The Impact of Post-Quantum Cryptography on DNSSEC

SIGCOMM 21

Moritz Müller[1,2], Maran van Heesch[3], Jins de Jong[3], Benno Overeinder[4], Roland van Rijswijk-Deij[2,4]

[1]SIDN Labs, [2]University of Twente, [3]TNO, [4]NLnet Labs

The Problem

- Quantum Computers *could* break current public-key cryptography
- This is a threat to many Internet protocols, *including DNSSEC*
- New *quantum-safe* algorithms are assessed

Main Research Question:

Are these new quantum-safe algorithms suitable for DNSSEC?

Post Quantum Cryptography

Quantum computing

- Shor's algorithm breaks RSA and discrete logarithm cryptography

  → **All current public key cryptography must be replaced by a quantum-safe alternative!**

- DNSSEC's signature schemes must be replaced
- First capable quantum quantum computer *maybe* in the 2030's [1]

[1] Migration to quantum-safe cryptography, TNO, 2020.

DNSSEC and Shor's algorithm

The bad

Replacing an algorithm in DNSSEC takes years [2]

The not so bad

Attack time window relatively small, compared to e.g., TLS

[2] Müller, Moritz, et al. "The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle." *Proceedings of the ACM Internet Measurement Conference*. 2020.

The NIST competition

- 3rd round with 3 finalist and 3 alternate signing algorithms [3]
- 2 Lattice based algorithms
- 2 Multivariate algorithms
- 2 Hash based algorithms

[3] Moody, Dustin. Status Update on the 3rd Round. *"3rd PQC Standardization Conference".* 2021.

Applying PQC to DNSSEC

Restrictions of DNSSEC

- Key and Signature Size
- Validation Performance
- Signing Performance

Restrictions of DNSSEC

- **Key and Signature Size**
- Validation Performance
- Signing Performance

- > 1,232 bytes often cause fragmentation
- Larger records attractive for DDoS attacks

