

Post-Quantum Cryptography in OpenPGP

Securing email encryption & signing against
cryptographically relevant quantum computers

OpenPGP today

- Released RFC 9580 in July 2024
 - Obsoletes RFC 4880 from November 2007
 - Modernized the available cryptography
 - But everything is still classical cryptography



By IBM Research

State of quantum computers

Published on May 11, 2022 [In AI Features](#)

Fault-tolerant quantum computing era is a decade away: Srinjoy Ganguly, Fractal

"A practical quantum computer is now less than 10 years away"

📅 22 March 2006

QUANTUM | NEWS

Practical quantum computers remain at least a decade away

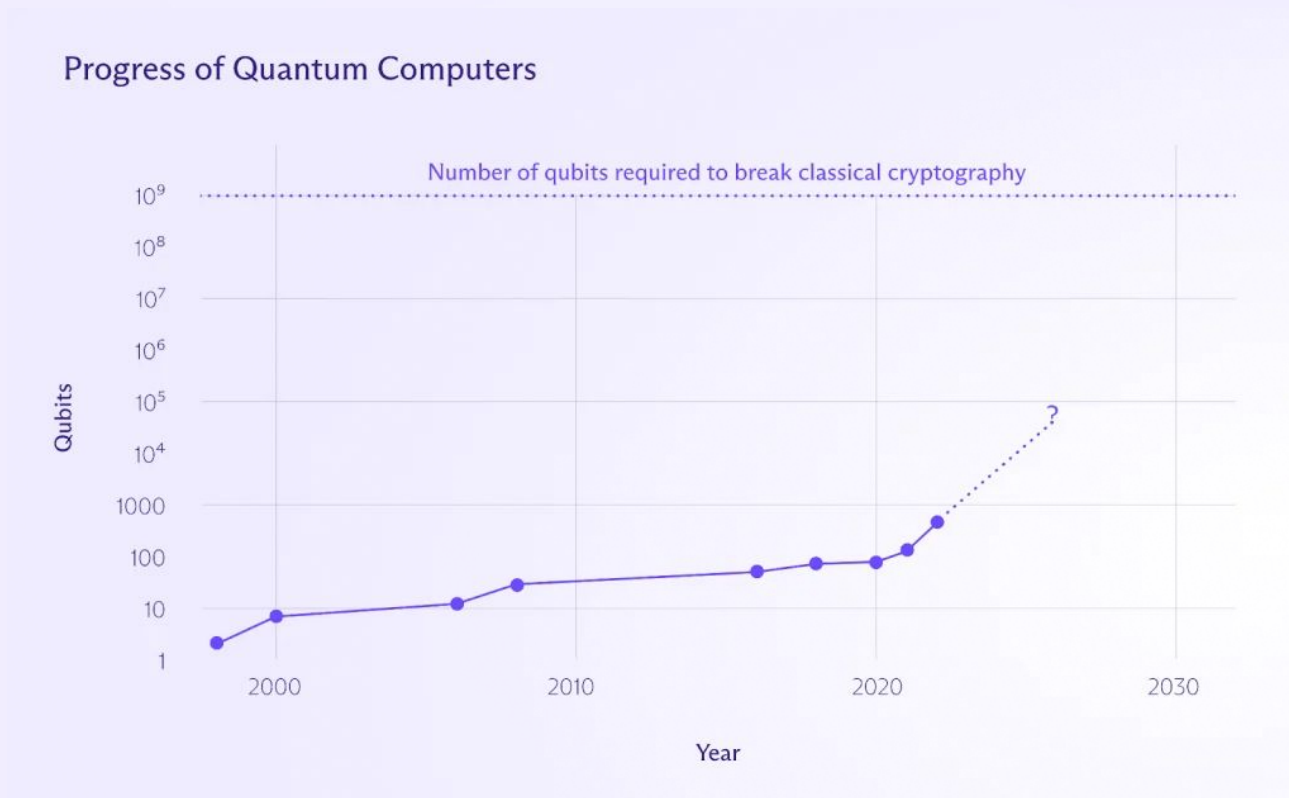
12 Dec 2018

Quantum computing stocks tumble after Nvidia CEO says "very useful" quantum computers are 20 years away

"Jensen threw a wet blanket on the quantum story"

By [Shawn Knight](#) January 8, 2025 at 3:50 PM | [26 comments](#)

State of quantum computers



State of quantum computers



Quantum computing promises to solve problems that are out of reach for classical systems, but today's quantum computers are still experimental, noisy, and lack scalability.

