Post-Quantum Hybrid KEMTLS Performance in Simulated and Real Network Environments

Alexandre Augusto Giron[1,2], João Pedro Adami do Nascimento[1], Ricardo Custódio[1], Lucas Pandolfo Perin[3] and Victor Mateu[3]

[1]Computer Security Lab - Federal University of Santa Catarina (UFSC), Florianópolis-SC, Brazil
[2] Federal University of Technology - Parana (UTFPR), Toledo-PR, Brazil
[3] Technology Innovation Institute (TII), Abu Dhabi, UAE

October 6, 2023

Introduction

- Network protocols and Transport Layer Security (TLS) 1.3
  - Widely used
  - Rely on Public-Key Cryptography
- Requirements:
  - Security:
    - Authenticated Key Exchange (AKE)
  - But performance is paramount
    - Applications: Internet browsing, Internet-of-Things (IoT), Microservices, etc.

LabSEC Laboratório de Segurança em Computação

Main Problem

- Public-Key Cryptography (PKC) schemes are insecure under the threat of a Cryptographically Relevant Quantum Computer (CRQC) [4]
  - Shor's algorithm [7] breaks public-key schemes in use today
  - *record-now-decrypt-later* attacks urge for a solution

- Post-Quantum Cryptography (PQC) transition: adoption of new schemes of cryptography
  - Expected security in both classical and quantum computing paradigms

LabSEC Laboratório de Segurança em Computação

PQC adoption in TLS

- PQTLS (Post-Quantum TLS)
  - **Key Exchange:** Key Encapsulation Mechanism (KEM)
  - **Authentication:** Post-quantum digital signatures
- KEMTLS
  - **Key Exchange:** Key Encapsulation Mechanism
  - **Authentication:** Key Encapsulation Mechanism

LabSEC
Laboratório de Segurança em Computação

PQC adoption challenges

- Performance of PQC
  - Computational cost
  - Network Protocol level: increased sizes
- Confidence in PQC's security
  - Underlying mathematical problem → Algorithm → Implementation
  - Studying time / algorithm scrutiny time / code verification & analysis time

LabSEC
Laboratório de Segurança em Computação

PQC adoption challenges

- Performance of PQC
  - Computational cost
  - Network Protocol level: increased sizes
  - **KEMTLS: PQ Key Encapsulation Mechanisms (KEMs) in TLS** [6]
- Confidence in PQC's security
  - Underlying mathematical problem → Algorithm → Implementation
  - Studying time / algorithm scrutiny time / code verification & analysis time

LabSEC Laboratório de Segurança em Computação

PQC adoption challenges

- Performance of PQC
  - Computational cost
  - Network Protocol level: increased sizes
  - **KEMTLS: PQ Key Encapsulation Mechanisms (KEMs) in TLS** [6]
- Confidence in PQC's security
  - Underlying mathematical problem → Algorithm → Implementation
  - Studying time / algorithm scrutiny time / code verification & analysis time
  - **Hybrid PQC: combining PQC with classical schemes**

LabSEC Laboratório de Segurança em Computação

PQC adoption challenges

- Performance of PQC
  - Computational cost
  - Network Protocol level: increased sizes
  - **KEMTLS: PQ Key Encapsulation Mechanisms (KEMs) in TLS** [6]
- Confidence in PQC's security
  - Underlying mathematical problem → Algorithm → Implementation
  - Studying time / algorithm scrutiny time / code verification & analysis time
  - **Hybrid PQC: combining PQC with classical schemes**

KEMTLS has not yet been analyzed in the hybrid mode

LabSEC Laboratório de Segurança em Computação

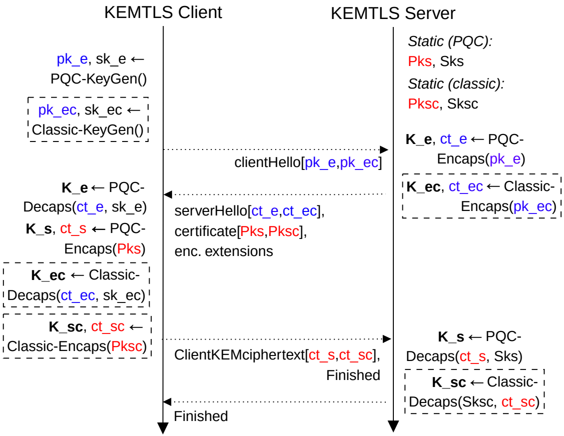
Contributions

1. A Hybrid KEMTLS design and implementation[1]
   - Adding classical cryptography to all of NIST's Round 3 finalist KEM schemes;
2. An extensive evaluation of the Hybrid KEMTLS
   - Considering simulated networks and geographical-distant servers;
3. A comparison of Hybrids between KEMTLS, KEMTLS-PDK, and PQTLS,
   - Under the same network conditions and security levels

