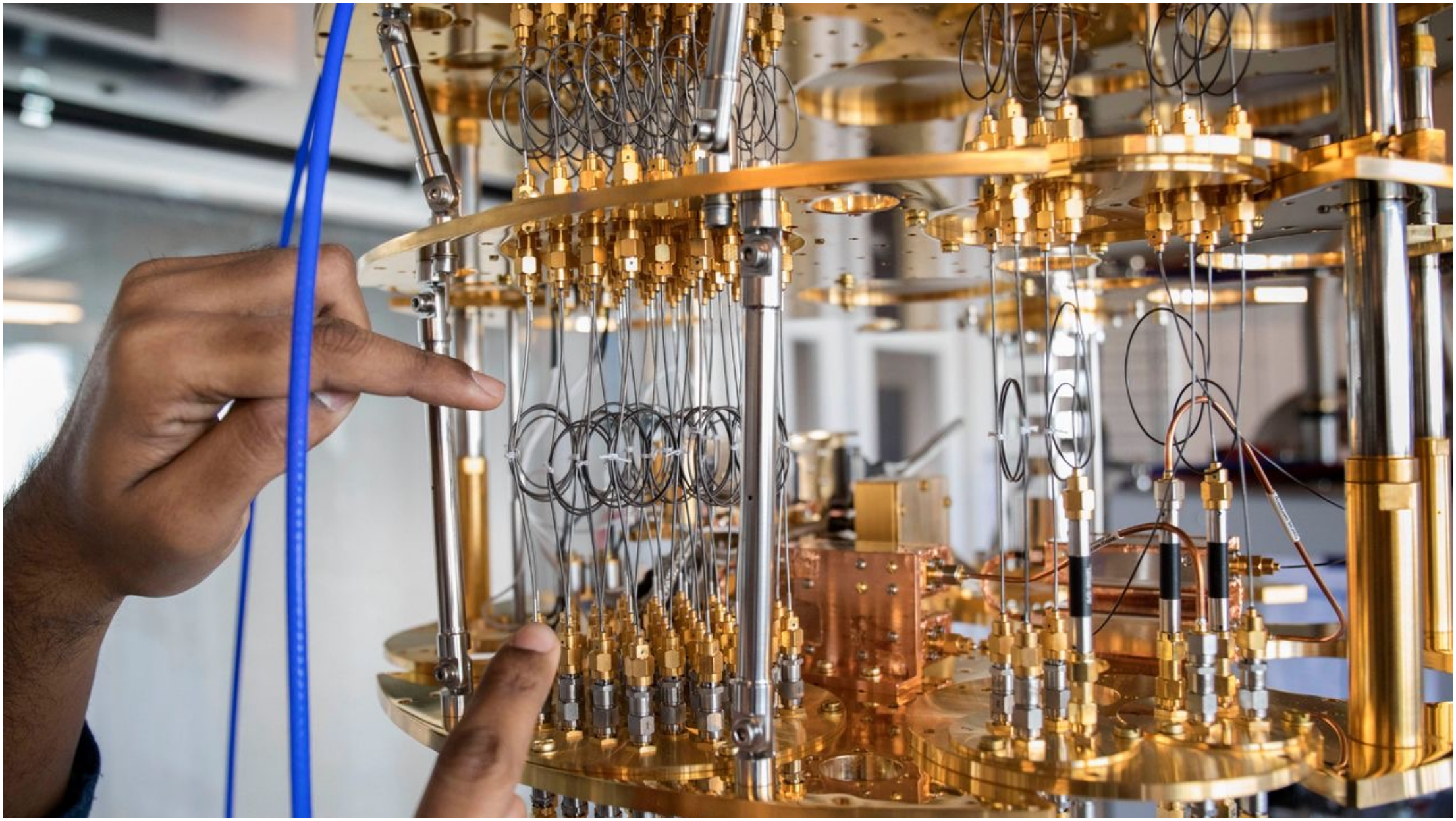
PATAD: an open-source testbed for evaluating post-quantum cryptography for DNSSEC

