency



Forward-secrecy

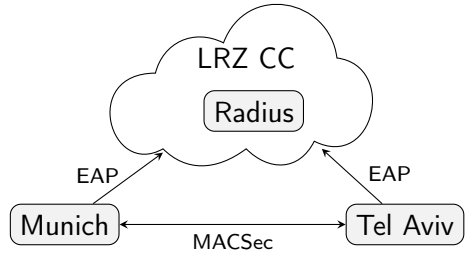
- Forward-secrecy by design
  - NIST uses Three-way API
  - Generate, Encapsulate, Decapsulate
- Little impact on most algorithms
- Exception: SIDH/SIKE



Practical Evaluation

- Part of QuaSiModO
- Cooperation with ADVA Optical Networking
- Selected PQ schemes compared to classical schemes

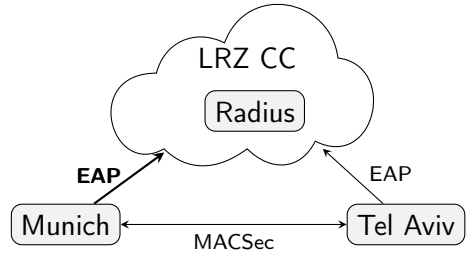
Setting	Signature	KEX
PQ	falcon1024	Saber
ECDH	P-521	P-384
Hybrid	falcon1024 || P-521	Saber || P-384
RSA	RSA4096	P-384



Practical Evaluation

- Part of QuaSiModO
- Cooperation with ADVA Optical Networking
- Selected PQ schemes compared to classical schemes

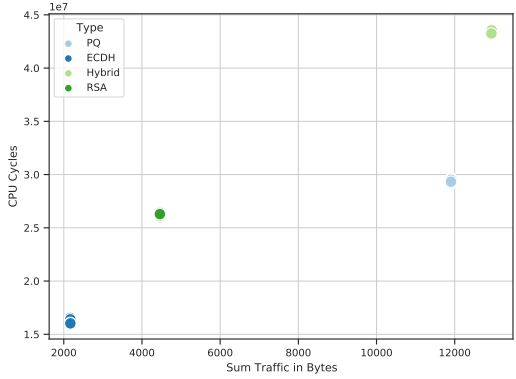
Setting	Signature	KEX
PQ	falcon1024	Saber
ECDH	P-521	P-384
Hybrid	falcon1024 || P-521	Saber || P-384
RSA	RSA4096	P-384



Practical Evaluation

- Part of QuaSiModO
- Cooperation with ADVA Optical Networking
- Selected PQ schemes compared to classical schemes

Setting	Signature	KEX
PQ	falcon1024	Saber
ECDH	P-521	P-384
Hybrid	falcon1024 || P-521	Saber || P-384
RSA	RSA4096	P-384



Summary

Summary

Conclusion

- PQ Crypto is feasible
- Biggest concern are key sizes
- Lattice-based ciphers performs best
- EAP/Radius are bottlenecks

Summary

Conclusion

- PQ Crypto is feasible
- Biggest concern are key sizes
- Lattice-based ciphers performs best
- EAP/Radius are bottlenecks

Contribution

- PQ IEEE802.1X/EAP-TLS
- PQ TLS1.3 implementation of hostapd/FreeRADIUS
- Contributions for liboqs/OpenSSL
- Extensive evaluation
- Real-World proof-of-concept

Summary

Conclusion

- PQ Crypto is feasible
- Biggest concern are key sizes
- Lattice-based ciphers performs best
- EAP/Radius are bottlenecks

Contribution

- PQ IEEE802.1X/EAP-TLS
- PQ TLS1.3 implementation of hostapd/FreeRADIUS
- Contributions for liboqs/OpenSSL
- Extensive evaluation
- Real-World proof-of-concept

Future Work

- TEAP instead of EAP-TLS
- (PQ-)TLS 1.4?
- Further NIST project development

References I

[1] "Ieee standard for local and metropolitan area networks–port-based network access control," Institute of Electrical and Electronics Engineers, Standard, Feb. 2002.

[2] "Ieee standard for local and metropolitan area networks-media access control (mac) security," Institute of Electrical and Electronics Engineers, Standard, Sep. 2018.

[3] J. Vollbrecht, J. D. Carlson, L. Blunk, D. B. D. A. Ph.D., and H. Levkowetz, *Extensible authentication protocol (eap)*, RFC 3748, Jun. 2004. DOI: 10.17487/RFC3748. [Online]. Available: https://rfc-editor.org/rfc/rfc3748.txt.

[4] E. Berlekamp, R. McEliece, and H. Van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

References II

[5] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report CSL-98, SRI International, Tech. Rep., 1979.

[6] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 1988, pp. 419–453.

[7] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 99–108.

[8] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *International Workshop on Post-Quantum Cryptography*, Springer, 2011, pp. 19–34.

