PQC-Update 2023
Fraunhofer AISEC
28. Februar 2023

Dr. Peter Thomassen
peter.thomassen@securesystems.de

PQ-Kryptographie auf dem Prüfstand

Falcon-512 für DNSSEC

Zur Person

Dr. Peter Thomassen
peter.thomassen@securesystems.de

Senior Solutions Architect bei Secure Systems Engineering

- IT-Sicherheit in verschiedenen Branchen
  (media & tech, financial, health, public/gov)
- **Defensiv** (Planung, Implementierung, Audit/Review) und
  offensiv (Penetrationstests)

Mitgliedschaften

- ICANN Security and Stability Advisory Committee
- Advisory Board des Internet Namespace Security Observatory
- DNS Root Zone Algorithm Rollover Study Design Team

Andere Personas

- Teilchenphysiker
- Leidenschaftlicher Chorsänger

Motivation

Heutige DNS-Signaturverfahren halten Shors Algorithmus nicht Stand

- Ausreichend starke Quantencomputer in Sicht
- Neue Signaturverfahren erforderlich
- DoH/DoT/DoQ garantieren lediglich Transportverschlüsselung

DNSSEC-Anforderungen:

- Schnelle Validierung
- Kurze Signaturen
- Kurze Schlüssel

Mission: Möglichst realitätsnahes Experiment

In Kooperation mit:
Nils Wisiol und **Matthieu Grillere** (TU Berlin)

Warum FALCON-512?

Algorithm	NIST Verdict	Approach	Private key	Public key	Signature	Sign/s	Verify/s
Crystals-Dilithium-II [29]	Finalist	Lattice	2.8kB	1.2kB	2.0kB		
Falcon-512 [31]	Finalist	Lattice	57kB	0.9kB	0.7kB	3,307	20,228
Rainbow-I_a [56]	Finalist	Multivariate	101kB	158kB	66B	8,332	11,065
RedGeMSS128 [16]	Candidate	Multivariate	16B	375kB	35B	545	10,365
Sphincs$^+$-Haraka-128s [11]	Candidate	Hash	64B	32B	8kB		
Picnic-L1-FS [17]	Candidate	Hash	16B	32B	34kB		
Picnic2-L1-FS [17]	Candidate	Hash	16B	32B	14kB		
EdDSA-Ed22519 [12]		Elliptic curve	64B	32B	64B	25,935	7,954
ECDSA-P256 [12]		Elliptic curve	96B	64B	64B	40,509	13,078
RSA-2048 [12]		Prime	2kB	0.3kB	0.3kB	1,485	49,367

Müller, M. et al.: Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. SIGCOMM Comput. Comm. Rev. 50, 49–57 (2020)

- Bester Fit unter den Kandidaten des NIST-Wettbewerbs
- Sicherheitsniveau vergleichbar mit 256-bit ECDSA (stärker als RSA-2048)

Implementierung und Schlüsselspeicher

OpenSSL-Fork von
Open Quantum Safe (OQS)