Elmer Lastdrager, Caspar Schutijser, Ralph Koning, Cristian Hesselman

ICANN 81 Tech Day, Istanbul, Turkey

Mon Nov 13, 2024

SIDN LABS



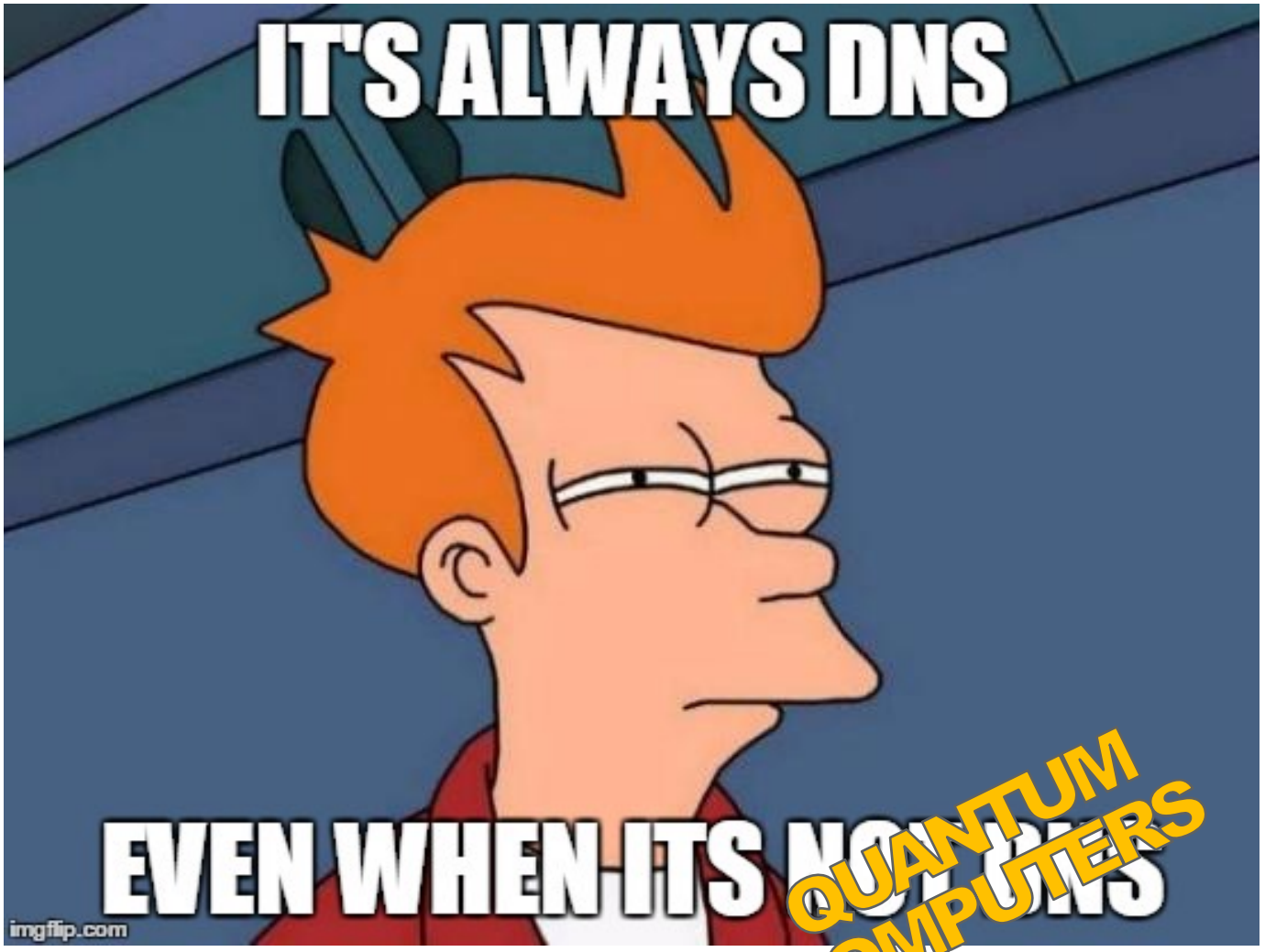
What are the expectations?