LabSEC Laboratório de Segurança em Computação

[1] `https://github.com/AAGiron/hybrid-kemtls-tests`

Hybrid KEMTLS Handshake



Hybrid KEMTLS Key Schedule

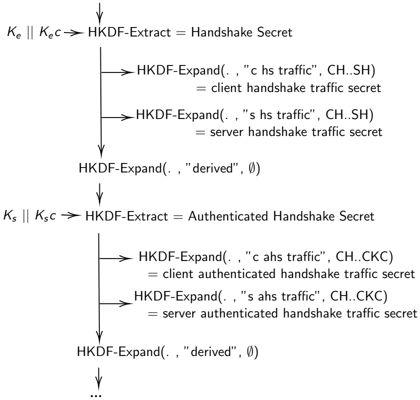


Figure: Snippet of the Hybrid KEMTLS Key Schedule[2]

[2] Early Secret and Master Secret were omitted

Hybrid KEMTLS Key Schedule

Hybrid KEMTLS incorporates the dualPRF combiner, proposed by Bindel et al. [1]

- Paper: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange
- Security is mantained even if one of the KEMs is compromised

Evaluation Methodology

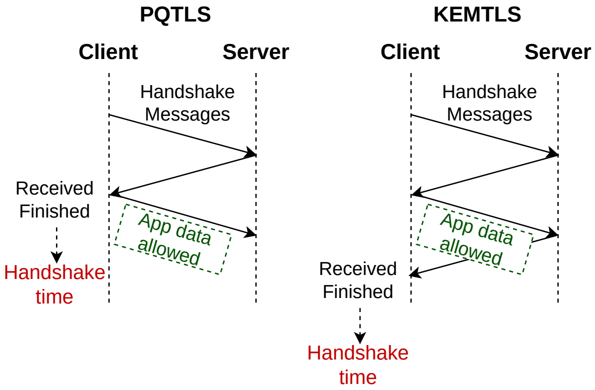
1. Environment:
   - **Geographical-distant servers:**
     Central Europe and South America
   - **Simulated network[3]:**
     Parameters: Latency and packet loss probabilities
2. Metrics:
   - Handshake completion time
   - Time to send application data
   - Hybrid Penalty
3. Implementations:
   - Go Standard Library[4]
   - OQS liboqs-go wrapper [5]

[3] Using NetEM[3], Linux's network emulator

[4] Adapted from Celi et al. [2]

Evaluation Methodology

Handshake time vs Time to send application data



LabSEC Laboratório de Segurança em Computação

KEMs Computational Cost

Timings for 100 executions

Security Level	KeyGen		Encaps		Decaps	
	Kyber (PQ)	Kyber (Hybrid)	Kyber (PQ)	Kyber (Hybrid)	Kyber (PQ)	Kyber (Hybrid)
1	0.02 ms	0.04 ms	0.02 ms	0.12 ms	0.01 ms	0.01 ms
3	0.02 ms	0.39 ms	0.02 ms	0.77 ms	0.02 ms	0.75 ms
5	0.03 ms	6.5 ms	0.03 ms	12.9 ms	0.02 ms	12.7 ms

LabSEC Laboratório de Segurança em Computação

Hybrid Penalty in Geographical-distant servers

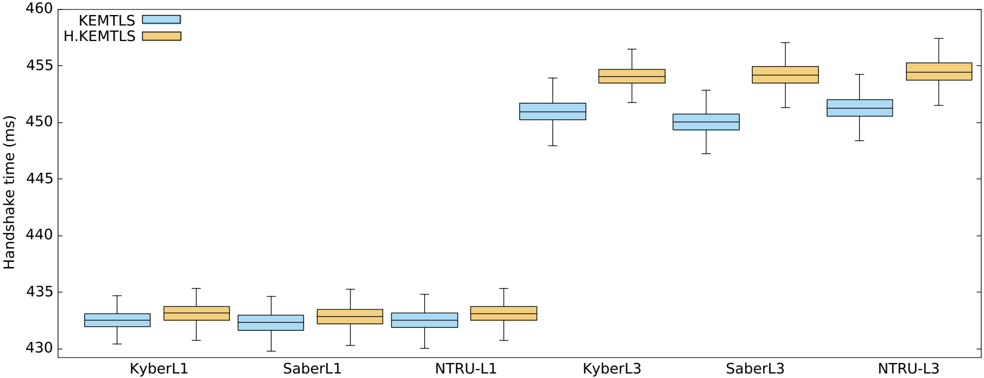


Figure: KEMTLS and Hybrid KEMTLS (L1-L3)

