Post-quantum cryptography for DNSSEC in practice

Joeri de Ruiter (SURF)

Quantum apocalypse

- Quantum computer can break asymmetric cryptography
- Not yet (as far as we know)

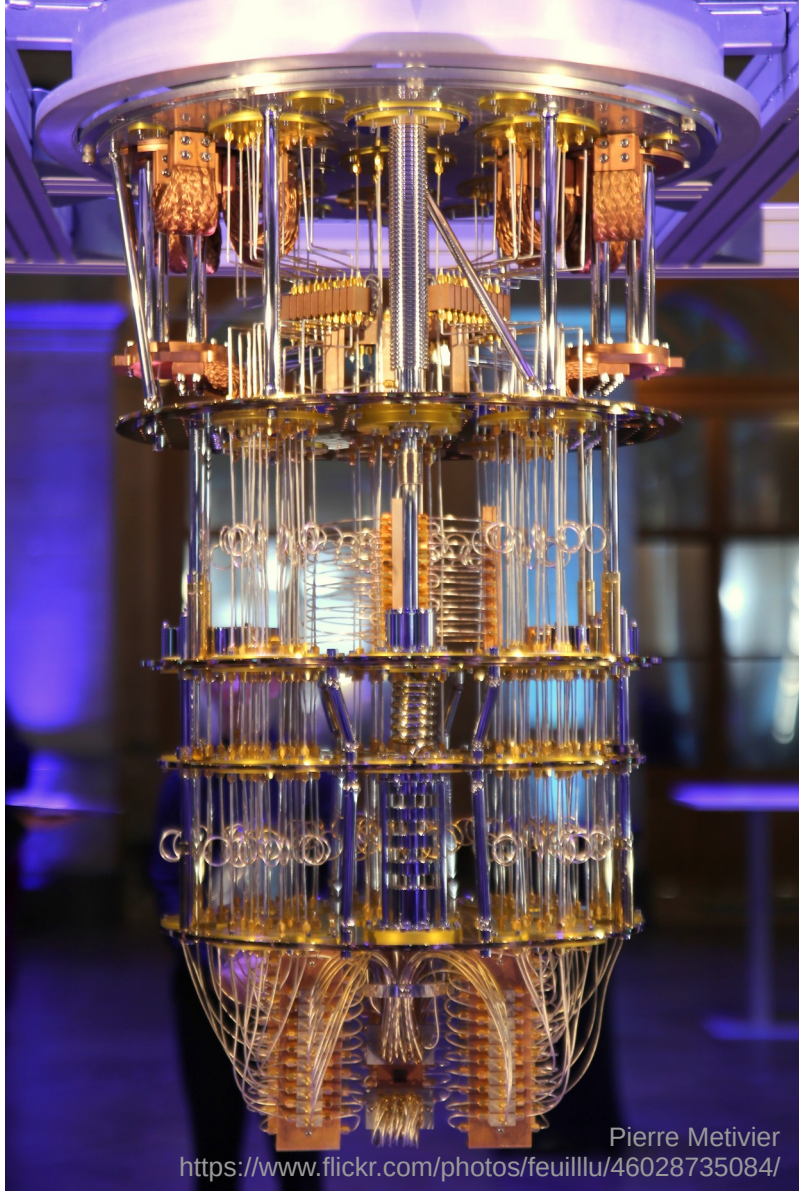


Photo by panumas nikhomkhai
https://www.pexels.com/photo/close-up-photo-of-mining-rig-1148820/

When will this become a problem?

Encryption: “store now, decrypt later”

Integrity: once a powerful quantum computer is available

Post-quantum cryptography

- New cryptographic algorithms needed
  - Different mathematical principles
- A lot happening
  - First algorithms standardised by NIST
  - Guidelines by BSI