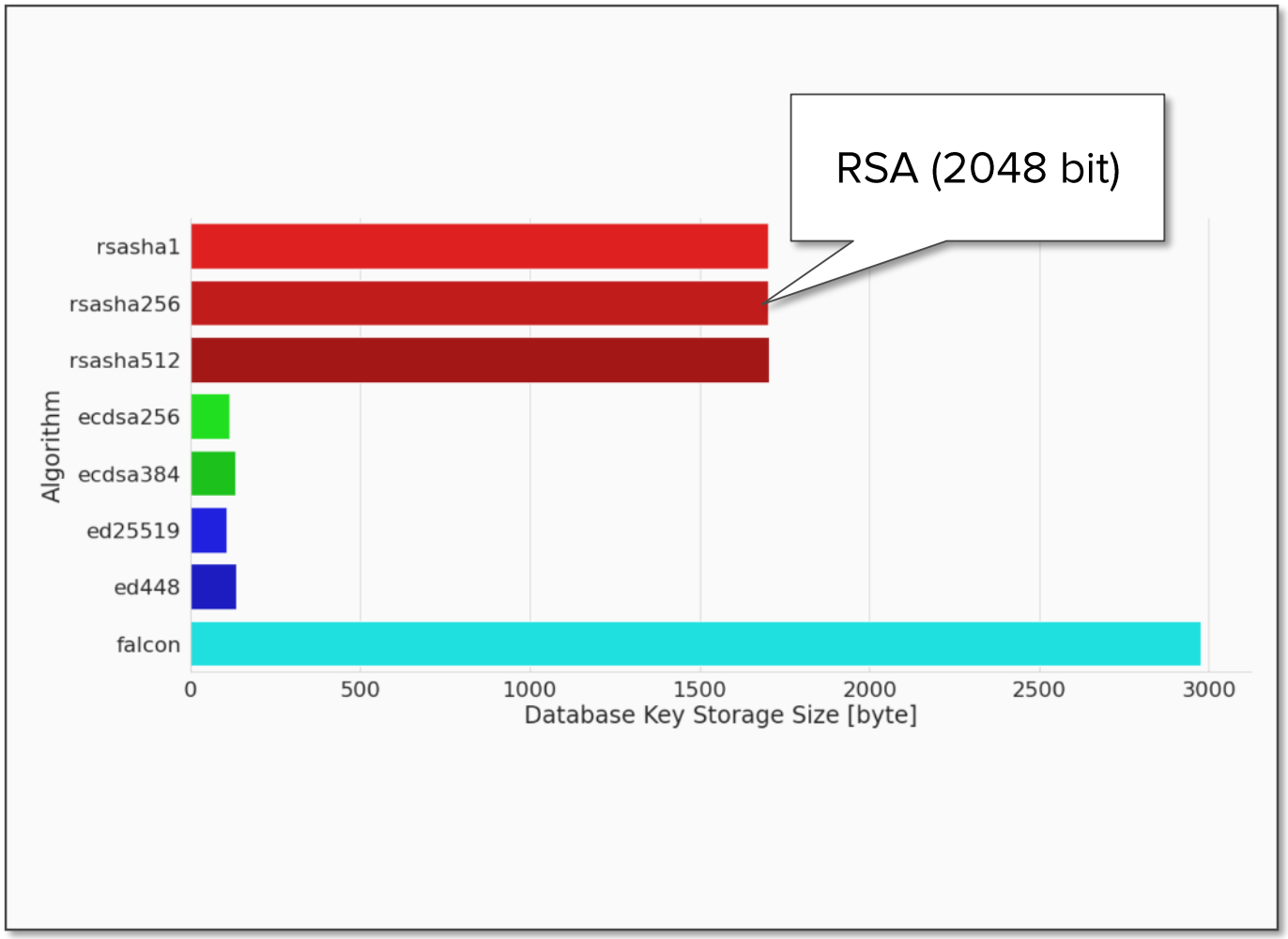
- neu: high-level API für FALCON-512

PowerDNS-Fork

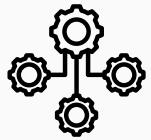
- neu: `CryptoKeyEngine` für OQS
- auch für anderen PQ-Verfahren nutzbar

Speicheranforderungen

- Schlüssel (zzgl. base64-Kodierung)
  - privat: 1.281 Bytes
    (57 KB „expanded” zur Laufzeit)
  - öffentlicher: 897 Bytes
- Signatur: 666 Bytes