- Applications such as accelerated drug discovery, improved machine learning, development of revolutionary materials

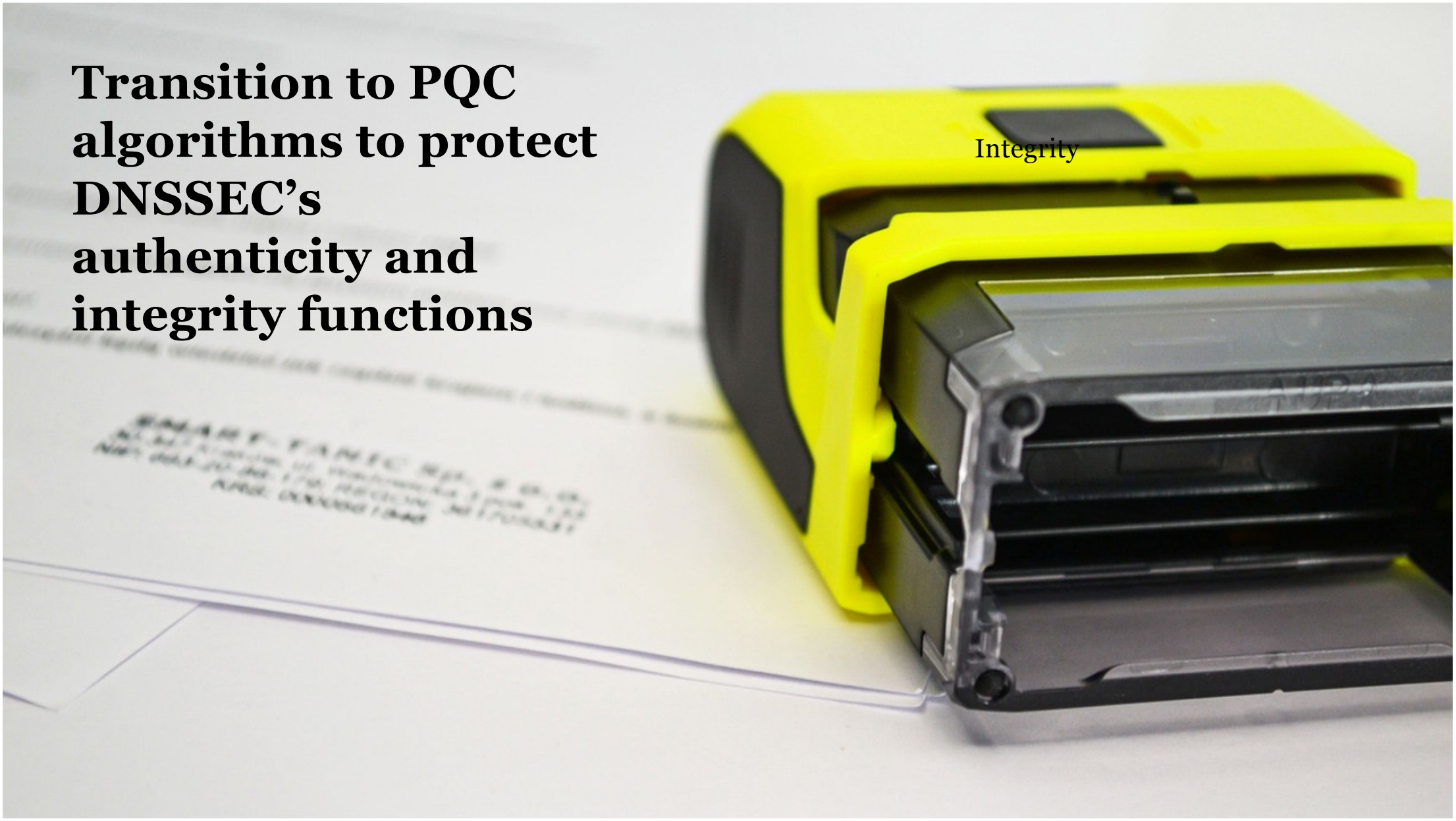
- Dooms day application: breaking state-of-the-art cryptography
  - Requires 20 million qubits to do that in 8 hours
  - Largest quantum computer has 443 qubits (May 2023)
  - Capabilities that only large companies and “state actors” might have

