
Cryptographic Changes Inbound!
You MAY have time to get ready.
This time
Photo by Jens Herrndorff on Unsplash

Disclaimer

This talk contains no maths.

SSL Report: sectigo.com (91.199.212.90)

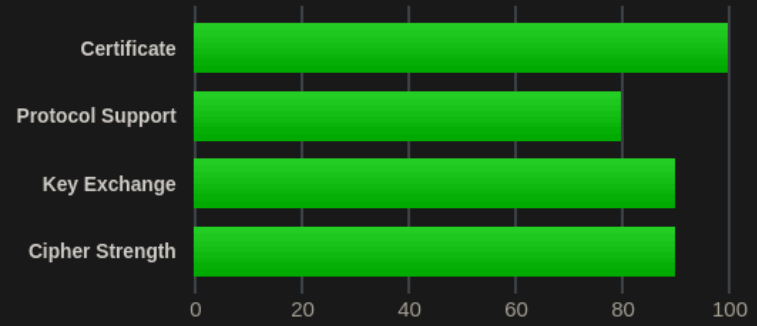
Assessed on: Fri, 27 Feb 2026 13:30:49 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A-



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server does not support TLS 1.3. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Non-Exhaustive Cryptographic Attacks History

Post-Snowden Files

Feature	Attack
SSL 3	POODLE
Compression	CRIME/BREACH
Export-Grade	LogJam
SHA-1	SHAttered

More Recently

Distrusting Entrust

Certificate Lifetime Reduction

Ever had an outage due to an expired Certificate?

(I know I did!)

Max TTLs

Date	TTL (d)
(Current)	398
2026-03-15	200
2027-03-15	100
2029-03-15	47

Rationale

- Reducing the duration of the impacts of a compromised certificate
- Driving adoption of certificate automations (eg: ACME)

90-days corporate renewal policy?

Please Share Tips on How to Update it?

> This is just $hrinkflation!
>
> They want more money for the same service!
>
> En-💩-ification!
>
> - Someone who probably pays for Extended Validation (EV) Certificate

Paying for a certificate?

LetsEncrypt:

- A Free CA
- 90d or 7d certificates
- DV only

Automation

- **ACME: Automated Certificate Management Environment**
- SCEP: Simple Certificate Enrollment Protocol
- CMP: Certificate Management Protocol
- EST: Enrollment over Secure Transport