So why are we already building software for them?

This will be discussed tomorrow afternoon in room K.4.401, here we discuss why do we build software against them.

Post-quantum cryptography (PQC)

- There exists cryptography running on classical computers, that cannot (yet) be broken by quantum computers:
 - Some trapdoor problems for asymmetric cryptography are also resistant: Lattice, Error-correction, Multivariate, Hash, ...
 - But larger and slower than classical
 - Symmetric cryptography is just partially affected
- NIST standardized in 2024: ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205)

The OpenPGP PQC project

- Project started in March 2022 at IETF 113, in Vienna
- A draft in the OpenPGP working group, implements:
 - ML-KEM hybrid with X25519 and X448
 - ML-DSA hybrid with Ed25519 and Ed448
 - SLH-DSA standalone

We aim to bring PQC to the OpenPGP protocol without breaking existing deployments

State of the implementations

The Project PQC@Thunderbird led by MTG AG is implementing the draft in Thunderbird, funded by the BSI

Proton is implementing the draft in the open source libraries it maintains, OpenPGP.js and GopenPGP

Encrypt-Decrypt roundtrip with a PQC key

🔗 pqc v6

Encrypt-Decrypt roundtrip with a PQC key from Appendix A.1 of draft-ietf-openpgp-pqc.

Additional artifacts:

- Certificate 🔗
- Key 🔗

Producer	Consumer					Expectation
	Artifact	GopenPGP 3.0.0-beta.0+pqc	OpenPGP.js 6.0.0-beta.3.patch.1+pqc	mp 0.17.1+pqc		
GopenPGP 3.0.0-beta.0+pqc	🔗	✓	✓	✓	✓	Int
OpenPGP.js 6.0.0-beta.3.patch.1+pqc	🔗	✓	✓	✓	✓	Int
mp 0.17.1+pqc	🔗	✓	✓	✓	✓	Int

Symmetric cryptography

- Asymmetric cryptography may be unnecessary
 - Drafts, archival, etc.
- Symmetric cryptography is faster and post-quantum secure

Persistent symmetric keys

- Normally, OpenPGP keys store asymmetric key material
- Let's store symmetric key material there instead!
- Then, when you encrypt with a private key, it's faster

State of the draft

- Adopted draft in the OpenPGP Working Group

Workgroup:	Network Working Group
Internet-Draft:	draft-ietf-openpgp-persistent-symmetric-keys-01
Updates:	9580 (if approved)
Published:	30 January 2025
Intended Status:	Standards Track
Expires:	3 August 2025
Author:	D. Huigens, Ed. <i>Proton AG</i>

Persistent Symmetric Keys in OpenPGP

Abstract

This document defines new algorithms for the OpenPGP standard (RFC 9580) to support persistent symmetric keys, for message encryption using authenticated encryption with additional data (AEAD) and for authentication with hash-based message authentication codes (HMAC). This enables the use of symmetric cryptography for data storage (and other contexts that do not require asymmetric cryptography), for improved performance, smaller keys, and improved resistance to quantum computing.

State of the implementations

- Experimental implementations in OpenPGP.js and GopenPGP
- RNP has expressed interest in implementing it
- Hopefully other implementers of PQC will implement both













Encrypt-Decrypt roundtrip with a persistent symmetric key

draft

Encrypt-Decrypt roundtrip using the persistent symmetric key from Appendix A.1 of draft-ietf-openpgp-persistent-symmetric-keys.

Additional artifacts:

- Certificate 
- Key 

Producer	Artifact	Consumer	GopenPGP 3.0.0+pqc	OpenPGP.js 6.0.0+pqc	Expectation	Comment
GopenPGP 3.0.0+pqc					 	Interoperability concern.
OpenPGP.js 6.0.0+pqc					 	Interoperability concern.

Conclusion

- Quantum computers are coming(?)
- Post-quantum cryptography is coming!
- Will be bigger and slower
- But, symmetric case will be smaller and faster

Thanks! Questions?