- Experts think this won’t happen for another 10-15 years

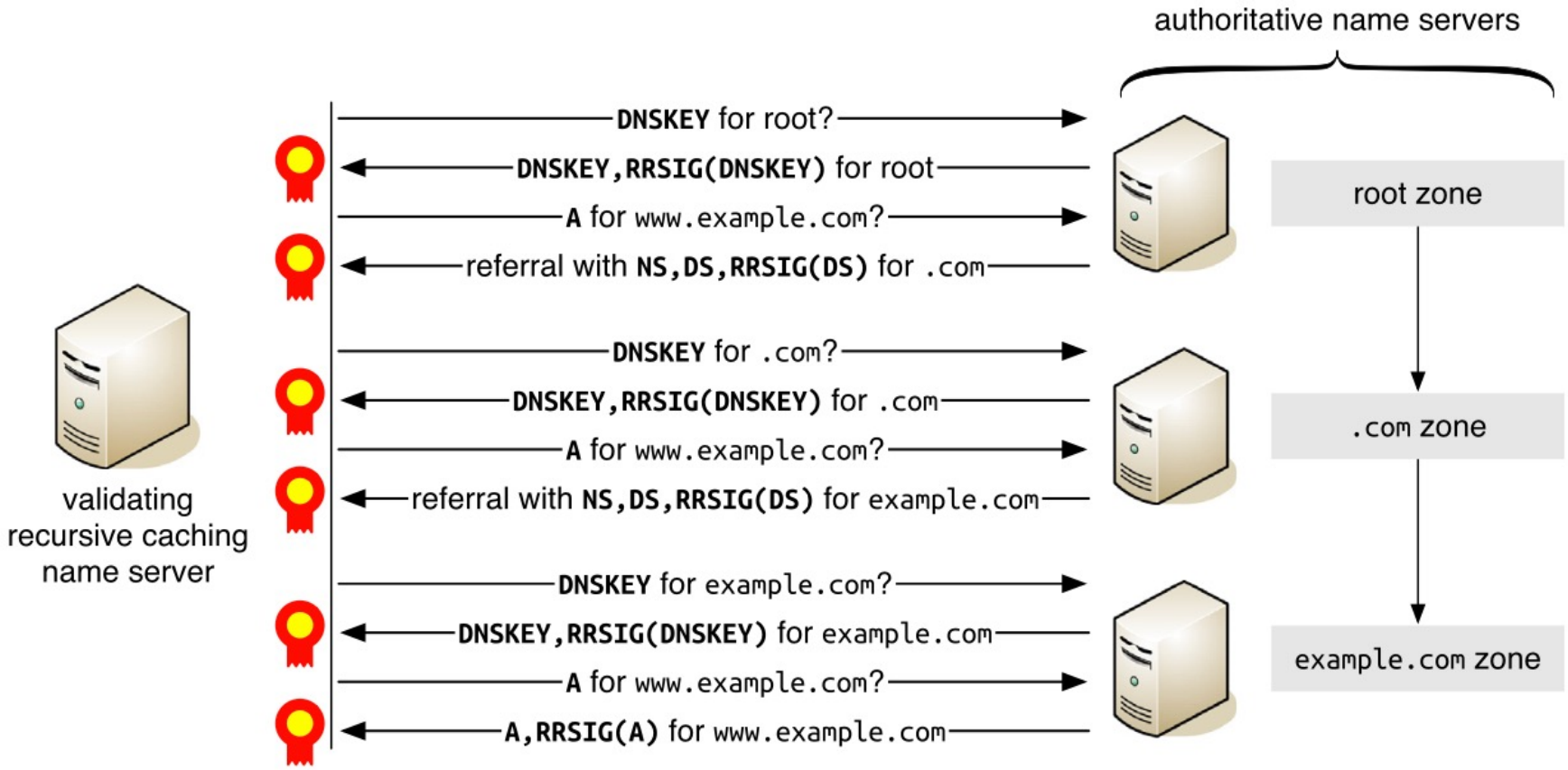
“The race to find the quantum hotspot”, Nature, May 2023
R. de Wolf, “The potential impact of quantum computers on society”, Ethics and Information Technology, 2017


IT'S ALWAYS DNS
EVEN WHEN ITS NOT DNS
imgflip.com
QUANTUM
COMPUTERS

Transition to PQC algorithms to protect DNSSEC's authenticity and integrity functions