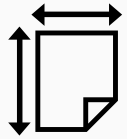


Performance



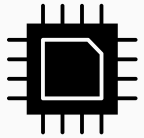
PowerDNS-eigener Performance-Test

`pdnsutil test-algorithms`



Samplegröße

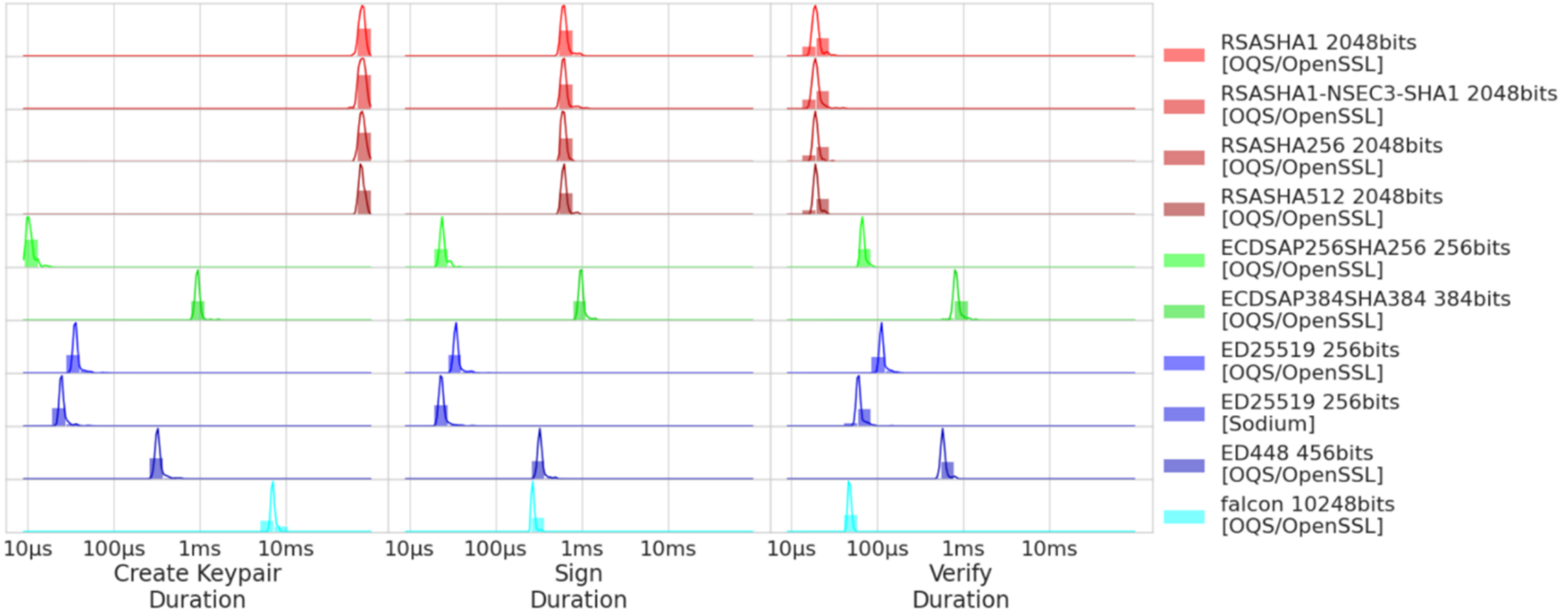