Hybrid Penalty in Geographical-distant servers

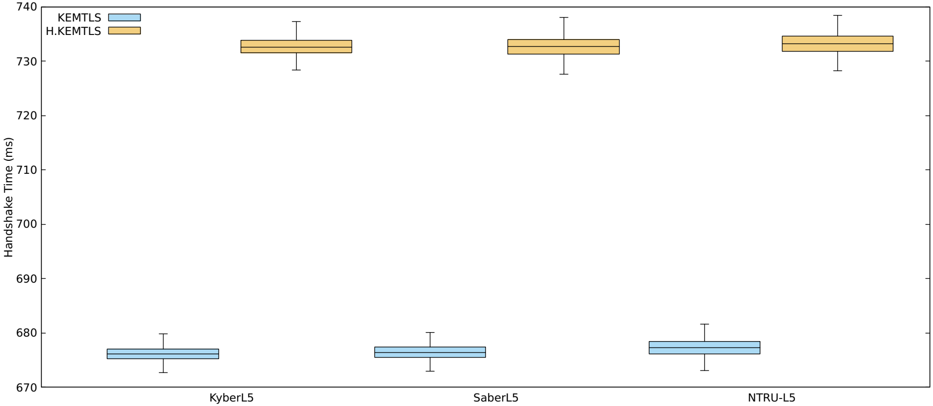


Figure: KEMTLS and Hybrid KEMTLS (L5)

Hybrid Penalty in Simulated Environment

Latency

Table: Average Handshake time (in ms) for PQC-Only and Hybrid KEMTLS

Algorithm and Security Level	Latency: 1 ms			Latency: 5 ms			Latency: 50 ms			Latency: 150 ms		
	HS Time	Penalty	St. Dev.	HS Time	Penalty	St. Dev.	HS Time	Penalty	St. Dev.	HS Time	Penalty	St. Dev.
KyberL1	6.0	-	0.4	22.3	-	0.3	202.8	-	0.2	602.9	-	0.2
KyberL1 H.	7.0	**1.0**	0.4	23.2	**0.9**	0.3	203.6	**0.9**	0.3	603.7	**0.8**	0.4
KyberL3	38.5	-	0.8	54.8	-	0.8	236.3	-	1.0	636.6	-	1.0
KyberL3 H.	46.8	**8.3**	0.9	62.9	**8.1**	2.3	243.2	**6.9**	1.2	643.9	**7.3**	1.6
KyberL5	63.0	-	0.8	78.4	-	0.8	261.1	-	6.0	659.9	-	1.0
KyberL5 H.	194.6	**131.6**	2.4	211.4	**133.0**	3.7	393.0	**132.0**	4.5	791.6	**131.7**	3.2

LabSEC Laboratório de Segurança em Computação

Hybrid Penalty in Simulated Environment

Packet loss probability

Table: Time-to-send-app-data (in ms) considering different packet loss probabilities.

Algorithm and	**Packet Loss: 1%**		**Packet Loss: 2%**		**Packet Loss: 3%**		**Packet Loss: 5%**	
Security Level	**Median**	**95% percentile**	**Median**	**95% percentile**	**Median**	**95% percentile**	**Median**	**95% percentile**
KyberL1	1.6	2.9	1.6	3.3	1.6	207.5	1.7	208.3
KyberL1 H.	2.3	3.4	2.3	7.9	2.3	207.3	2.4	209.4
KyberL3	34.0	36.1	34.3	39.2	34.8	239.6	34.9	242.0
KyberL3 H.	39.9	42.1	39.8	43.4	40.3	246.1	40.7	247.2
KyberL5	58.4	60.9	58.5	63.6	57.6	263.1	58.9	266.3
KyberL5 H.	162.6	166.8	162.0	167.2	161.0	359.2	162.1	368.0