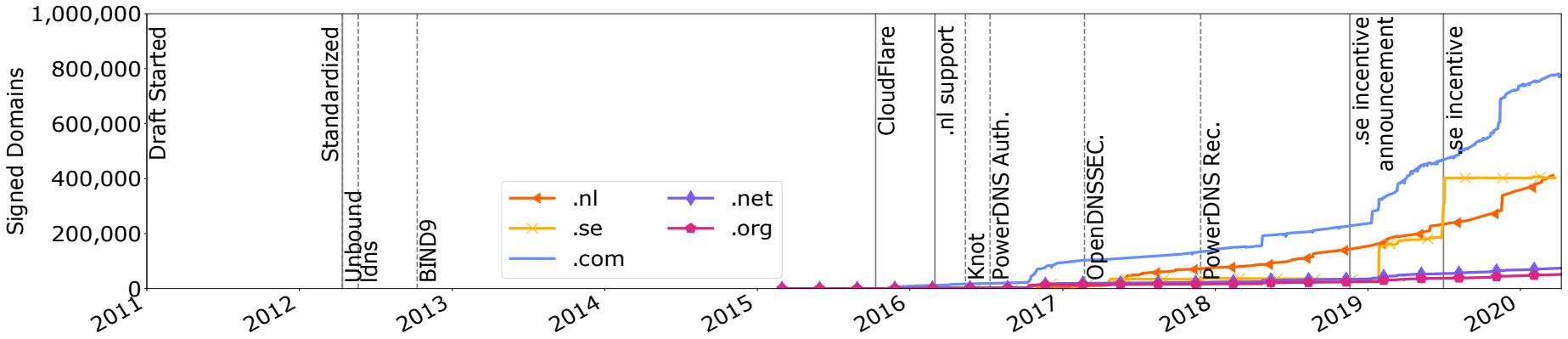


DNSSEC: key and signature interactions



O. van der Toorn, M. Müller, S. Dickinson, C. Hesselman, A. Sperotto & R. van Rijswijk-Deij, "Addressing the challenges of modern DNS: a comprehensive tutorial", Computer Science Review, June 2022

Why work on PQC in DNSSEC now?



Domains signed with ECDSA256 and resolvers able validating this algorithm

M. Müller, "Making DNSSEC Future Proof", Ph.D. thesis, University of Twente, Sep 2021

Requirements for quantum-safe algoritms

Prio	Requirement	Good	Accepted Conditionally
#1	Signature Size	≤ 1,232 bytes	—
#2	Validation Speed	≥ 1,000 sig/s	—
#3	Key Size	≤ 64 kilobytes	> 64 kilobytes
#4	Signing Speed	≥ 100 sig/s	—

M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

SIDN LABS

Theory: packet size

Scheme	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig
EdDSA 🧨	Ed25519	Pre-Q	32	64	96
🙂 MAYO	two	1	5,488	180	5,668
RSA 🧨	2048	Pre-Q	272	256	528
SNOVA	(24, 5, 16, 4)	1	1,016	248	1,264
SNOVA	(25, 8, 16, 3)	1	2,320	165	2,485
SNOVA	(28, 17, 16, 2)	1	9,842	106	9,948
🙂 SQIsign	I	1	64	177	241
VOX	128	1	9,104	102	9,206