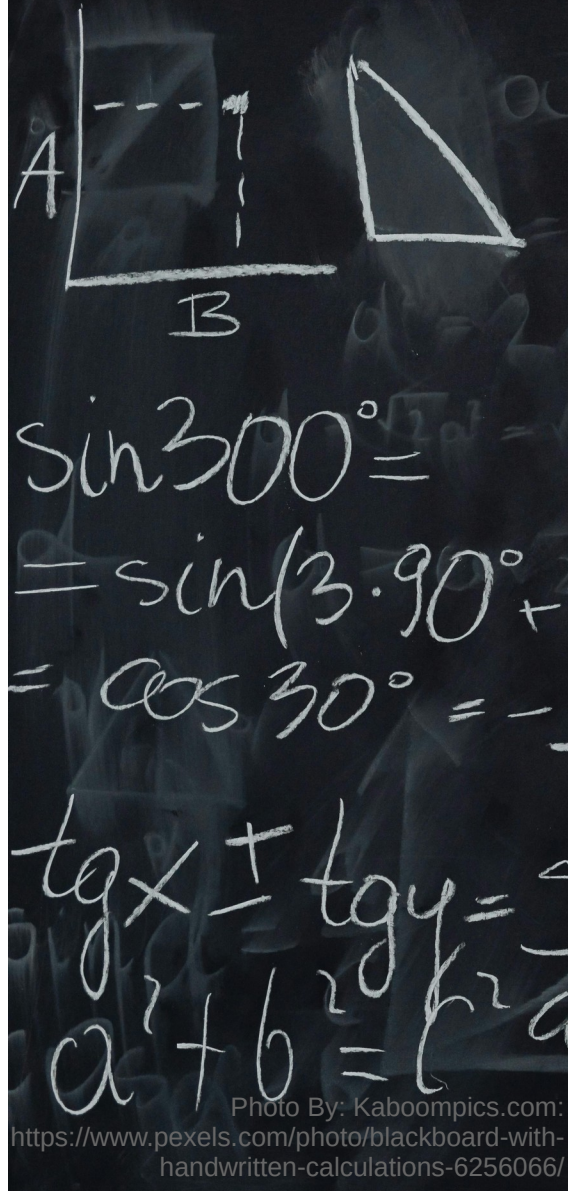


Photo By: Kaboompics.com: https://www.pexels.com/photo/blackboard-with-handwritten-calculations-6256066/

PQC and DNS

- DNS: phonebook of the internet
- Asymetric cryptography is used for DNSSEC-signatures
- No confidentiality offered by DNSSEC
  - Only integrity/authenticity
  - “Store now, decrypt later” not a problem
- Slow adoption rate

Impact on DNS

- Properties of PQC very different
- Bigger keys and signatures → bigger packets
  - Fallback from UDP to TCP
- Computations can take longer
  - Signing of zones on authoritative nameservers
  - Validation on resolvers

Query www.sidnlabs.nl

ECC

167 bytes

Query www.sidnlabs.nl

ECC

167 bytes

Falcon-512

760 bytes

Query DNSKEY

ECC

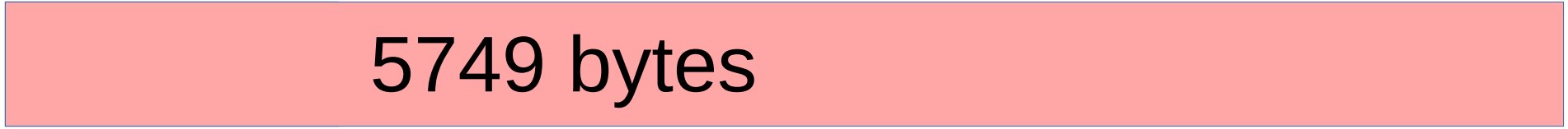
289 bytes

Query DNSKEY

ECC

289 bytes

MAYO-2



Joint research

- Impact of PQC on DNSSEC in real-life scenarios
- Input based on our respective roles
  - SIDN as TLD-registry
  - SURF as provider of resolvers and authoritative nameservers

UNIVERSITY OF TWENTE.

