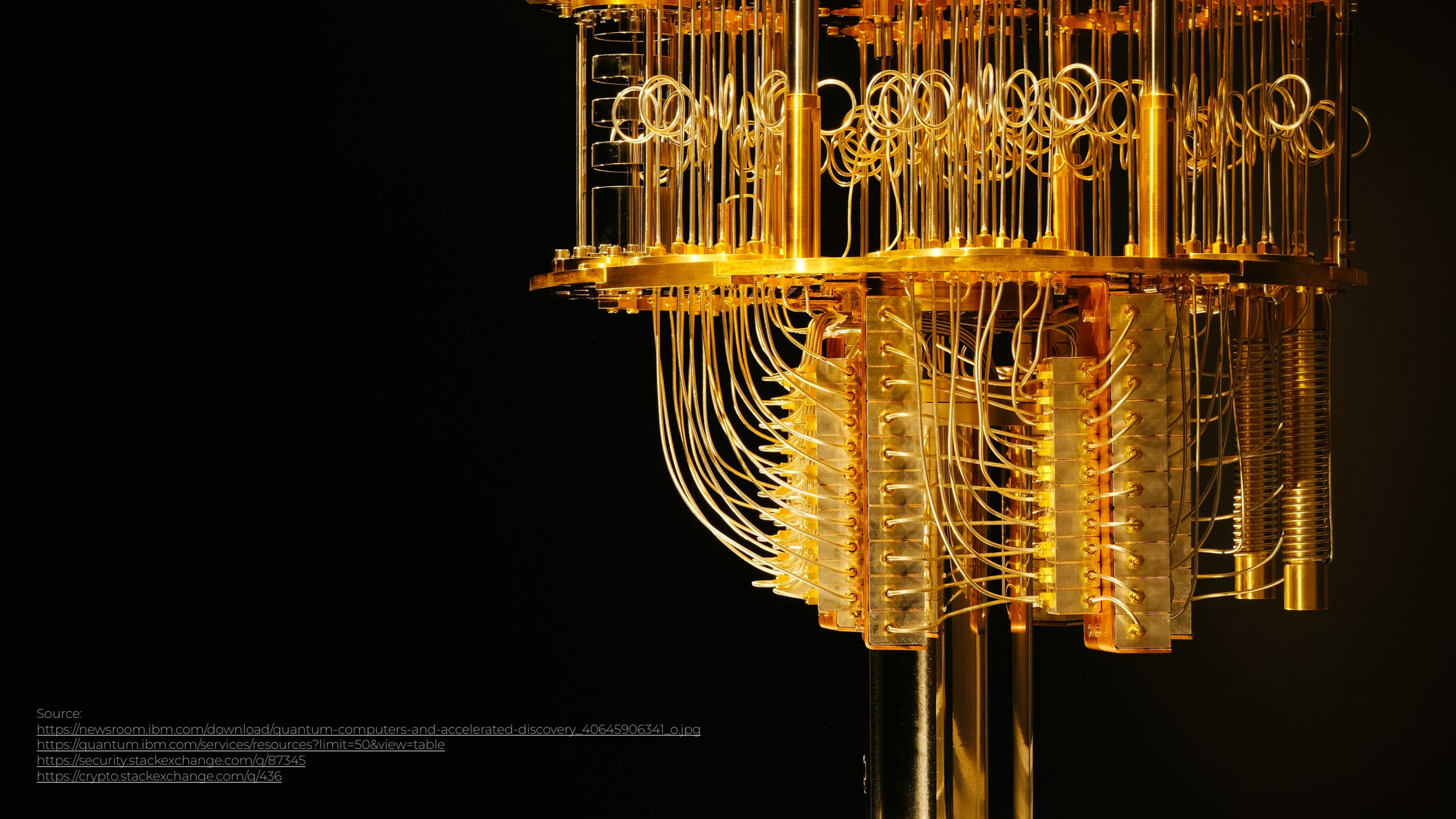
The road ahead to post-quantum cryptography

Clemens Lang
Product Owner RHEL Crypto Team

@neverpanic@chaos.social
cllang@redhat.com
neverpanic



Source:
https://newsroom.ibm.com/download/quantum-computers-and-accelerated-discovery_40645906341_o.jpg
https://quantum.ibm.com/services/resources?limit=50&view=table
https://security.stackexchange.com/q/87345
https://crypto.stackexchange.com/q/436

What we'll cover today

- Quantum Computers
- Harvest now, Decrypt later
- Timelines
- Protocols
  - TLS, SSH
  - OpenPGP

Types of Cryptography

Symmetric

- shared key
- fast
- quantum-safe (with larger keys)

Asymmetric: Key Establishment

- establish shared secret key over public channel
- vulnerable to passive QC attackers

Asymmetric: Signatures

- used for non-repudiation, authentication
- vulnerable against active QC attackers

Harvest now, Decrypt Later

Nobody has a relevant quantum computer today.