Post-quantum signatures zoo: https://pqshield.github.io/nist-sigs-zoo

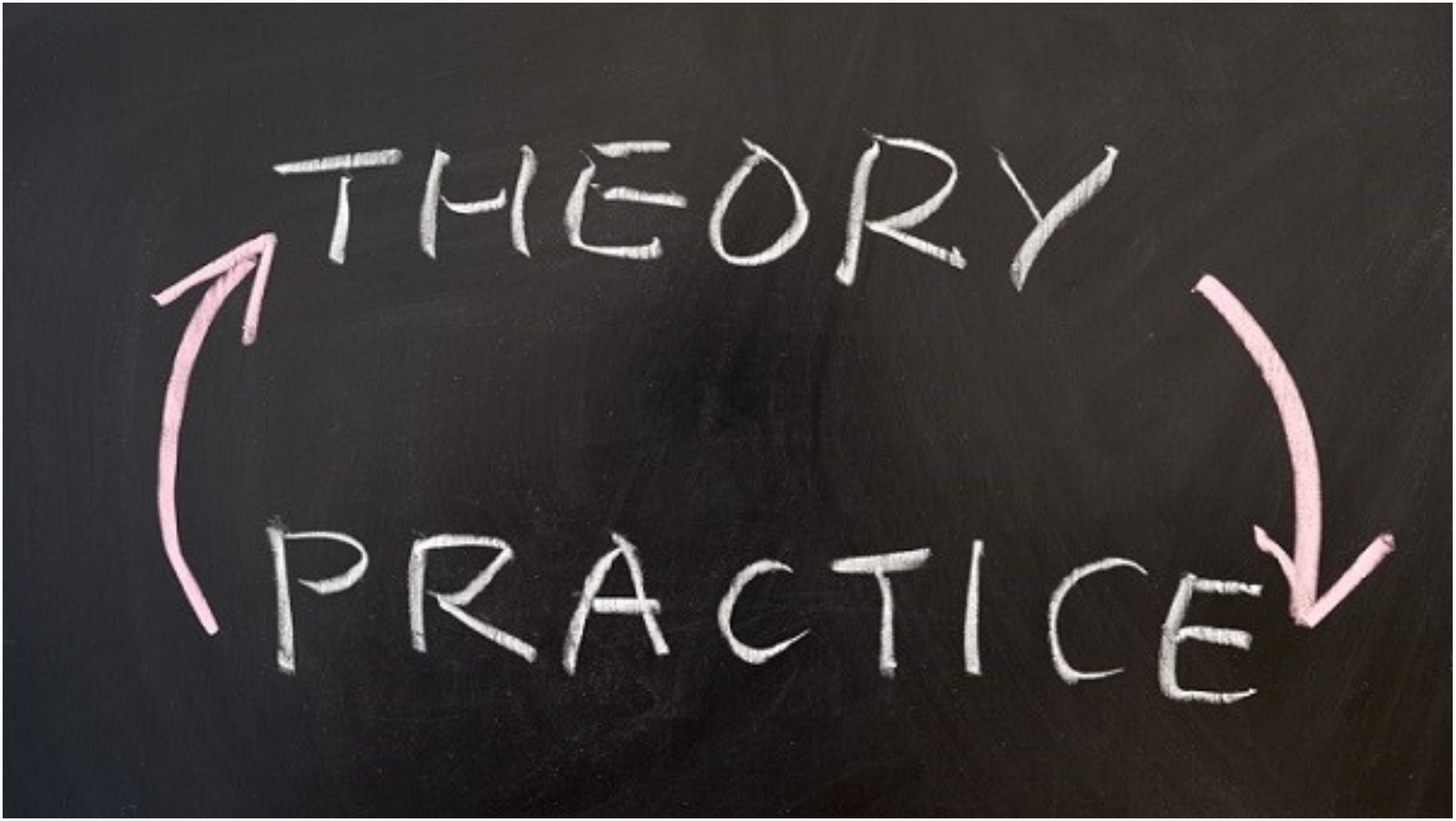
Theory: signing and verification speed

Scheme	Parameterset	NIST level	Sign (cycles)	Verify (cycles)
EdDSA ⚠️	Ed25519	Pre-Q	42,000	130,000
🙂 MAYO	two	1	563,900	91,512
RSA ⚠️	2048	Pre-Q	27,000,000	45,000
SNOVA	(24, 5, 16, 4)	1	19,681,409	8,086,815
SNOVA	(25, 8, 16, 3)	1	12,408,096	3,959,869
SNOVA	(28, 17, 16, 2)	1	10,964,945	3,161,199
☹️ SQIsign	I	1	5,669,000,000	108,000,000
VOX	128	1	664,265	168,567