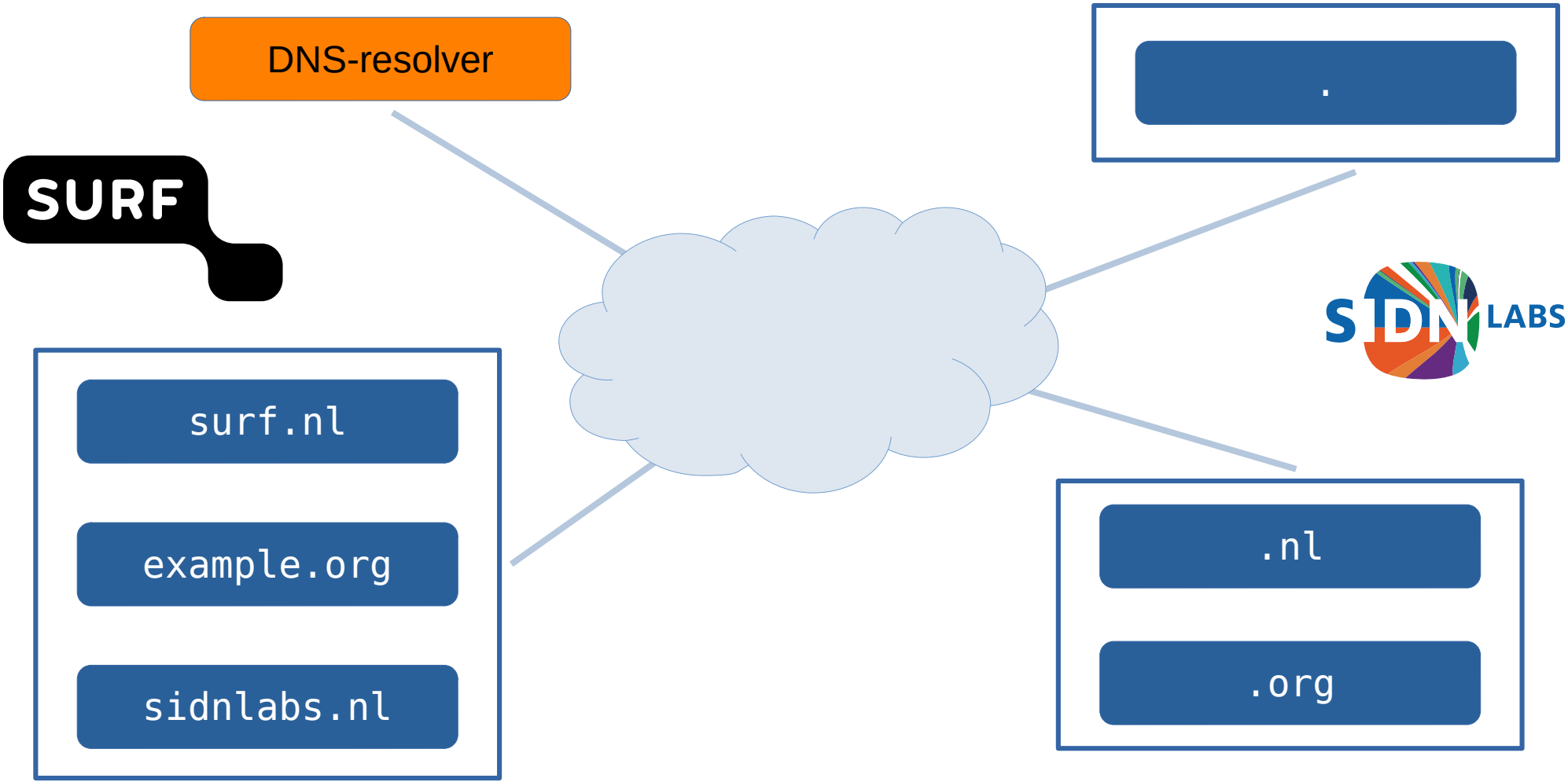
SIDN LABS

SURF

Photo by Jean-Paul Wettstein: https://www.pexels.com/photo/miniature-train-set-with-swiss-locomotive-29004797/

Testbed

- “Replication of the world”
  - Root (.)
  - Top-level domains (e.g. .nl)
  - Regular DNS-zones (e.g. surf.nl)
- PQC-support
  - DNSSEC-signers
  - Resolvers
- Data from production resolvers
  - Anonymised
  - Zones reconstructed


DNS-resolver
SURF
.
SIDN LABS
surf.nl
example.org
sidnlabs.nl
.nl
.org

Measurements

- Different scenarios/algorithms
- Impact on resolver
  - CPU
  - Memory
  - TCP fallbacks
  - Network traffic
- Should we add a bit of extra resources?
- Should we double capacity?
- Should we build new datacenters?

Photo by Alexander Gluschenko
https://www.pexels.com/photo/vintage-control-panel-in-armenian-facility-32654818/

First results

- ECC (ECDSA P-256) vs PQC (MAYO2)
- 13 million queries
  - Roughly 30 minutes of production traffic
- Replay of all queries

ECDSA P-256	17178 q/s
MAYO2	6741 q/s

Next steps

- More algorithms
- Measure realistic scenarios

Joeri de Ruiter (joeri.deruiter@surf.nl)