Restrictions of DNSSEC

- Key and Signature Size
- **Validation Performance**
- Signing Performance

- Resolvers can validate thousands of signatures per second

Restrictions of DNSSEC

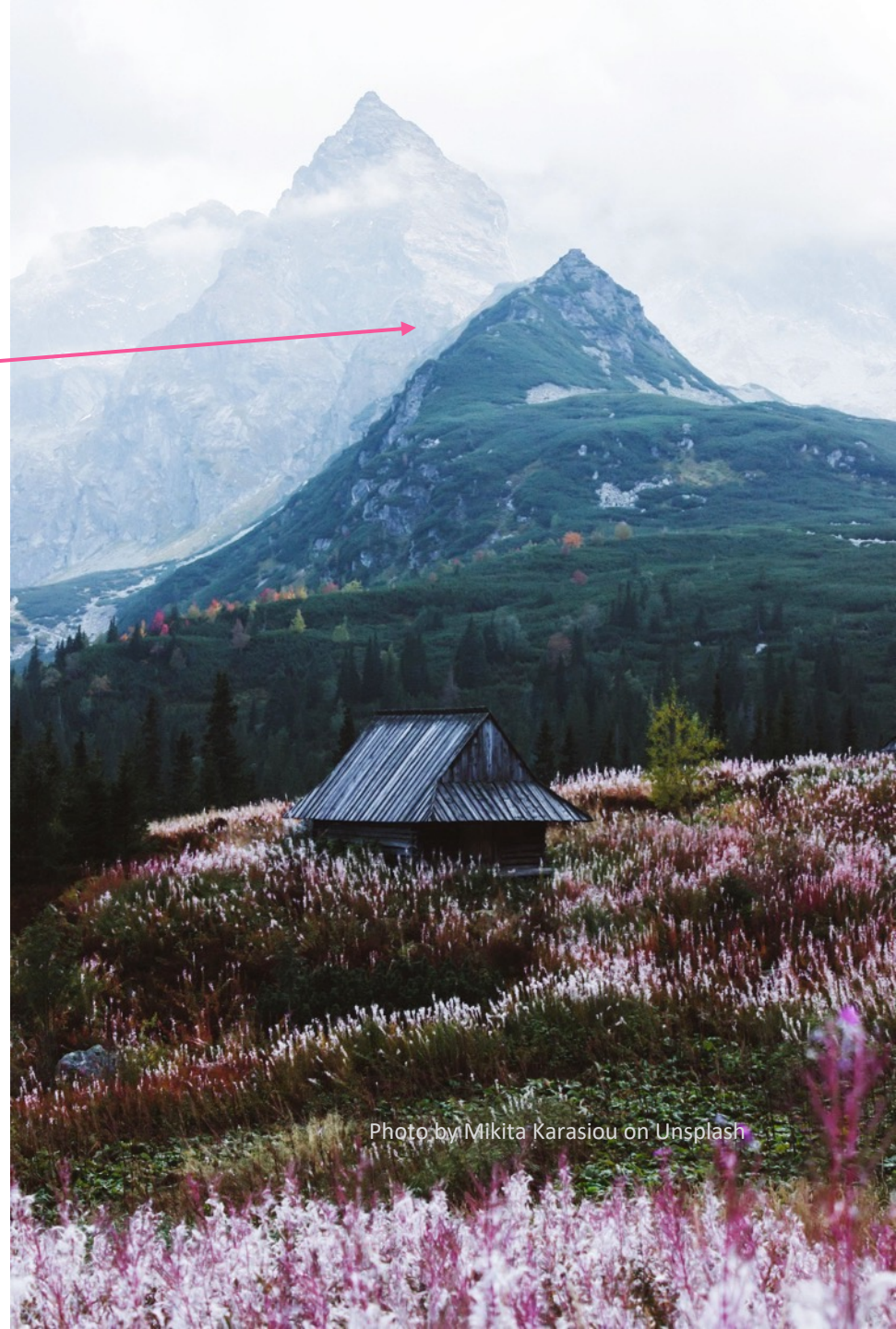
- Key and Signature Size
- Validation Performance
- **Signing Performance**
  - On-the-fly signing most time critical