Post-quantum signatures zoo: https://pqshield.github.io/nist-sigs-zoo

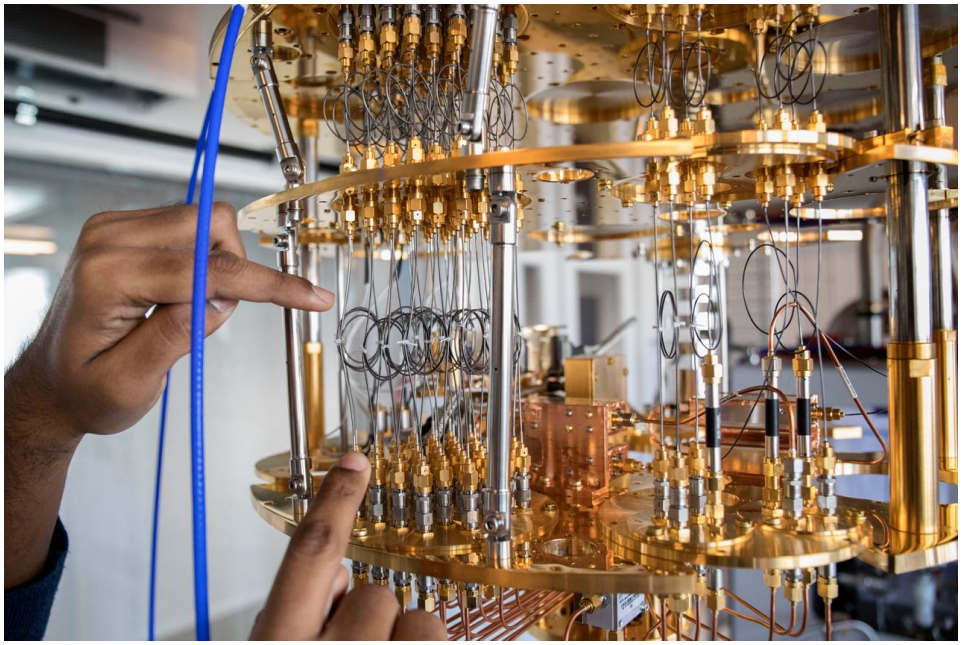
Expected operational risks

- Truncated responses not coming through
- More state on authoritative name servers because of TCP fallback
- Increased signature validation times and slower response times for users
- Increased signing times that do not align with zone file publication windows
- Larger responses during keyrolls


THEORY
PRACTICE

Research question: to what extent can proposed NIST PQC algorithms be used for DNSSEC?