LabSEC Laboratório de Segurança em Computação

Hybrid KEMTLS vs Hybrid PQTLS

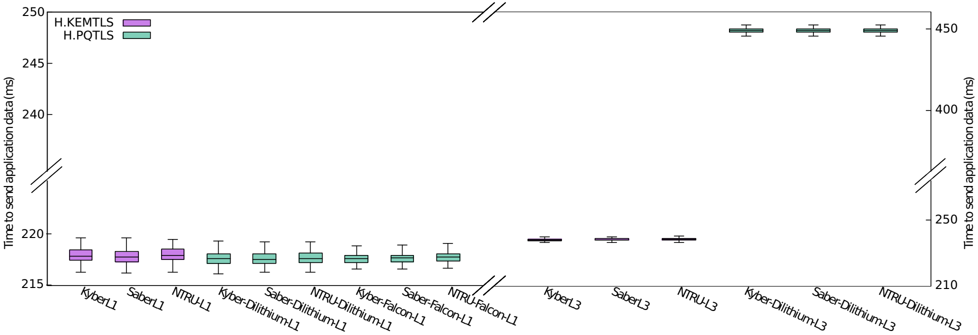


Figure: Hybrid comparison (L1-L3) in geographical-distant servers experiments

LabSEC Laboratório de Segurança em Computação

Hybrid KEMTLS vs Hybrid PQTLS

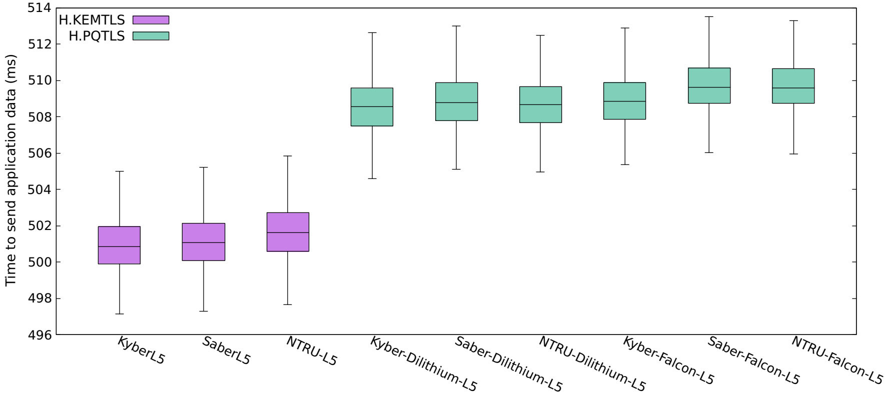


Figure: Hybrid comparison (L5) in geographical-distant servers experiments

Final Remarks

- Small hybrid penalty in KEMTLS in instantiations with lower security level parameters
- Closely matched average timing for NIST's Round 3 finalists schemes
- Network thresholds can greatly affect instantiations with bigger handshake sizes

LabSEC Laboratório de Segurança em Computação

Thank you for your attention!

Contact:
alexandregiron@utfpr.edu.br
joao.pedro.nascimento@grad.ufsc.br

LabSEC
Laboratório de Segurança em Computação

References I

- Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila.
  Hybrid key encapsulation mechanisms and authenticated key exchange.
  In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 206–226, Cham, 2019. Springer International Publishing.

- Sofía Celi, Armando Faz-Hernández, Nick Sullivan, Goutam Tamvada, Luke Valenta, Thom Wiggers, Bas Westerbaan, and Christopher A. Wood.
  Implementing and measuring kemtls.
  In Patrick Longa and Carla Ràfols, editors, *Progress in Cryptology – LATINCRYPT 2021*, pages 88–107, Cham, 2021. Springer International Publishing.

LabSEC Laboratório de Segurança em Computação

References II

- Stephen Hemminger.
  Linux network emulator.
  Online, 2011.
  https://www.linux.org/docs/man8/tc-netem.html.

- Michele Mosca and Marco Piani.
  Quantum threat timeline report 2020.
  Available at: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/. Accessed on 20.07.2021., 2020.

- Open Quantum Safe Project.
  liboqs-go: Go bindings for liboqs.
  Available at: https://github.com/open-quantum-safe/liboqs-go, 2022.
  [Online; accessed 25-Jan-2022].

LabSEC Laboratório de Segurança em Computação

References III

Peter Schwabe, Douglas Stebila, and Thom Wiggers.
Post-Quantum TLS Without Handshake Signatures, page 1461–1480.
Association for Computing Machinery, New York, NY, USA, 2020.

Peter W Shor.
Algorithms for quantum computation: discrete logarithms and factoring.
In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134, Santa Fe, NM, USA, 1994. IEEE, IEEE.

LabSEC
Laboratório de Segurança em Computação