OPEN QUANTUM SAFE

November 2023 release call

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

Led by University of Waterloo

Industry partners:
- Amazon Web Services
- Cisco
- evolutionQ
- IBM Research
- Microsoft Research
- SandboxAQ
- softwareQ

Additional contributors:
- PQClean project
- Individuals

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

Use in applications
- Apache httpd
- nginx
- curl, links
- OpenVPN

Integration into major libraries and languages
- C language library, common API
  - x86/x64, ARM, ...
  - Linux, Mac, Windows, Android

OpenSSL 3 Provider
- S/MIME, TLS 1.3, X.509

OpenSSH & libssh forks

Language SDKs
- C#, C++, Go, Java, Python, Rust

liboqs

key exchange / KEMs
- isogenies
- code-based
- lattice-based

signatures
- multi-variate polynomial
- hash-based / symmetric
liboqs
version 0.9.0
released October 12, 2023

Main updates:

- Classic McEliece updated to Round 4 version
- aarch64 implementations added for Kyber, Dilithium, Falcon
- Support for compiling for Windows on ARM64, Apple mobile, and Android platforms
liboqs work in progress

- Update HQC to Round 4 version
- Add support for stateful hash-based signatures
  - HSS/LMS
  - XMSS
- Improved documentation and unit testing
- Next target release: December 2023

Future goals:

- Formally verified implementation of Kyber from libjade
- Inclusion of selected signature on-ramp candidates – need community help!
What about updating Kyber and Dilithium to FIPS versions?

Waiting for resolution of incompatibility between version in NIST FIPS drafts and PQ-Crystals team updated software.

Anticipate having Kyber / Dilithium Round 3 and ML-KEM / ML-DSA both present for a period of time.
oqs-provider

version 0.5.2
released October 21, 2023

No major release as no functionally relevant liboqs update referenced

KEM en/decoders added
oqs-provider work in progress

- Fix various bugs (e.g., threading: #272)
- Add oqsprovider to brew (#227)
- Hash-n-sign support (#239)
- Include liboqs 0.10.0 (HQC) → Target date Dec 2023

Future goals:

- Add XMSS/LMS support
  - Unclear whether on same or separate branch
- Get code (security) review done and further harden the code base
  - Interdependence to liboqs (and its upstreams) not yet clear
OQS-OpenSSH
snapshot 2023-10
released October 21, 2023

McEliece alg names updated
OQS-OpenSSH work in progress

Future goals:

- Contribute to OpenSSH upstream by helping maintain currently supported quantum-safe KEMs (streamlined NTRU Prime + x25519) and adding support for additional KEMs.
Epiphany and ngtcp integrations moved to OpenSSL3 & oqs-provider

Chromium update

Test server logic updated to PQ chains

Various upstream changes adapted to
liboqs language wrappers

Main updates: new language wrapper releases (0.9.0) for

- liboqs-cpp
- liboqs-go
- liboqs-python
- liboqs-rust
Language wrappers

- Common API across various mainstream languages
- Actively-maintained language wrappers
  - liboqs-cpp (version 0.9.1, released on Nov. 1, 2023)
  - liboqs-go (version 0.9.0, released on Oct. 30, 2023)
  - liboqs-python (version 0.9.0, released on Oct. 30, 2023)
  - liboqs-rust (version 0.9.0 (oqs)/0.9.1 (oqs-sys), released on Oct. 19/Oct. 23, 2023)
- Less frequently updated
  - liboqs-dotnet (version 0.3.0, released on Jul. 9, 2020)
- Inactive
  - liboqs-java (version 0.1.0, released on Jul. 9, 2021)
liboqs-rust

- **Two crates**
  - `oqs`: Idiomatic Rust interface to liboqs
  - `oqs-sys`: Direct ffi interface to liboqs (mostly generated via `bindgen`)
    - This crate builds or finds (since 0.9.0) liboqs depending on vendored feature

- **Versioning up to (and including) 0.9.0 tied to liboqs**
  - Future releases will be dependent on breaking changes (both Rust-side and liboqs-side) and independent of liboqs releases
  - Downstream demands for API/packaging features/fixes had been held back in the past
  - `oqs-sys` crate will include packaged liboqs version in version number for visibility
    - e.g. `oqs-sys version 0.X.Y+liboqs-0.9.0`
    - Stuff after + is not used in dependency resolution
    - Currently the vendored liboqs version is the minimum looked-for liboqs version by pkg-config, might need to loosen this restriction at some point.
  - `main` branch now locked to latest liboqs release (no more weekly dependabot merges)
Organizational plans

In discussions to move OQS into the Linux Foundation as a permanent home
Contact Douglas Stebila for information on joining the discussion
Your feedback

- How are you using OQS?
- What features do you need?
- How would you like to be involved?