Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC

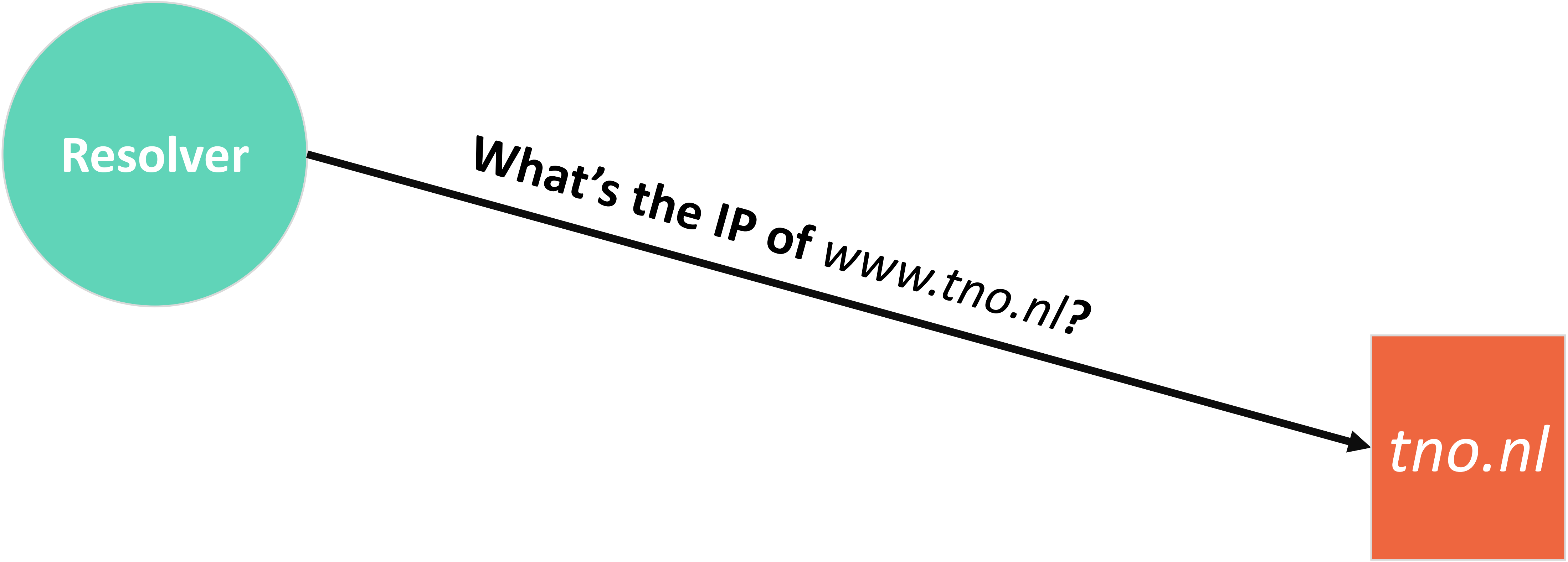
Moritz Müller, Maran van Heesch, Jins de Jong,
Benno Overeinder, Roland van Rijswijk-Deij