Three letter agencies have lots of storage.

Idea:

1) Store encrypted communication now
2) break key exchange when a QC is available
3) ???
4) passwords, medical records, etc.

Booting Up: New NSA Data Farm Takes Root In Utah

SEPTEMBER 23, 2013 · 5:39 PM ET

By Howard Berkes

The National Security Agency says its massive new data center near Salt Lake City will enhance the agency's ability to analyze the email, text message, cellphone and landline metadata it collects.

Rick Bowmer/AP

cllang@redhat.com

Timelines: Regulation

- US: PQC by default between 2025 and 2030
- EU: by 2030-12-31:
  - “PQC transition for high-risk use cases has been completed”
  - “Quantum-safe software and firmware upgrades are enabled by default”
- Many others with similar timelines

cllang@redhat.com

https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/
https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Timelines: Common Sense

Time to transition

Time to build a quantum computer

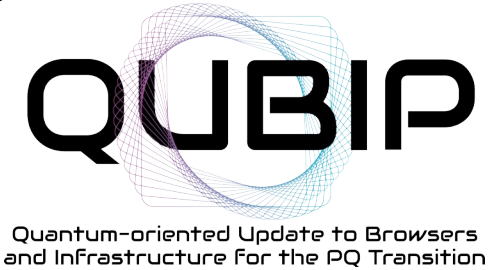
Time you need your data to stay secure

cllang@redhat.com

Protocols

TLS

- TLS 1.3 required
- Standardization ongoing
- OpenSSL, GnuTLS, NSS, Go already support ML-KEM
- OpenSSL, GnuTLS support ML-DSA
- EU Project QUBIP funded some of this work



SSH

- OpenSSH 10.0 and later supports ML-KEM
- ML-KEM support merged upstream in libssh
- Standardization ongoing, signatures later

cllang@redhat.com

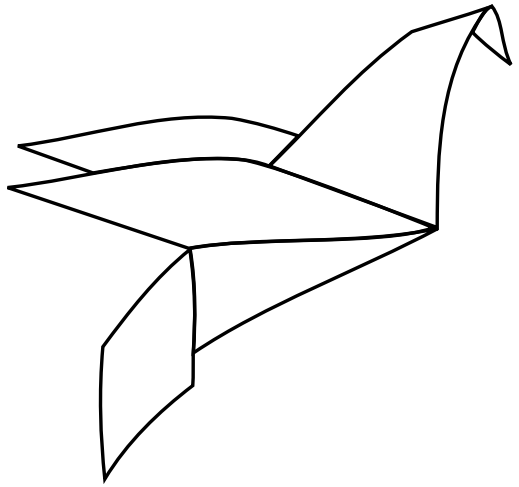
TLS

```
$> openssl s_client \
   -CAfile CA.crt \
   -connect test.openquantumsafe.org:6195 \
   </dev/null \
      |& grep -A1 'Peer signature type:'
Peer signature type: mldsa65
Negotiated TLS1.3 group: X25519MLKEM768
```

cllang@redhat.com

OpenPGP and RPM Signatures

- OpenPGP PQC draft in RFC editor queue
- ML-KEM for encryption against HN;DL
- Remember: “Quantum-safe software and firmware upgrades are enabled by default”
  - LibrePGP/GnuPG have no PQC signatures
  - Sequoia has a pre-release, with ML-DSA, SLH-DSA and PKCS#11 support
  - RPMv6 supports multiple OpenPGP sigs



Sequoia-PGP

clang@redhat.com

Demo

https://github.com/neverpanic/fosdem-rpm-pqc-signing-demo/

Demo Wrap-Up

So RPM signatures are done? – Well…

- Signing Tooling Support
- Hardware Security Module
- Key Generation & Distribution
- Bootstrapping on older releases
- Signatures on other artifacts (containers, flatpaks, ostree images, bootc, …)

- Tools that use GnuPG to parse public keys
- What about COPR?
- … or EPEL?

Other Protocols

Here be dragons

Kerberos PKINIT	WebAuthn	JWT
IPSec	HW security tokens	WiFi/Bluetooth
DNSSEC	OpenVPN	Samba
Kernel Module Signatures	Clevis/Tang	SNMP
IMA/EVM	DKIM	Matrix
S/MIME	Keylime	XML Signatures
TPM	OAuth	PDF Signatures

cllang@redhat.com

Fedora is on track, but there's
a lot of work still ahead of us.

Questions?

Clemens Lang
Product Owner RHEL Crypto Team

@neverpanic@chaos.social
cllang@redhat.com
neverpanic