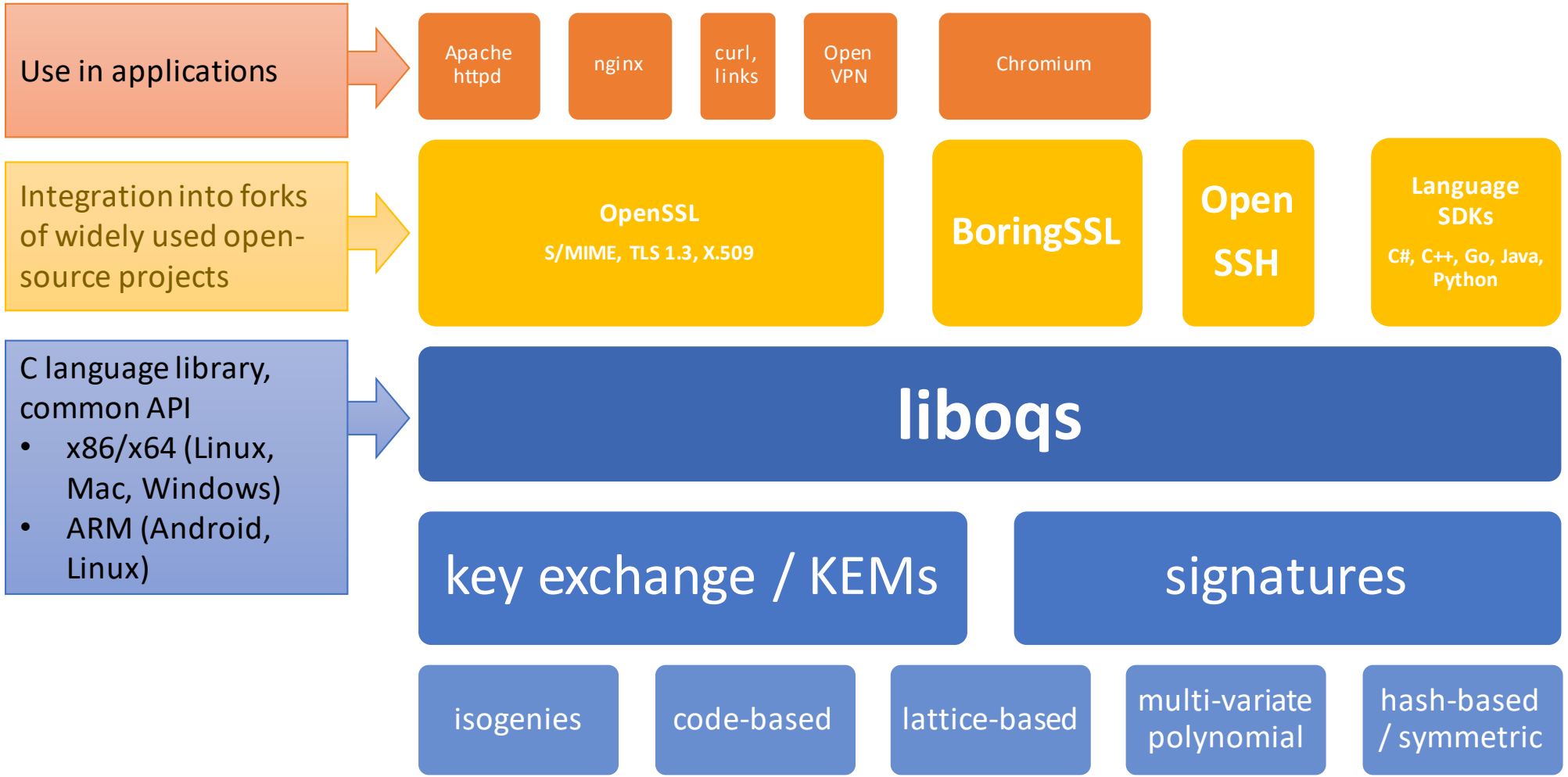
Prototyping post-quantum crypto in software and Internet protocols

Douglas Stebila

Open Quantum Safe Project



Industry partners:
- Amazon Web Services
- evolutionQ
- IBM Research
- Microsoft Research