National Institute of Standards and Technology
U.S. Department of Commerce

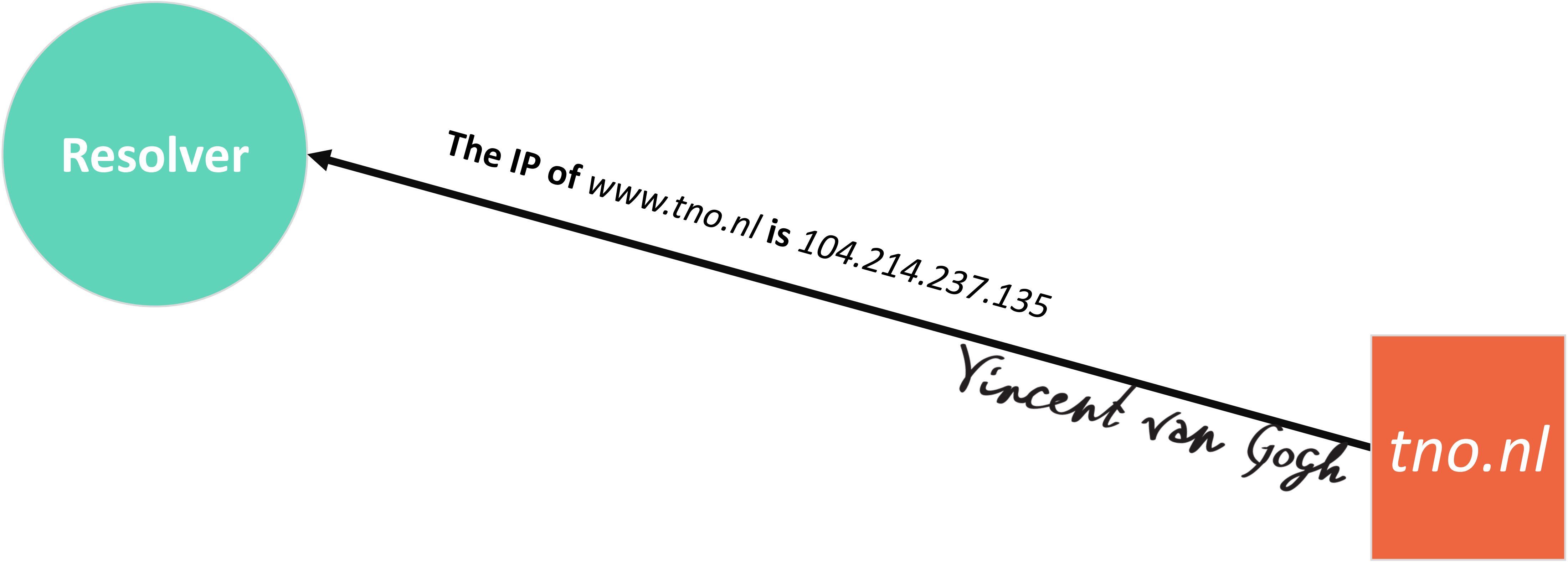
UNIVERSITY OF TWENTE. TNO innovation for life NLNETLABS SIDN LABS

