Updates from the Open Quantum Safe project

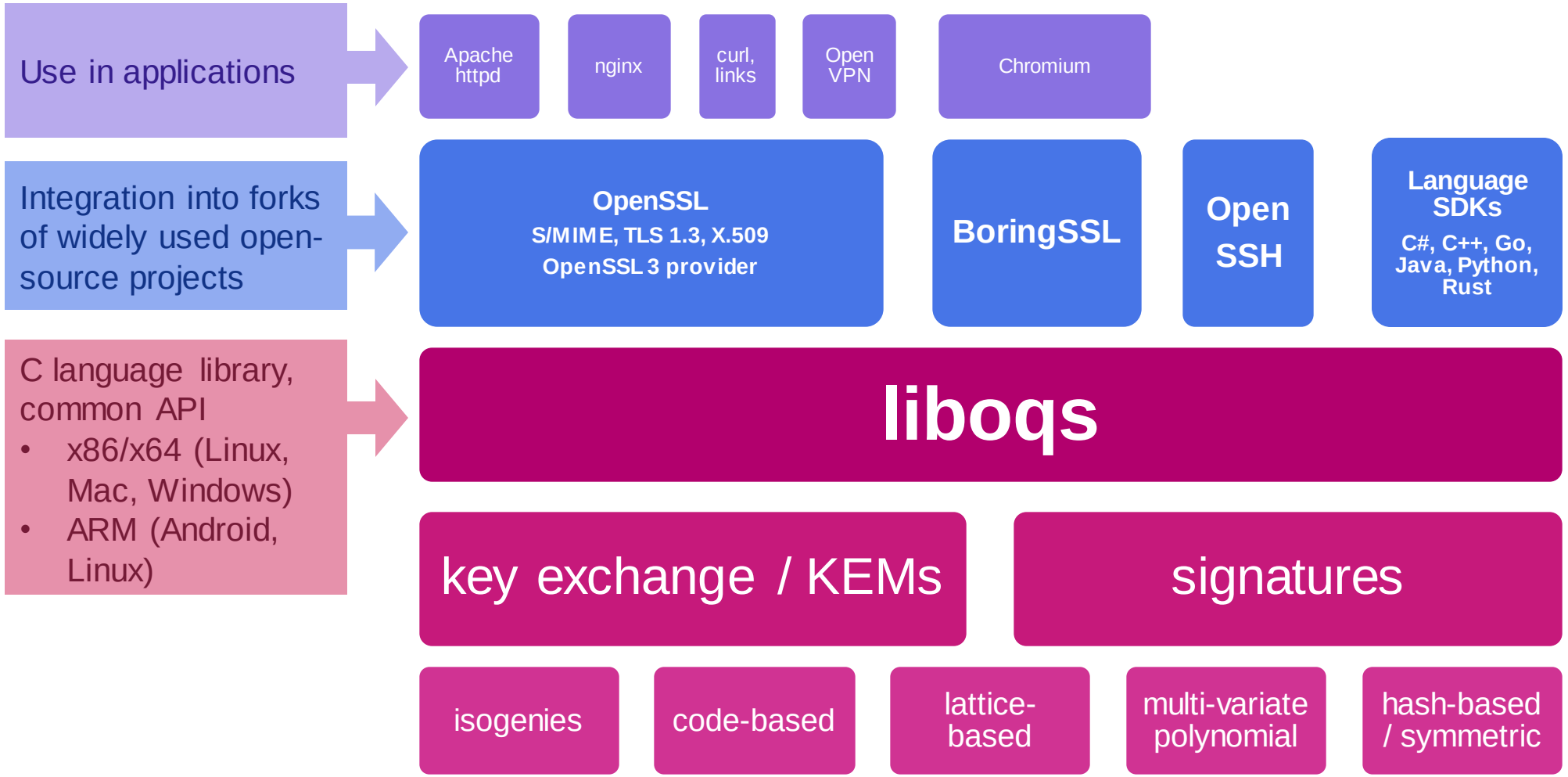
John Schanck

OQS core team: **Michael Baentsch**, **Eric Crockett** (AWS), **Vlad Gheorghiu** (University of Waterloo), **Basil Hess** (IBM Research), **Christian Paquin** (Microsoft Research), **John Schanck** (University of Waterloo), **Douglas Stebila** (University of Waterloo), **Goutam Tamvada** (University of Waterloo)