$n = 100$



Mehrfach ausgeführt auf

Intel Core i7-8550U
CPU @ 1.80GHz

Performance



Performance II

Resolver mit manuell konfiguriertem Vertrauensanker für example.com

- Eine Subdomain je Kryptoverfahren
  ➜ falcon.example.com

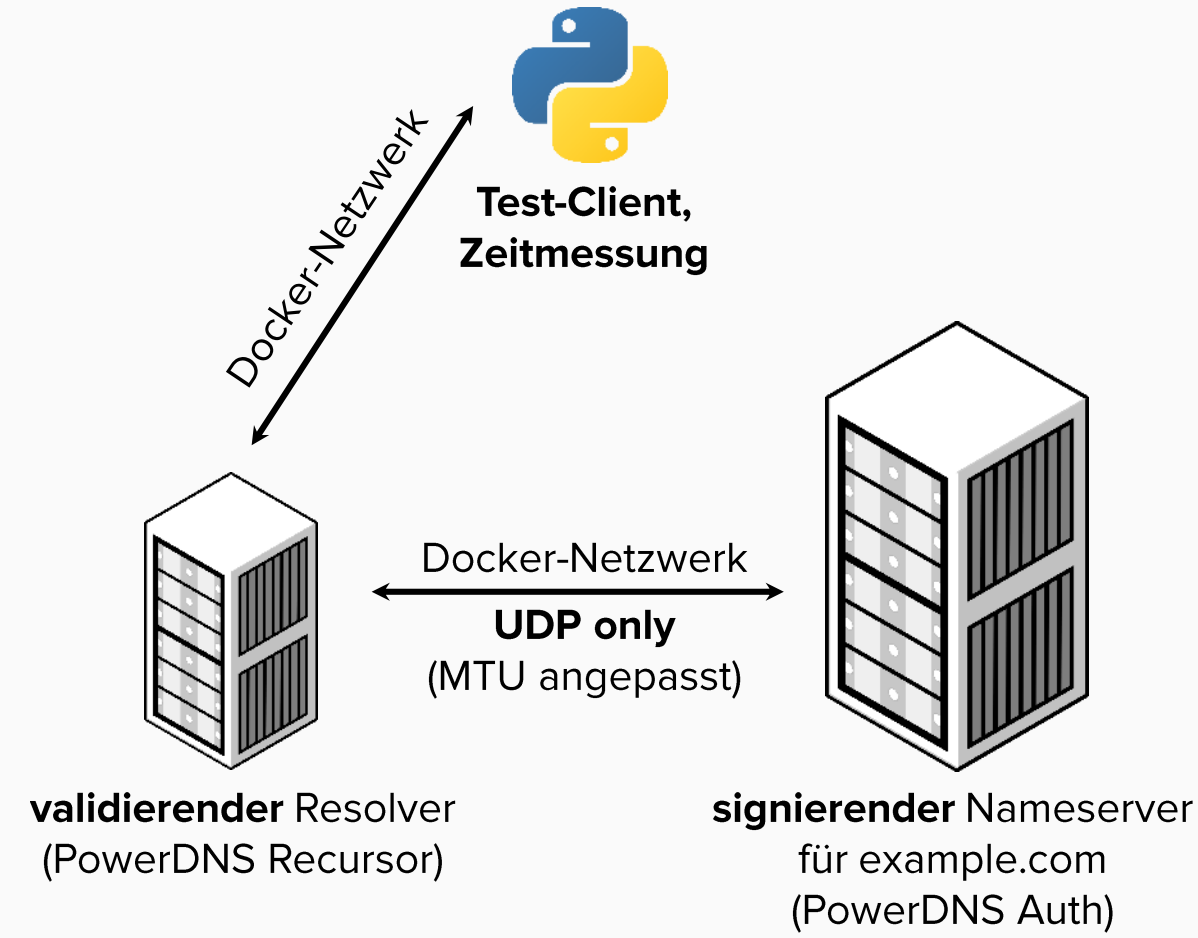
Validierung jeder einzelnen Query

- Umgehung des DNS-Caches

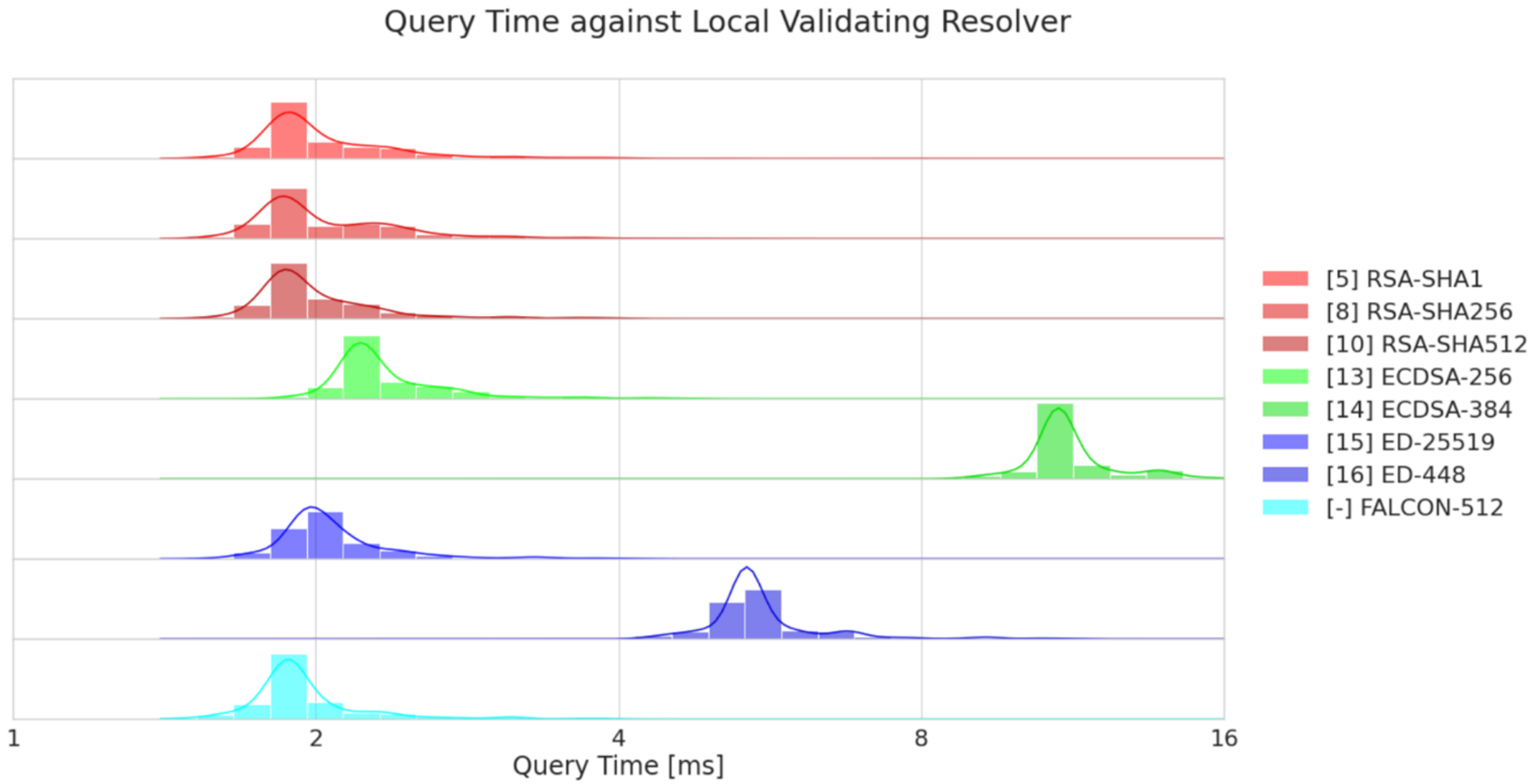
Iterative Testanfragen zu jeder Konfigurationsvariante