DNSSEC Basics and Challenges

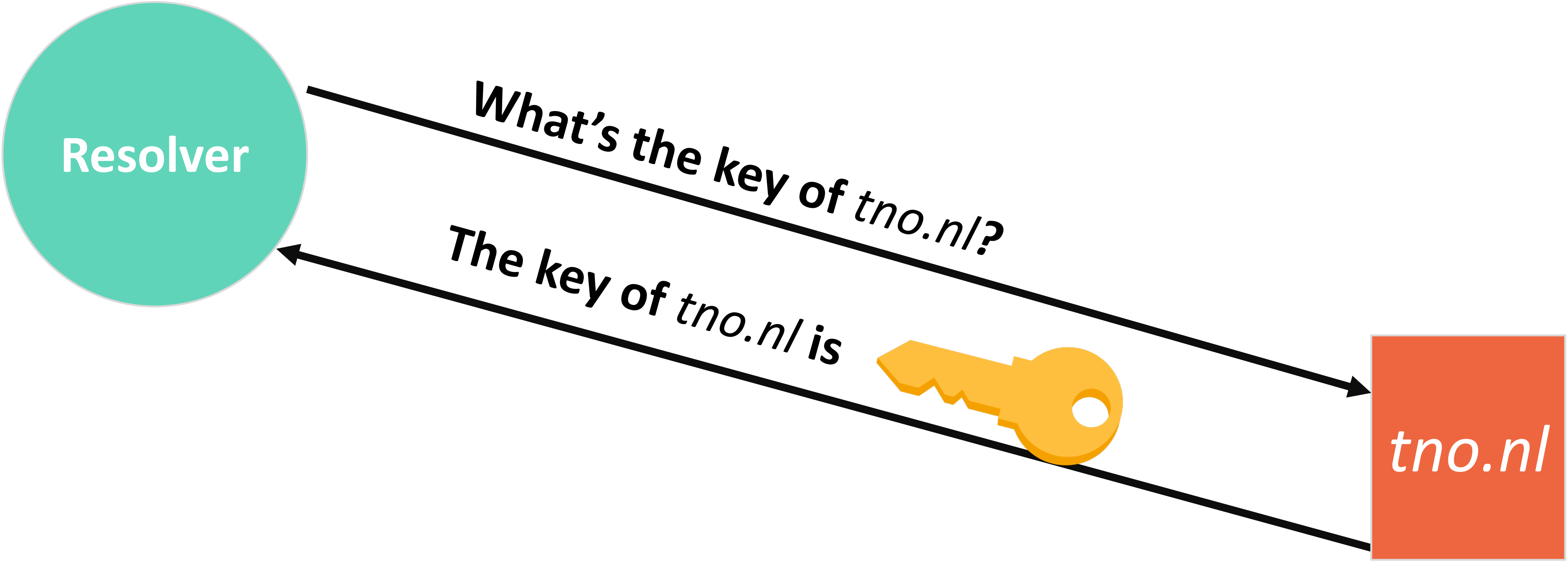
DNSSEC Basics and Challenges



DNSSEC Basics and Challenges



DNSSEC Basics and Challenges



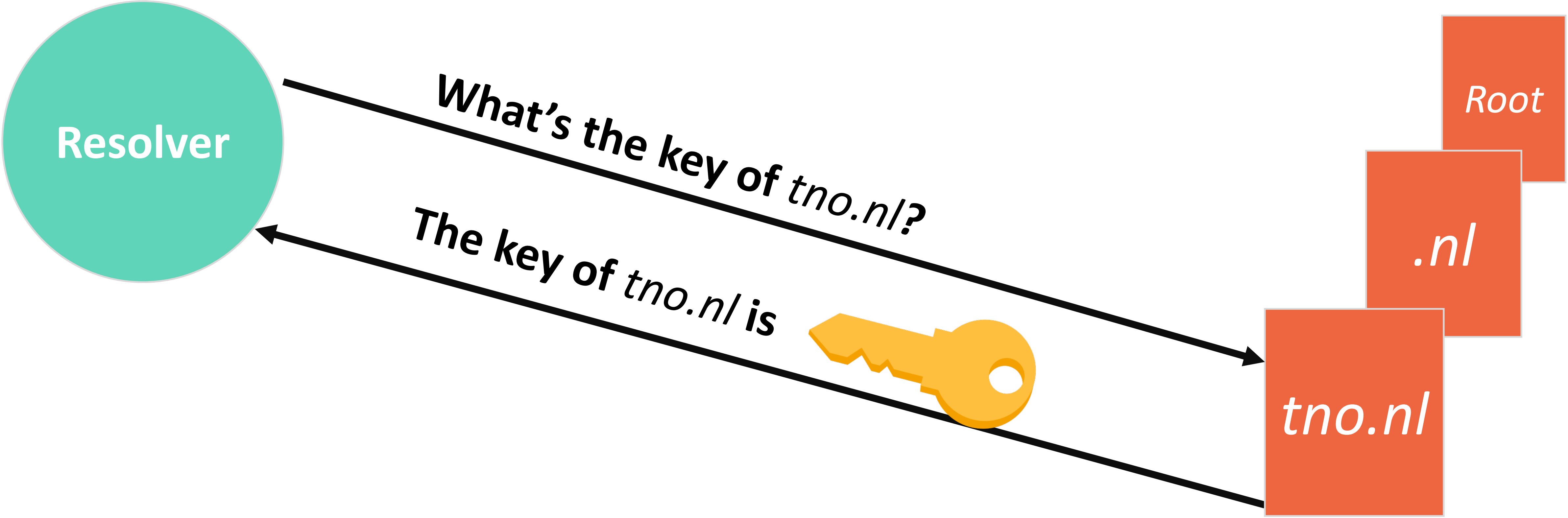
Resolver

What's the key of *tno.nl*?