Post-Quantum Cryptography

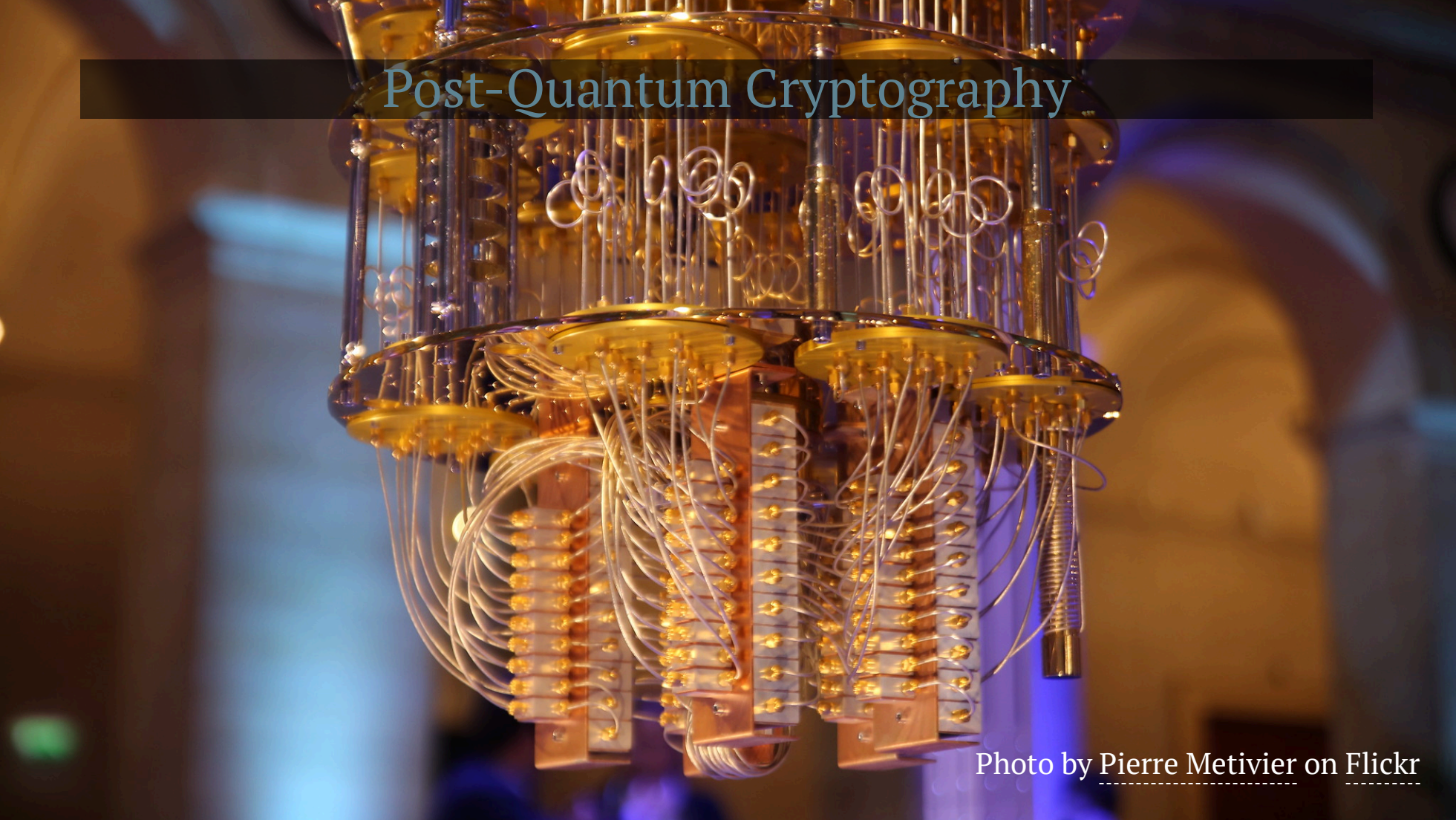


Photo by Pierre Metivier on Flickr

Post-Quantum Cryptography

Effects of Quantum Computers on Algorithms

Symmetric (ex: AES)

Halves effective strength

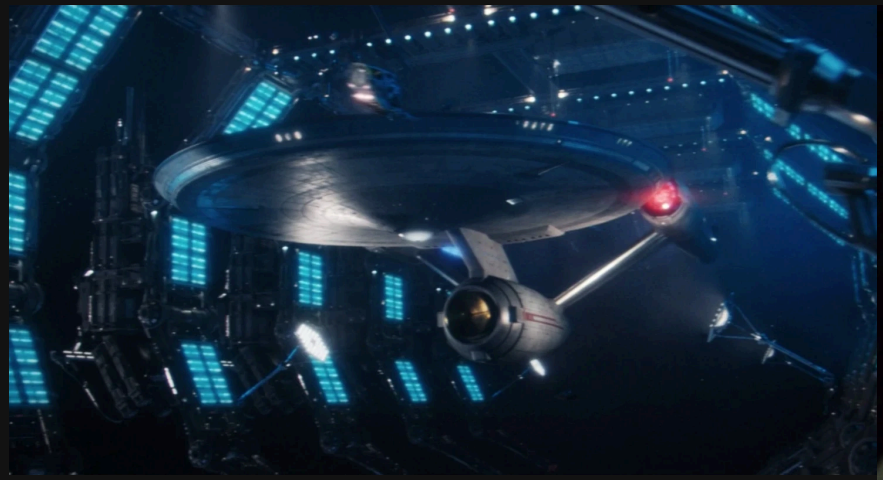
Asymmetric (ex: RSA)

Breaks the cipher

TLS uses Asymmetric Cryptography to negociate Ephemeral (Session) Symmetric Cryptography

First Selected Algorithms: Crystals-Lattice

Dilithium



Source: Memory Alpha

Kyber

Source: Wookiepedia

I’m not as courageous as Rendle to confuse them!

First Selected Algorithms: Crystals-Lattice

Dilithium

ML-DSA

Module-Lattice-Based Digital Signature Algorithm

FIPS-204

Kyber

ML-KEM

Module-Lattice-Based Key Encapsulation Mechanism

FIPS-203

Timeline

2030

PQC Support SHOULD Be Enabled

2035

Traditional Cryptography is Deprecated

Don't Panic