Main Challenges

- Keys & Signatures > 1.232B
- Keys > 64kB

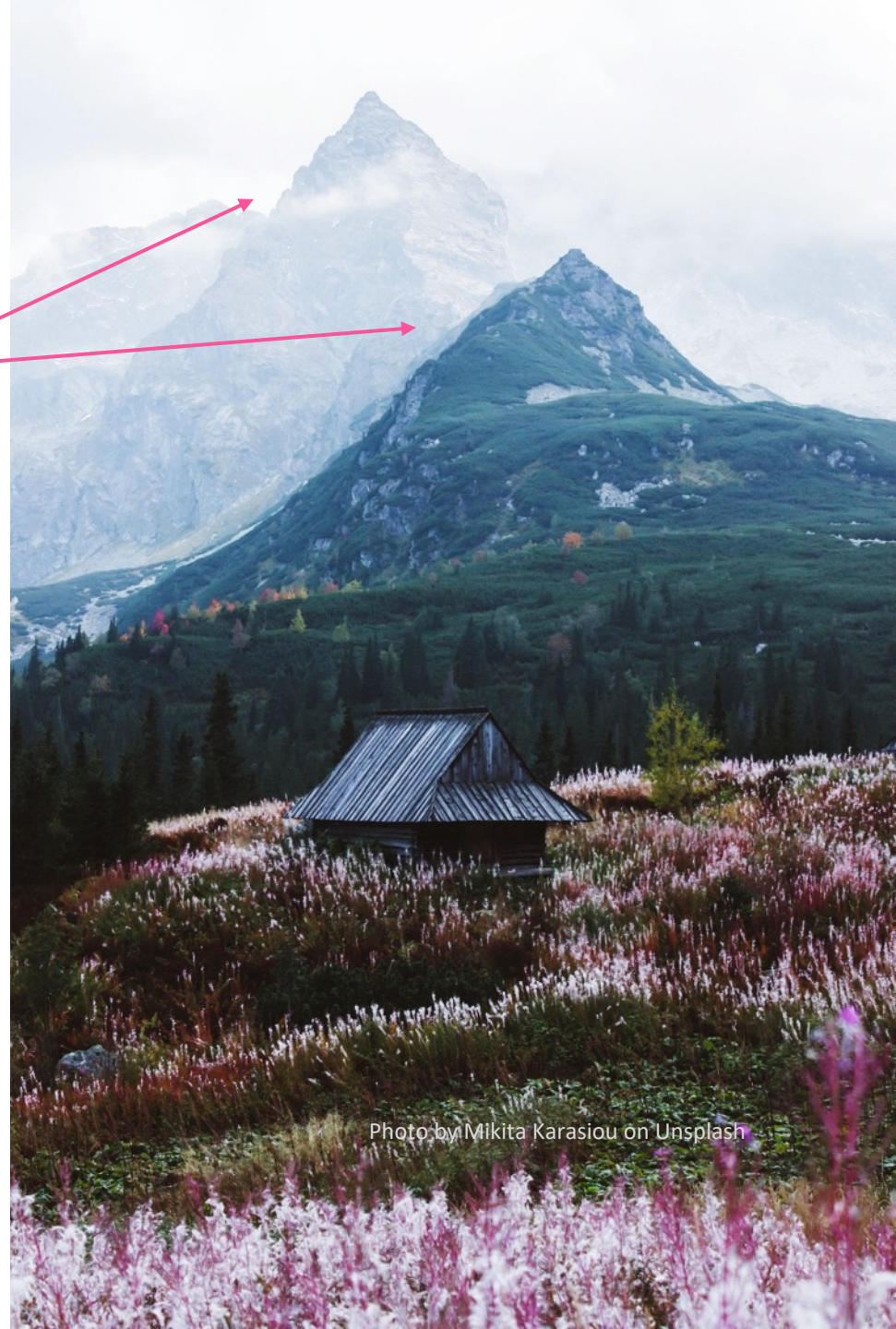
Main Challenges

- Keys & Signatures > 1.232B
- Keys > 64kB



Main Challenges

- Keys & Signatures > 1.232B
- Keys > 64kB



Finding the Right Algorithm

Algorithm	Public Key	Signature	Sign/s	Verify/s
Falcon-512	0.9kB	0.7kB	~ 3,300	~20,000
Rainbow-Ia	158kB	64B	~ 8,300	~ 11,000
RedGeMSS128	375kB	36B	~ 540	~ 10,000
ED25519	32B	64B	~ 26,000	~8,000
RSA-2048	0.3kB	0.3kN	~1,500	~50,000