The key of *tno.nl* is

tno.nl

DNSSEC Basics and Challenges



DNSSEC Basics and Challenges

- Signatures are transmitted with every response
- In some cases multiple keys and signatures in the same response
- Multiple signing algorithms are already supported
- Transport usually is UDP, with TCP fallback

Applying PQC to DNSSEC

Restrictions

- Payload > 1,232 bytes often causes fragmentation
- Resolvers validate thousands of signatures per second
- Signing in some cases on the fly

Requirements for Algorithms

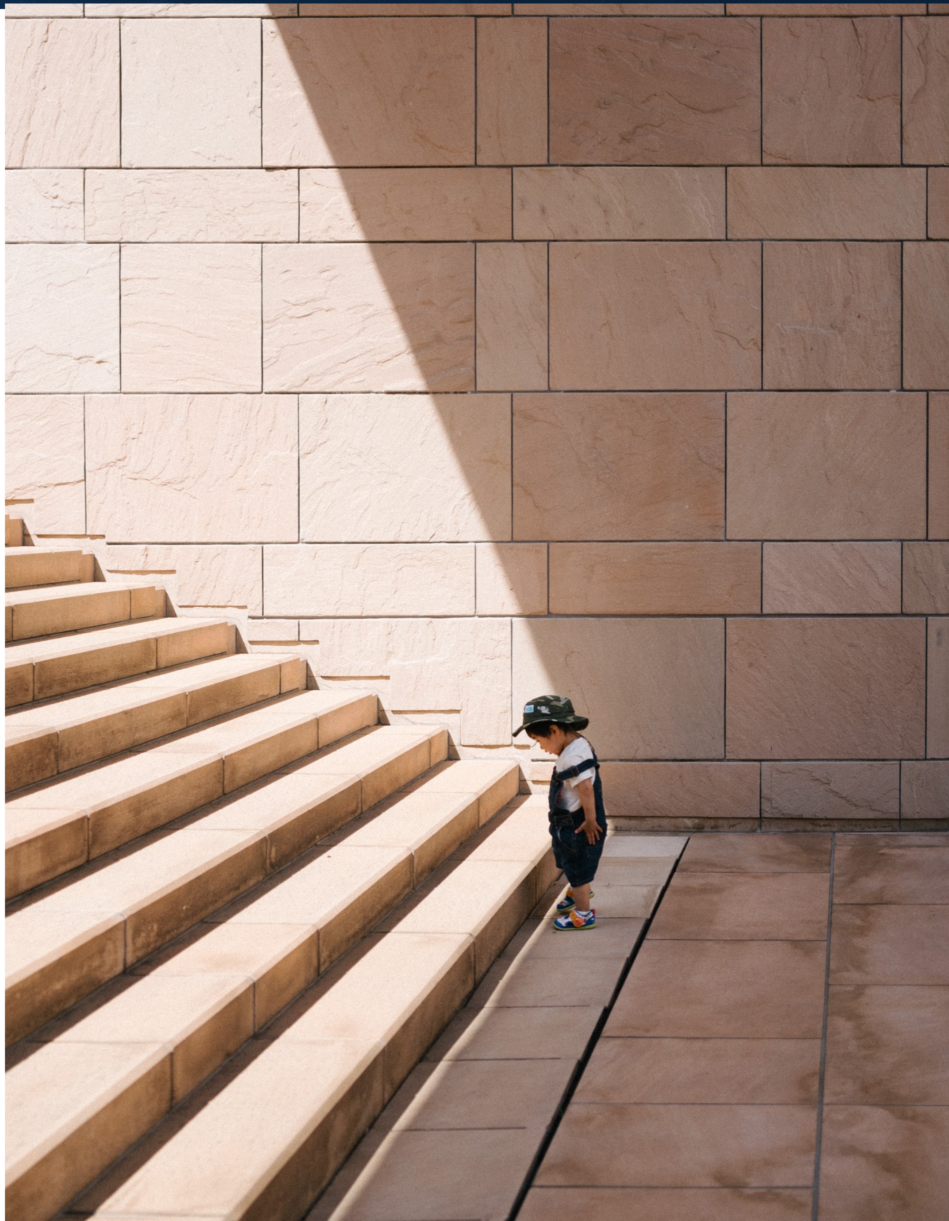
Signature Size:	≤ 1,232 bytes
Validation Performance:	≥ 1000 sig/s
Signing Performance:	≥ 100 sig/s

Finding the Right Algorithm

Algorithm	Public Key	Signature	Sign/s	Verify/s
Falcon-512	0.9kB	0.7kB	~ 3,300	~20,000
Rainbow-Ia	149kB	64B	~ 8,300	~ 11,000
RedGeMSS128	445kB	35B	~ 540	~ 10,000