Additional contributors:
- Cisco
- Senetas
- Individuals

Financial support:
- AWS
- Canadian Centre for Cyber Security
- NSERC

https://openquantumsafe.org/ • https://github.com/open-quantum-safe/

Constraints on PQ in SSH and TLS

Eric Crockett, Christian Paquin, Douglas Stebila. **Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.** NIST 2nd PQC Standardization Conference, August 2019. https://eprint.iacr.org/2019/858

1 Protocol limits too small

TLS 1.3 max certificate size: 2^{24}-1 bytes
TLS 1.3 max signature size: 2^{16}-1 bytes
- Picnic L3, L5 too big

SSHv2 max packet size: 2^{18} bytes
- Rainbow III, V too big

Need protocol changes to fix

2 Default buffers too small

OpenSSL max certificate size: 102,400 B
OpenSSL max signature size: 2^{14} bytes
- Picnic L1, most SPHINCS too big

OpenSSL max key exchange size: 20 KB
- FrodoKEM L5 too big

Can be fixed by increasing buffer size and recompiling

Internet-Draft for hybrid key exchange in TLS 1.3

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 17 October 2020

D. Stebila
University of Waterloo
S. Fluhrer
Cisco Systems
S. Gueron
U. Haifa, Amazon Web Services
15 April 2020

Hybrid key exchange in TLS 1.3
draft-ietf-tls-hybrid-design-00

Abstract

Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography. This document provides a construction for hybrid key exchange in the Transport Layer Security (TLS) protocol version 1.3.

Discussion of this work is encouraged to happen on the TLS IETF mailing list tls@ietf.org or on the GitHub repository which contains the draft: https://github.com/dstebila/draft-ietf-tls-hybrid-design.