Possible Solutions

- Keys & Signatures > 1.232B

- TCP fallback

+ regular DNS

- not everywhere supported

- increased server requirements

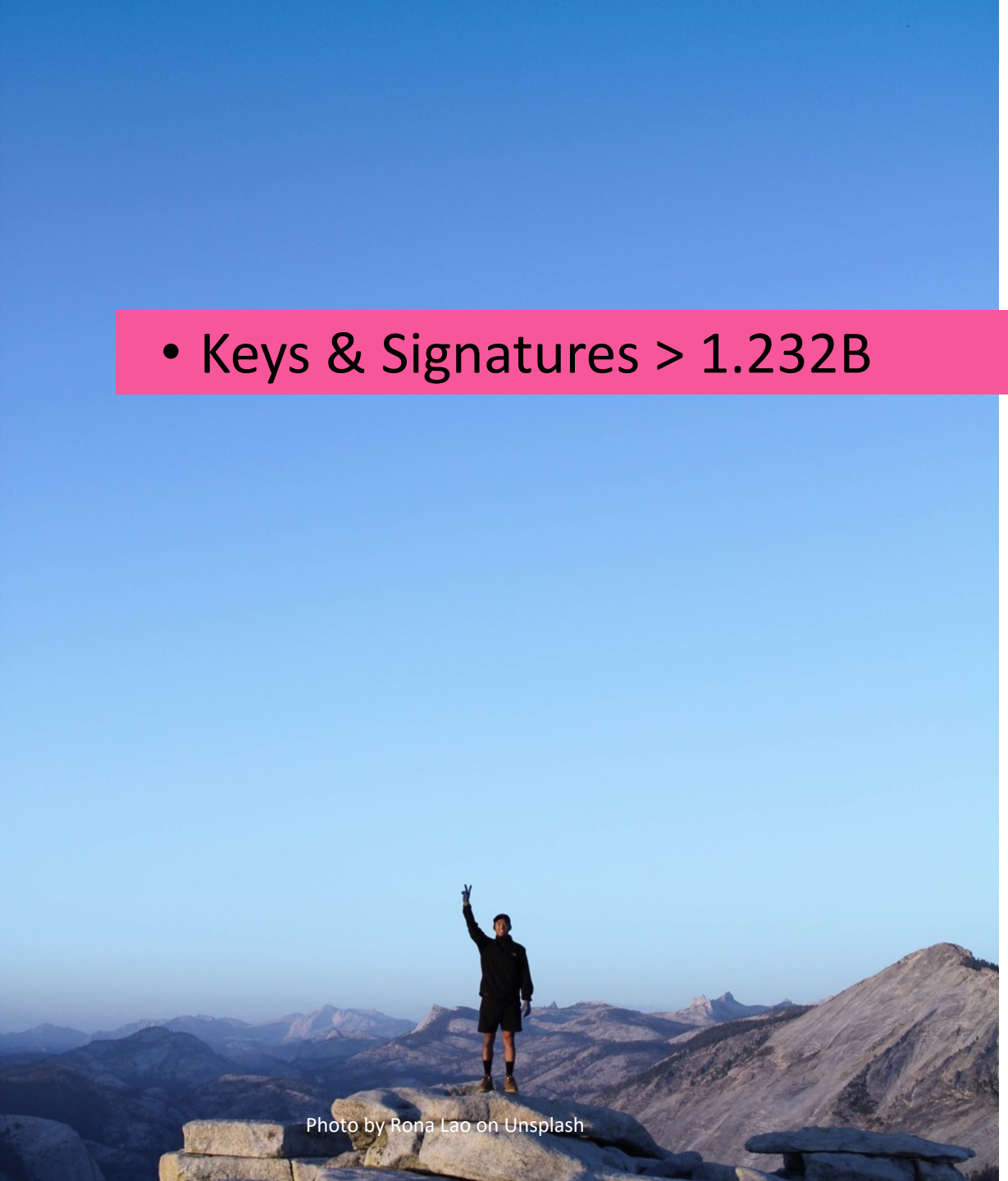


Photo by Rona Lao on Unsplash

Possible Solutions

- Keys & Signatures > 1.232B

- TCP fallback

+ regular DNS

- *? not everywhere supported ? [1]*

- *? increased server requirements ? [2]*

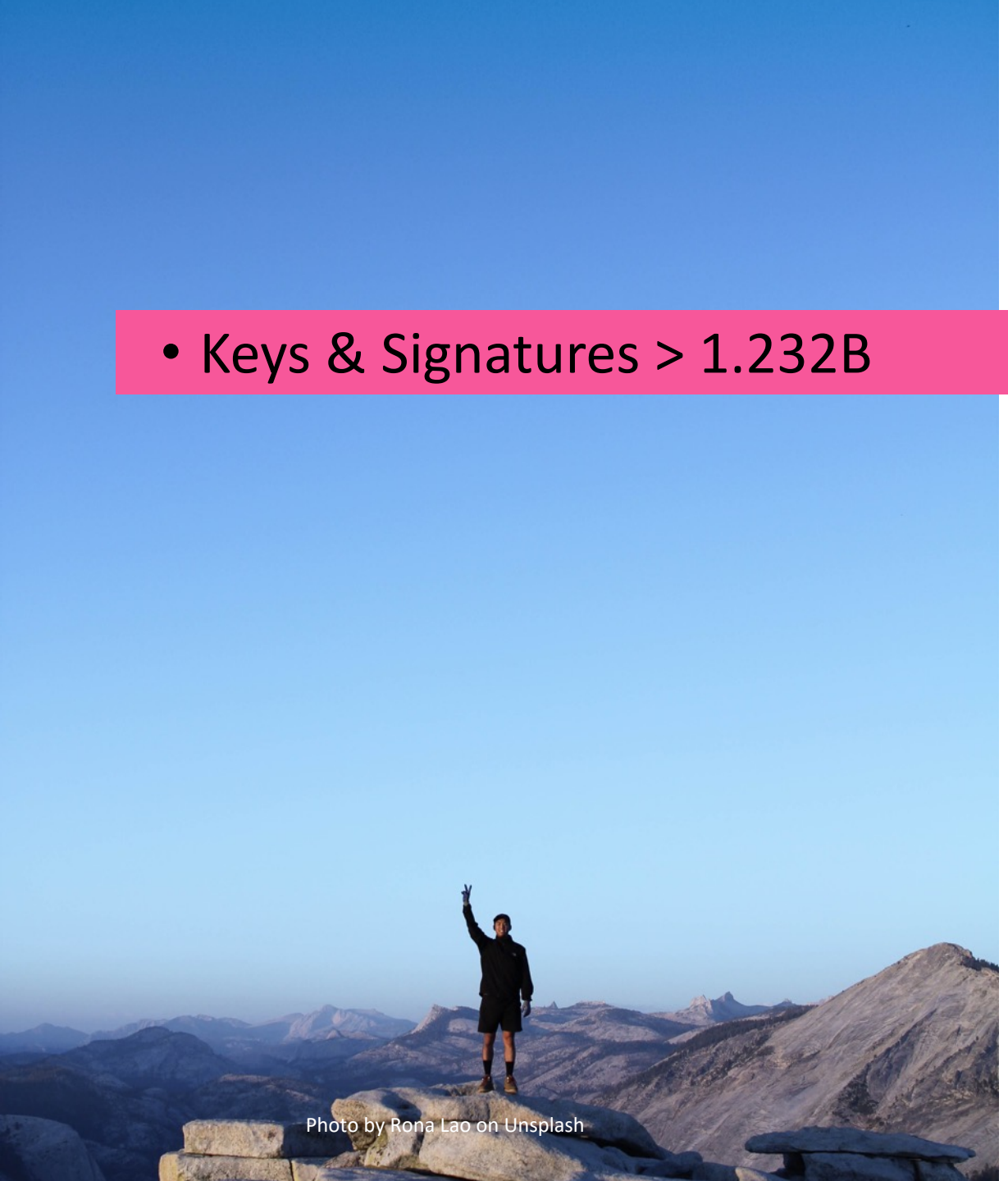


Photo by Rona Lao on Unsplash

[1] https://blog.apnic.net/2020/12/14/measuring-the-impact-of-dns-flag-day-2020/

[2] L. Zhu, Z. Hu, J. Heidemann, D. Wessels, A. Mankin and N. Somaiya, "Connection-Oriented DNS to Improve Privacy and Security," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, USA, 2015, pp. 171-186, doi: 10.1109/SP.2015.18.

Possible Solutions

- Keys > 64kB

- Splitting key in RRs

+ modest DNS extension

- additional round trips

- higher risk of packet loss

Photo by Rona Lao on Unsplash

Possible Solutions

- Keys > 64kB

- Splitting key in RRs

+ modest DNS extension

- additional round trips

- higher risk of packet loss

- Distributing key out of band

+ less prone to packet loss

- requires support of different protocol

Photo by Rona Lao on Unsplash

Possible Solutions

- Keys > 64kB

- Splitting key in RRs
- Distributing key out of band

+ Keys are not exchanged often
- Add to the “DNS Camel”

Next Steps and Conclusions

- Future developments may force us to reconsider our options/preferences
- Keep in mind: *rolling* to a new algorithm *will take time*
- *Paper: https://ccronline.sigcomm.org/2020/ccr-october-2020/retrofitting-post-quantum-cryptography-in-internet-protocols-a-case-study-of-dnssec/*