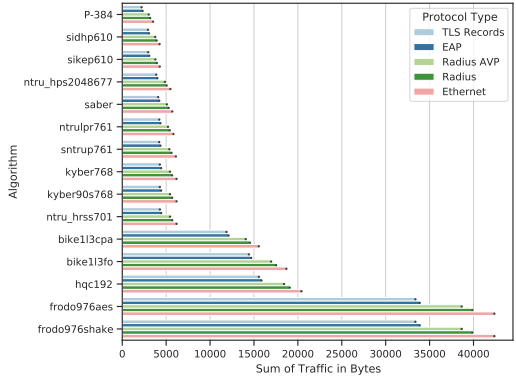
Traffic Evaluation

- Algo. selection depends heavily on use-case
- Small keys vs. small signatures

Traffic Evaluation

- Algo. selection depends heavily on use-case
- Small keys vs. small signatures

Background	Scheme
Code-Based	BIKE
	Classic McEliece
	HQC
Lattice-Based	SABER
	CRYSTALS-KYBER
	NTRU
	NTRU Prime
	FrodoKEM
Isogeny-Based	SIKE

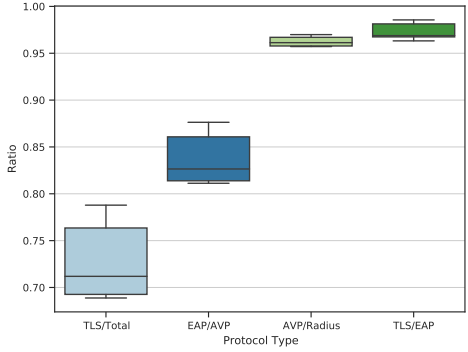


Protocol Overhead

- Many protocol layers
- Results in large overhead

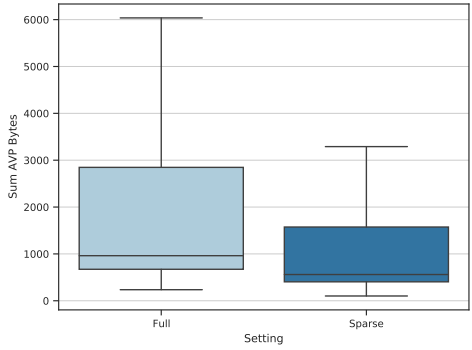
Protocol Overhead

- Many protocol layers
- Results in large overhead

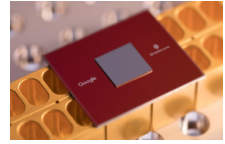


Protocol Overhead

- Many protocol layers
- Results in large overhead
- Redundant AVP values
- Sparse variant can save up to 40%

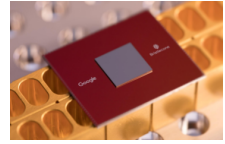


Post-Quantum Cryptography



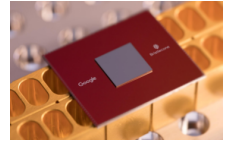
Post-Quantum Cryptography

- 40 Years of quantum computing:
  - 1980: First (theoretical) model of a quantum turing machine
  - 2018: 72-Qubit “Bristlecone” architecture

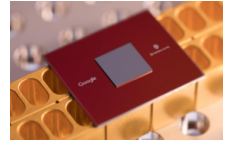


Post-Quantum Cryptography

- 40 Years of quantum computing:
  - 1980: First (theoretical) model of a quantum turing machine
  - 2018: 72-Qubit "Bristlecone" architecture
- Quantum-effects allow for faster algorithms:
  - Shor's algorithm: Breaks RSA and (EC)DH in polynomial time
  - Grover's algorithm: Weaken symmetric schemes by $\sqrt{n}$

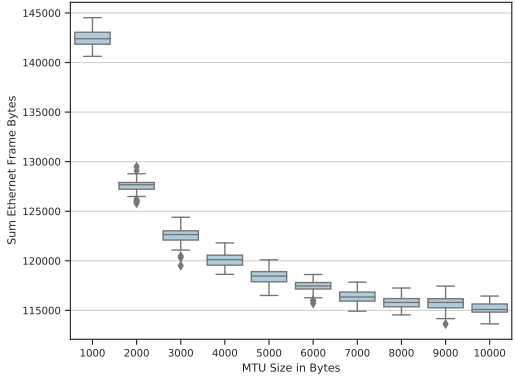


Post-Quantum Cryptography

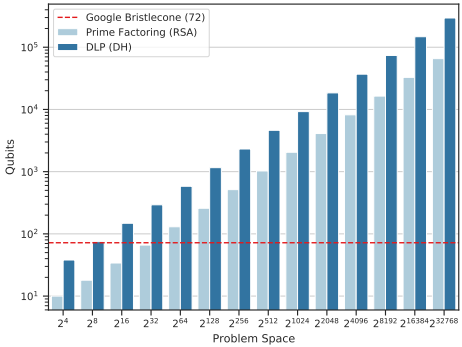


- 40 Years of quantum computing:
  - 1980: First (theoretical) model of a quantum turing machine
  - 2018: 72-Qubit "Bristlecone" architecture
- Quantum-effects allow for faster algorithms:
  - Shor's algorithm: Breaks RSA and (EC)DH in polynomial time
  - Grover's algorithm: Weaken symmetric schemes by $\sqrt{n}$
- When will quantum computer be able to break RSA2048?

Fragment Size



Shor


Google Bristlecone (72)
Prime Factoring (RSA)
DLP (DH)
Qubits
10^5
10^4
10^3
10^2
10^1
2^4 2^8 2^{16} 2^{32} 2^{64} 2^{128} 2^{256} 2^{512} 2^{1024} 2^{2048} 2^{4096} 2^{8192} 2^{16384} 2^{32768}
Problem Space