Laboraufbau auf GitHub verfügbar

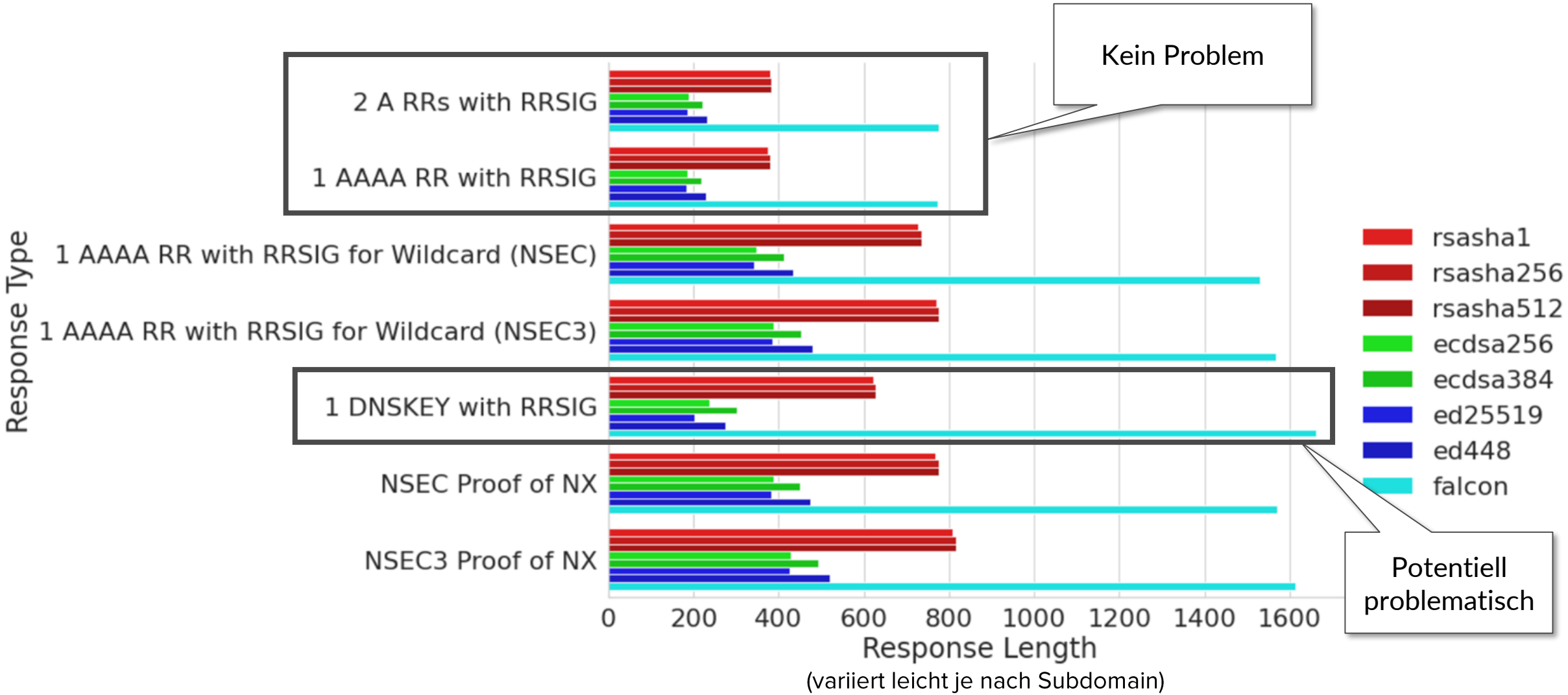
- github.com/nils-wisiol/dns-falcon/



Performance II



Paketgrößen



(variiert leicht je nach Subdomain)

DNS-Abfrage mit non-PQ-Resolver

`dig +dnssec TXT falcon.example.pq-dnssec.dedyn.io @8.8.8.8`

```
; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> +dnssec TXT falcon.example.pq-dnssec.dedyn.io @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36224
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;falcon.example.pq-dnssec.dedyn.io. IN  TXT

;; ANSWER SECTION:
falcon.example.pq-dnssec.dedyn.io. 3600 IN TXT    "FALCON DNSSEQ PoC; details: github.com/nils-wisiol/dns-falcon"
falcon.example.pq-dnssec.dedyn.io. 3600 IN RRSIG TXT 17 5 3600 20230309000000 20230216000000 11130 falcon.example.pq-
dnssec.dedyn.io. Ob7Ptq9ieDaIVVWxoVYXm7UcfEUTo1PiyPYCeGBeUKjihiZ6Ysuo1IV2
I7nEMS/BjTT+AQ35uUhPBlGHqmVcS4oJxuIQt57Z5agk1lYIgQvED627 hjJRdt34TEoR2DElBRApT2YdCmi4kCXl3ST9UytmzlJcDH93PwZzZ5Rc
rjU7XHXukUIxaQM0S4QYReO5CIzb7rxTuM3PCVt+3tlt+xbg02cUOviK nOxiIIGYdK91noJfGa57Z4NtDr5MRrW5pVsE9Fj9cAQdboC6yl6jKMGy
7Zkwht2+PUZhwOPqGHZPHHa9wmuH3lBE8SI7fTRG2VhkDtyRcBCnkcd4 Z5glppDLsfCj+5j53rCIm9SFaPq9674/rsHPWej/Z9cWRabKQUDV6Zn4
d7/yaWwMFLHMWBJyl+HRsXxY2bc95kXMMSpNshPRbtMnKXaOaaeDj43/ [...shortened...]PF4/utewJjTzUbayA1aApwqh0lFOAki8SYyEA==

;; Query time: 356 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Feb 24 11:17:22 CET 2023
;; MSG SIZE  rcvd: 859
```

