

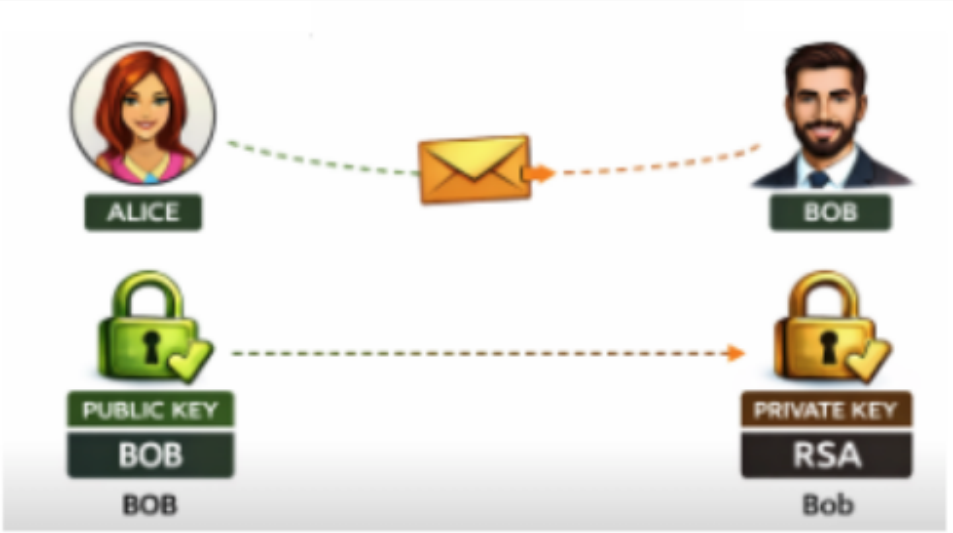
afnic
Internet
made in France

PQC Webinar - 26/02/2026

PQC Implications for the DNS Ecosystem : *An Introduction*

– Sandoche BALAKRICHENAN

Impact on Classical Asymmetric Cryptography



How Quantum Computers break RSA - Simple overview

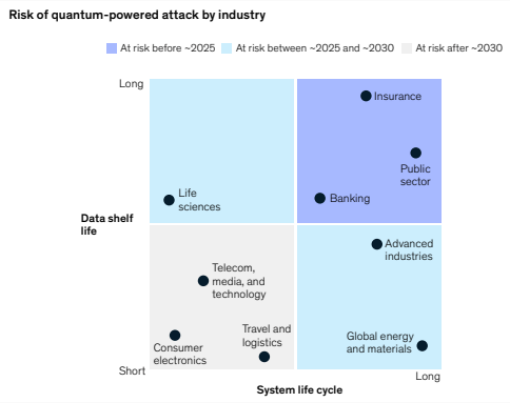
- RSA's security relies on the difficulty of prime factorization.
  - If n ='21' => Prime factors are 'p'(3) * 'q'(7)
  - Once n = p*q is factored -> attacker reconstructs the private key (d).

- Classical computers cannot factor 2048 bit numbers in reasonable time.
  - n = '32452843... (617 digits long)'
  - $\approx 10^{615}$ possible primes to test n

- Quantum Computers running Shor's algorithm could factor 'n' in hours to days .

Preparing for the Quantum threat

- Post Quantum Cryptography (PQC) - Migrate to new algorithms that are resistant to Quantum attacks.



Source: McKinsey Digital

PQC Impact on DNSSEC

- PQC signatures (Falcon, Mayo, SPHINCS etc.) are **much larger**:
  - Bigger DNSKEY and RRSIG records.
- Operational impacts:
  - Higher validation overhead on resolvers.
  - Key rollovers become more complex.
  - HSMs and signing software must support PQC.



Broader PQC Impacts on the DNS Ecosystem

- Zone Transfers (AXFR/IXFR)
  - XFR-over-TLS inherits PQC impacts of TLS.
- Transport Security
  - DoT, DoH, and DoQ rely on **TLS 1.3**, which will adopt PQC.
- Registrar–Registry Protocols (EPP, RDAP)
  - PQC certificates and TLS handshakes required for secure channels.
- DANE / TLSA Records
  - TLSA may contain PQC keys → larger DNS records.

PQC work at the IETF

TLS

- ML-KEM for TLS 1.3
  `draft-ietf-tls-mlkem-05`
- ML-DSA in TLS 1.3
  `draft-ietf-tls-mldsa-01`

DNSSEC

- PQC Research Agenda for DNSSEC
  `draft-fregly-research-agenda-for-pqc-dnssec-02`
- PQC Strategy for DNSSEC
  `draft-sheth-pqc-dnssec-strategy-00`

Conclusion: Why We Need a PQC Webinar?

- Quantum computers will eventually break RSA and ECC, impacting DNSSEC, TLS, and PKI.
- Attackers can **harvest encrypted data now** and decrypt it later (HNLD threat).
- PQC migration affects the **entire DNS ecosystem**: resolvers, authoritative servers, registries, registrars, and infrastructure tools.
- Preparing early reduces operational risk
- The webinar helps stakeholders understand impacts, standards, and the path to a safe transition.

Thank You

Contact: sandoche.balakrichenan@afnic.fr

Questions?