Post-quantum Algorithm Testing and Analysis for the DNS

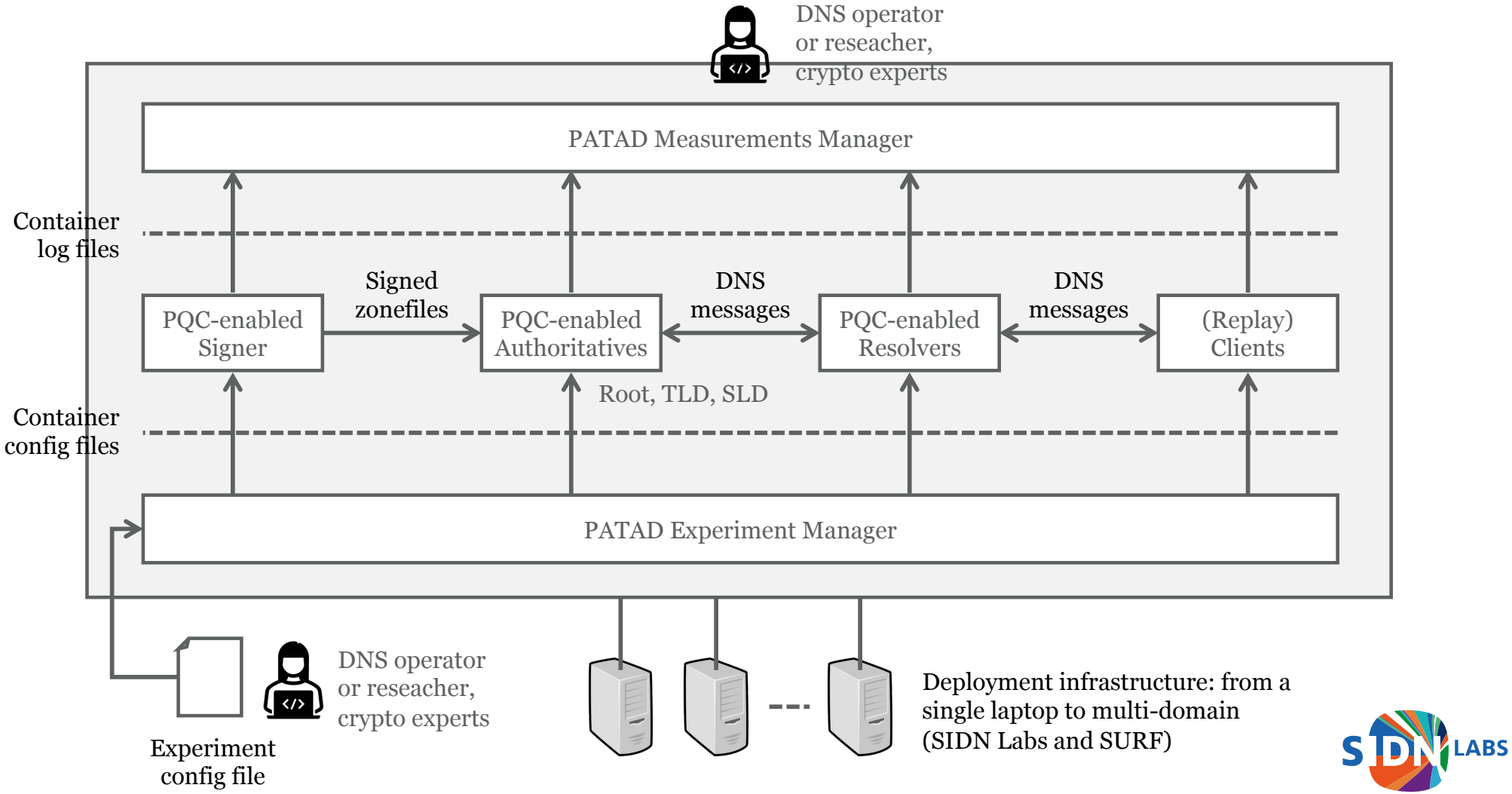


SURF

UNIVERSITY OF TWENTE.

SIDN LABS

PATAD testbed overview



Example experiment configuration file

pqc-testbed / example / docker-compose.yml ↑ Top

Code Blame 106 lines (104 loc) · 4.42 KB Raw

```
# CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
# OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
# OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

version: "3.8"
services:
  exp1-root:
    image: ghcr.io/sidn/pqc-auth-powerdns:latest
    ports:
    - "5302:53/udp"
    - "5302:53/tcp"
    networks:
      examplenet:
        ipv4_address: 10.0.1.2
        ipv6_address: fc01::2
    volumes:
    - ./pdns.conf:/var/lib/powerdns/pdns.conf:ro
    - ./named-root.conf:/var/lib/powerdns/named.conf:ro
    - ./zone-root:/var/lib/powerdns/zones/zone-root-orig:ro
    entrypoint: bash -c 'ln -s /var/lib/powerdns/pdns.conf /usr/local/etc/pdns.conf ; cp /var/lib/powerdns/zones/zone-root-orig /var/
  exp1-nl:
    image: ghcr.io/sidn/pqc-auth-powerdns:latest
    ports:
    - "5303:53/udp"
    - "5303:53/tcp"
    networks:
      examplenet:
        ipv4_address: 10.0.1.3
        ipv6_address: fc01::3
    volumes:
```

SIDN LABS

Current experiments

- Support for Falcon-512, SQISign-1, MAYO-2
- PowerDNS extensions to support PQC algoritms
- Custom signer with measurement extensions
- Using several (large) TLD zones

Future work

- Further improve the testbed, for instance
  - Add NIST algorithms
  - Instrument Auths and Resolvers for real-time measurements
- New experiments, such as replay real-world resolver traffic
- Translate measurements to operational guidelines
- Publications: academic, tech reports, blogs

SIDN LABS

It’s open source!

https://patad.sidnlabs.nl
https://github.com/SIDN/pqc-testbed

Questions and feedback ☺

www.sidnlabs.nl | stats.sidnlabs.nl

PATAD contact person: elmer.lastdrager@sidn.nl

Cristian Hesselman
Director of SIDN Labs
cristian.hesselman@sidn.nl
+31 6 25 07 87 33