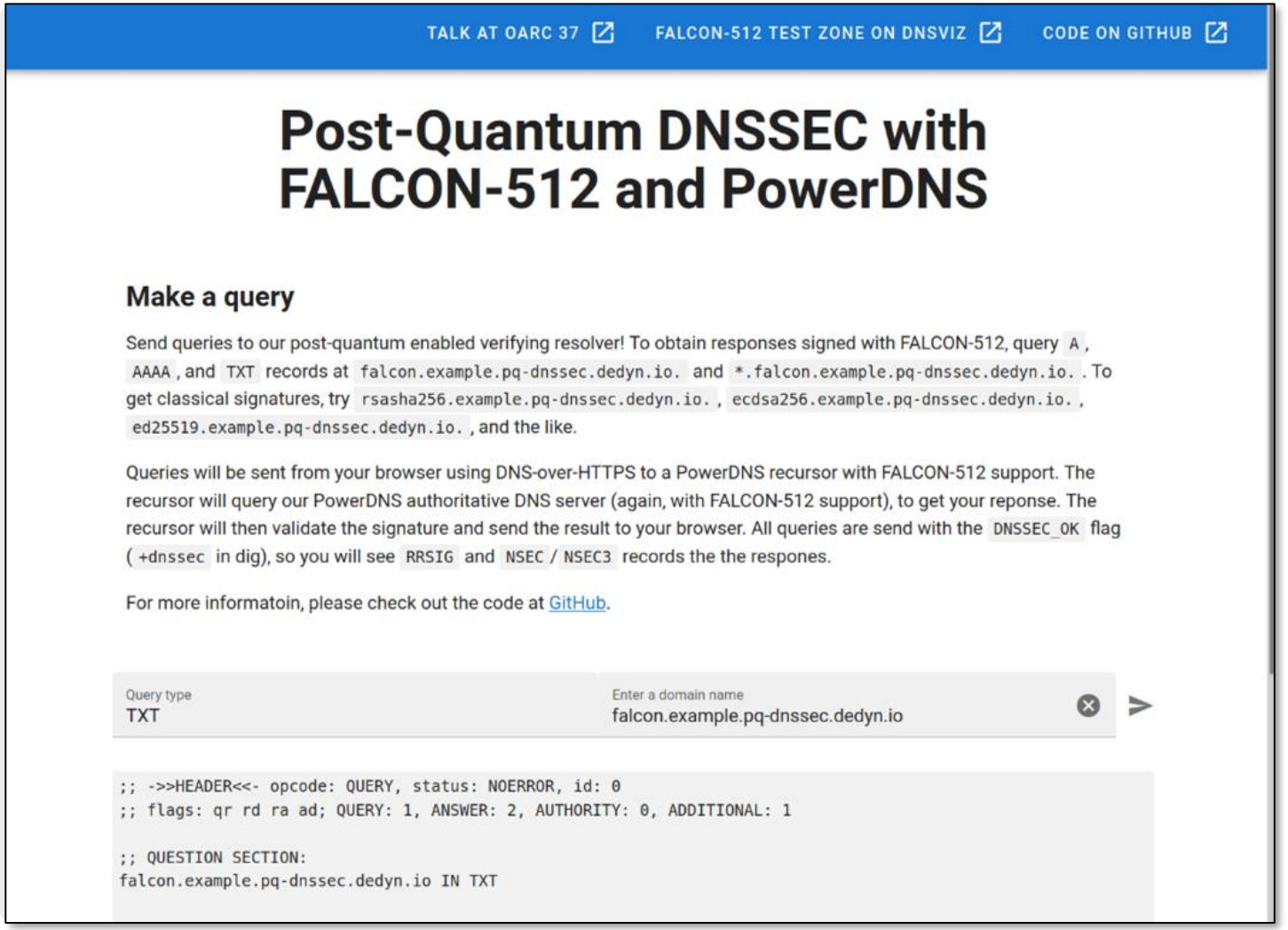
DNS-Abfrage mit PQ-Resolver

dig +dnssec TXT falcon.example.pq-dnssec.dedyn.io @falcon.dedyn.io -p 5302

```
; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> +dnssec TXT falcon.example.pq-dnssec.dedyn.io @falcon.dedyn.io -p 5302
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51312
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;falcon.example.pq-dnssec.dedyn.io. IN  TXT

;; ANSWER SECTION:
falcon.example.pq-dnssec.dedyn.io. 3600 IN TXT    "FALCON DNSSEQ PoC; details: github.com/nils-wisiol/dns-falcon"
falcon.example.pq-dnssec.dedyn.io. 3600 IN RRSIG TXT 17 5 3600 20230309000000 20230216000000 11130 falcon.example.pq-
dnssec.dedyn.io. Ob7Ptq9ieDaIVVWxoVYXm7UcfEUTo1PiyPYCeGBeUKjihiZ6Ysuo1IV2
I7nEMS/BjTT+AQ35uUhPBlGHqmVcS4oJxuIQt57Z5agk1lYIgQvED627 hjJRdt34TEoR2DElBRApT2YdCmi4kCXl3ST9UytmzlJcDH93PwZzZ5Rc
rjU7XHXukUIxaQM0S4QYReO5CIzb7rxTuM3PCVt+3tlt+xbg02cUOviK nOxiIIGYdK91noJfGa57Z4NtDr5MRrW5pVsE9Fj9cAQdboC6yl6jKMGy
7Zkwht2+PUZhwOPqGHZPHHa9wmuH3lBE8SI7fTRG2VhkDtyRcBCnkcd4 Z5glppDLsfCj+5j53rCIm9SFaPq9674/rsHPWej/Z9cWRabKQUDV6Zn4
d7/yaWwMFLHMWBJyl+HRsXxY2bc95kXMMSpNshPRbtMnKXaOaaeDj43/ [...shortened...]PF4/utewJjTzUbayA1aApwqh0lFOAki8SYyEA==

;; Query time: 327 msec
;; SERVER: 95.217.209.184#5302(falcon.dedyn.io) (UDP)