https://openquantumsafe.org

https://github.com/open-quantum-safe

Open Quantum Safe Project



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

Additional contributors:
- Cisco
- Senetas
- PQClean project
- Individuals

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

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

liboqs

- Implementations from PQClean or direct contribution
- MIT License (and other free licenses)
- Builds on Windows, macOS, Linux; x86-64, ARM32v7, ARM64v8
- Wrappers for C++, Go, Java, .Net, Python, Rust

https://openquantumsafe.org/liboqs/

liboqs

- Version 0.5.0 released March 2021
  - Includes all Round 3 submissions (except GeMSS)
    - Some implementations still Round 2 versions
  - More robust testing:
    - LLVM address and undefined behavior sanitizers
    - Secret-dependent branching using Valgrind

- Version 0.6.0 to be released in June 2021
  - Algorithm updates
  - Common code deduplication (SHA3)
  - New build options and cross-compilation support
  - Improved code dispatching

https://openquantumsafe.org/liboqs/

TLS 1.3 implementations

	OQS-OpenSSL 1.1.1	OQS-OpenSSL 3 provider	OQS-BoringSSL
PQ key exchange in TLS 1.3	Yes	Yes	Yes
Hybrid key exchange in TLS 1.3	Yes	Coming soon	Yes
PQ certificates and signature authentication in TLS 1.3	Yes	API change required	Yes
Hybrid certificates and signature authentication in TLS 1.3	Yes	API change required	No

Using draft-ietf-tls-hybrid-design for hybrid key exchange

Interoperability test server running at https://test.openquantumsafe.org

https://openquantumsafe.org/applications/tls/

Applications

- Demo integrations into:
  - Apache
  - nginx
  - haproxy
  - curl
  - Chromium
- Docker images available.

- In most cases integration of updated OpenSSL required few/no modifications to application.
- Some algorithm-specific issues remain.

https://openquantumsafe.org/applications/tls/#demo-integrations

Other protocols

SSH

- Fork of OpenSSH v7 (soon: v8)
- PQ and hybrid key exchange
- PQ and hybrid authentication

CMS/SMIME

- In fork of OpenSSL
- PQ and hybrid signatures

X.509

- In fork of OpenSSL
- PQ and hybrid signatures

Benchmarking

https://openquantumsafe.org/benchmarking/

- Core algorithm speed and memory usage
- TLS performance in ideal network conditions
- Currently benchmarking on:
  - Intel Cannon Lake
  - ARM Cortex-A72 (reference code only)

Use in prototyping & research

- **Cisco**: Post-quantum TLS 1.3 and SSH performance (preliminary results)
  - https://blogs.cisco.com/security/tls-ssh-performance-pq-kem-auth
- **IBM**: IBM Cloud delivers quantum-safe cryptography and Hyper Protect Crypto Services to help protect data in the hybrid era
  - https://newsroom.ibm.com/2020-11-30-IBM-Cloud-Delivers-Quantum-Safe-Cryptography-and-Hyper-Protect-Crypto-Services-to-Help-Protect-Data-in-the-Hybrid-Era
  - https://github.com/IBM/qsc-ingress
- **Microsoft Research**: Post-quantum cryptography VPN
  - https://github.com/Microsoft/PQCrypto-VPN
- **strongSwan**: Post-quantum cryptography in IKEv2 using strongSwan
  - https://github.com/strongX509/docker/tree/master/pq-strongswan

https://openquantumsafe.org/research/

- **PQFabric: A permissioned blockchain secure from both classical and quantum attacks**, by Bhargav Das, Amelia Holcomb, Michele Mosca, and Geovandro C. C. F. Pereira. arXiv:2010.06571.
- **Post-quantum TLS without handshake signatures**, by Peter Schwabe, Douglas Stebila, and Thom Wiggers. ACM CCS 2020.
- **Benchmarking post-quantum cryptography in TLS**, by Christian Paquin, Douglas Stebila, and Goutam Tamvada. PQCrypto 2020.
- **Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH**, by Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. CoNEXT 2020.
- **Post-quantum authentication in TLS 1.3: A performance study**, by Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. NDSS 2020.
- **Towards quantum-safe VPNs and Internet**, by Maran van Heesch, Niels van Adrichem, Thomas Attema, and Thijs Veugen.
- **Two PQ signature use-cases: Non-issues, challenges and potential solutions**, by Panos Kampanakis and Dimitrios Sikeridis. 7th ETSI/IQC Quantum Safe Cryptography Workshop 2019.

Contributions welcome!

https://github.com/open-quantum-safe/