https://tools.ietf.org/id/draft-ietf-tls-hybrid-design-00.txt

Internet-Draft specifying hybrid key exchange in TLS 1.3

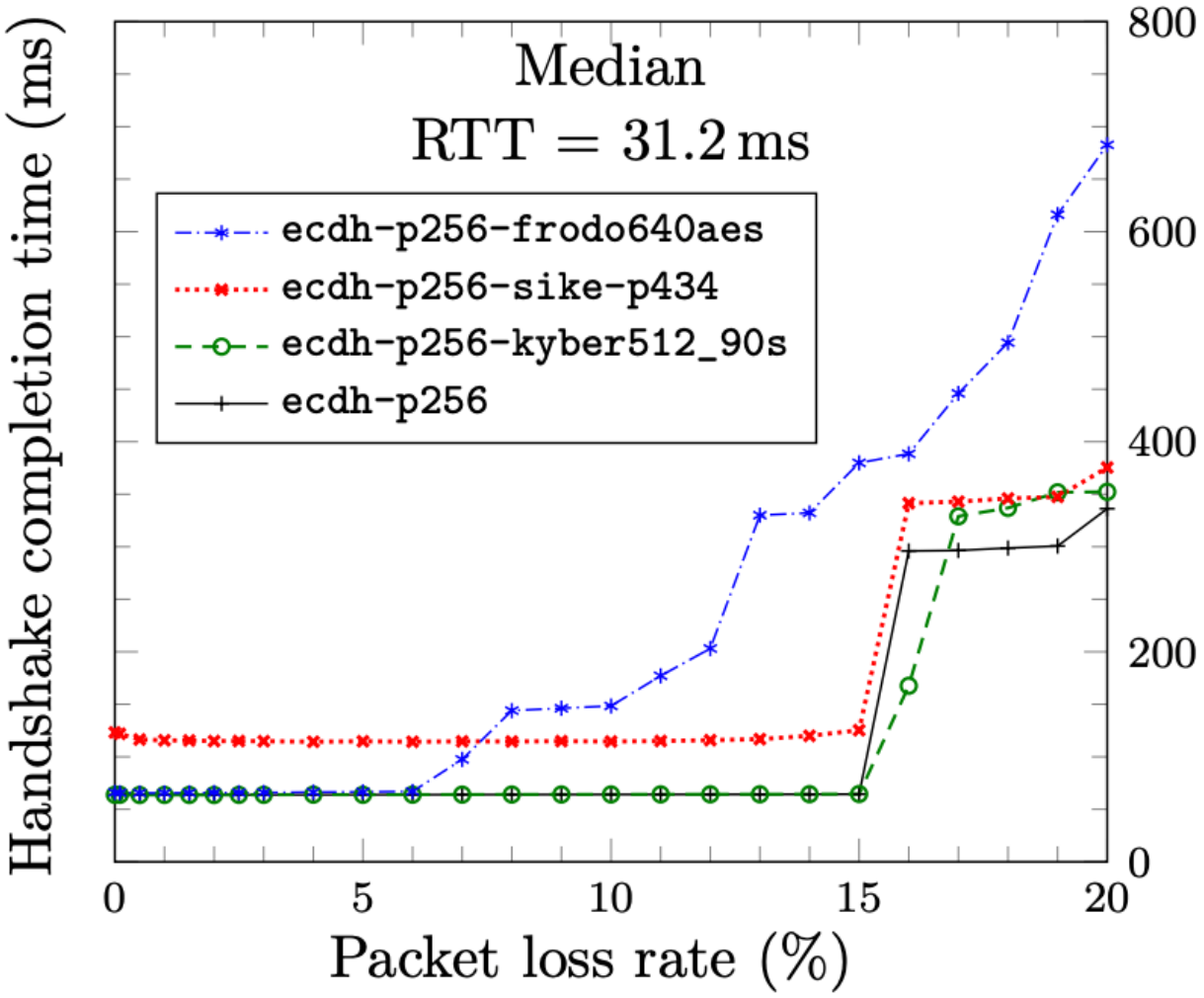
PQ algorithm agnostic

Demo software:
https://github.com/open-quantum-safe/oqs-demos

Interop test server:
https://test.openquantumsafe.org

Benchmarking PQ crypto in TLS

Christian Paquin, Douglas Stebila, Goutam Tamvada. **Benchmarking post-quantum cryptography in TLS.** PQCrypto 2020.
https://eprint.iacr.org/2019/1447



Measured effect of packet loss rate and connection latency on TLS handshake time for various PQ KEMs and signatures using a network emulation framework

PQ TLS without signatures

Peter Schwabe, Douglas Stebila, Thom Wiggers. **Post-quantum TLS without handshake signatures.** ACM CCS 2020.
https://eprint.iacr.org/2020/534

Problem: Post-quantum signatures are bigger than post-quantum KEMs.

Idea: Use KEMs for authenticated key exchange in the TLS handshake to save space.

- Simple to implement
- With isogenies, can get handshake size very close to current sizes
- Implicit rather than explicit authentication
- Different forward secrecy and downgrade resilience properties
- Increased benefits when caching intermediate CA certificates
- Interesting questions about certificate lifecycle management
- Working with Cloudflare to test within their infrastructure

UNIVERSITY OF WATERLOO

Lessons learned re: PQ software

1 Size constraints

Unexpected bugs due to larger public keys / ciphertexts / signatures

2 Memory constraints

Large stack usage problematic in multi-threaded software

3 API problems

NIST competition focuses on Key Encapsulation Mechanisms, but some cryptographic APIs lack abstractions for KEMs (e.g., OpenSSL EVP API)

4 Versioning difficulties

While NIST competition still in progress, algorithm specifications continue to change. Interoperability and algorithm versioning hard. Important to **not** set de facto algorithm standards now.

Thanks

Open Quantum Safe core team

Michael Baentsch
Eric Crockett
Vlad Gheorghiu
Christian Paquin
Goutam Tamvada

Research collaborators

Eric Crockett
Scott Fluhrer
Shay Gueron
Christian Paquin
Peter Schwabe
Goutam Tamvada
Thom Wiggers

Funding

Amazon Web Services
Canadian Centre for Cyber Security
Natural Sciences and Engineering Research Council of Canada (NSERC)

Prototyping post-quantum crypto in software and Internet protocols

Open Quantum Safe project
https://openquantumsafe.org/
https://github.com/open-quantum-safe/

Internet-Draft for hybrid key exchange in TLS 1.3
https://tools.ietf.org/id/draft-ietf-tls-hybrid-design-00.txt
https://github.com/open-quantum-safe/oqs-demos
https://test.openquantumsafe.org

Constraints on PQ in SSH and TLS
https://eprint.iacr.org/2019/858

Benchmarking PQ crypto in TLS
https://eprint.iacr.org/2019/1447

PQ TLS without signatures
https://eprint.iacr.org/2020/534

Douglas Stebila

UNIVERSITY OF WATERLOO