;; WHEN: Fri Feb 24 11:22:37 CET 2023
;; MSG SIZE  rcvd: 859
```

Live-Demo

https://pq-dnssec.securesystems.dev/



Zusammenfassung Falcon-512

Speicherbedarf öffentlicher Schlüssel / Signaturen: 2–3× 2048-bit RSA

Performance:

- Schlüsselerzeugung: schneller als 2048-bit RSA, langsamer als andere
- Signatur: schneller als 2048-bit RSA, langsamer als 256-bit ECDSA
- Validierung: langsamer als 2048-bit RSA, aber schneller als andere

Kompatibilität: Paketgrößen anfällig für TCP Fallback

- DoH/DoT/DoQ hat keine solche Limitierung

Ressourcen:

- Proof of Concept und Live-Demo: https://pq-dnssec.securesystems.dev/
- c’t 3/2023: Die schwierige Suche nach Quantencomputer-sicherer Kryptografie
- ICANN: Quantum Computing and the DNS

Ausblick

Wie viele *validierende* Resolver unterstützen *kein* TCP?

- oder stolpern über große Antworten

Andere PQ-Algorithmen?

- BLISS?
  - ähnliche Schlüssel-/Signaturgröße, aber nicht Teil des NIST-Wettbewerbs
- Merkle Tree

PQ-DNS erfordert Algorithmuswechsel an der DNS-Wurzel (ICANN)

- Schlüsselaustausch 2018 bereits sehr aufwändig (ohne Algorithmuswechsel)
- Paketgrößen könnten Legacy-Clients das Genick brechen

Kompatibilität mit BIND-Implementierung von FALCON-512?

- https://github.com/Martyrshot/OQS-Bind-testing-env (Jason Goertzen)

Vielen Dank! Fragen?