Preparing DNSSEC for PQC

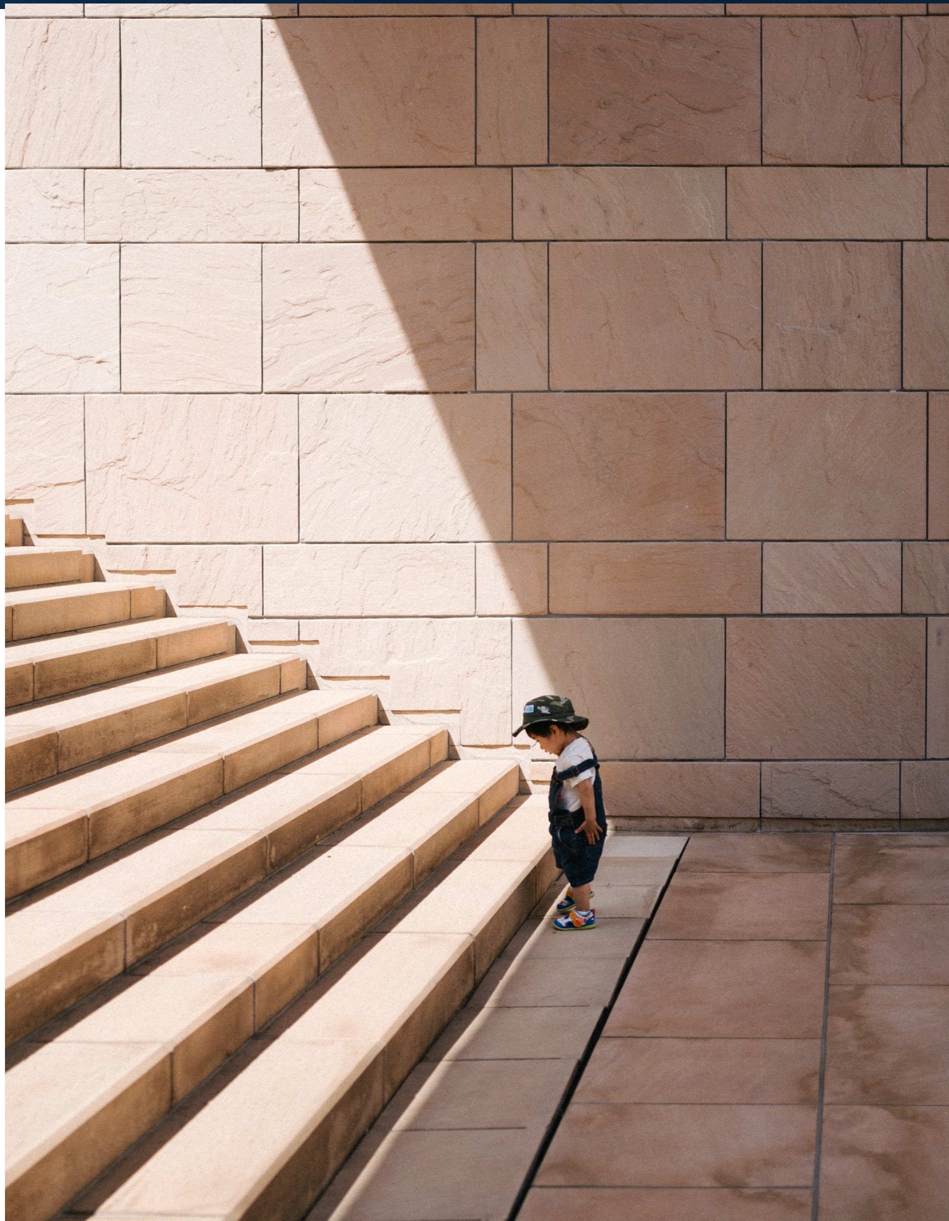
- Out of band key distribution
- Increased TCP support



Preparing DNSSEC for PQC

- Out of band key distribution
- Increased TCP support

- We are currently implementing and testing our proposals



Thank You!

Moritz Müller
SIDN Labs
Email: moritz.muller@sidn.nl
Twitter: @moritzcm_