Post-Quantum DNSSEC with FALCON-512 and PowerDNS

ICANN 73 - DNSSEC and Security Workshop
9 March 2022

Matthieu Grillere
Nils Wisiol
Technische Universität Berlin

Peter Thomassen
SSE Secure Systems Engineering

nils.wisiol@tu-berlin.de
https://github.com/nils-wisiol/dns-falcon

Motivation

- Shor's Algorithm breaks all signature schemes used in DNSSEC
  - Sufficiently large quantum computer could be available in the future
  - New signature scheme required
  - DoH, DoT only provide transport security
- DNSSEC requirements
  - Fast validation
  - Short signatures
  - Short-ish public keys

Mission: Create Real-World Experimental Setup

Photo CC-BY 2.0: IBM Research - https://www.flickr.com/photos/ibm_research_zurich/51248690716/

Why 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

- Best fit among NIST finalists and candidates (Müller, M., de Jong, J., van Heesch, M., Overeinder, B. & van Rijswijk-Deij, R. Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. SIGCOMM Comput. Commun. Rev. 50, 49–57 (2020).)
- Security equivalent to 256-bit ECDSA
- Security stronger than RSA-2048

Why FALCON-512?

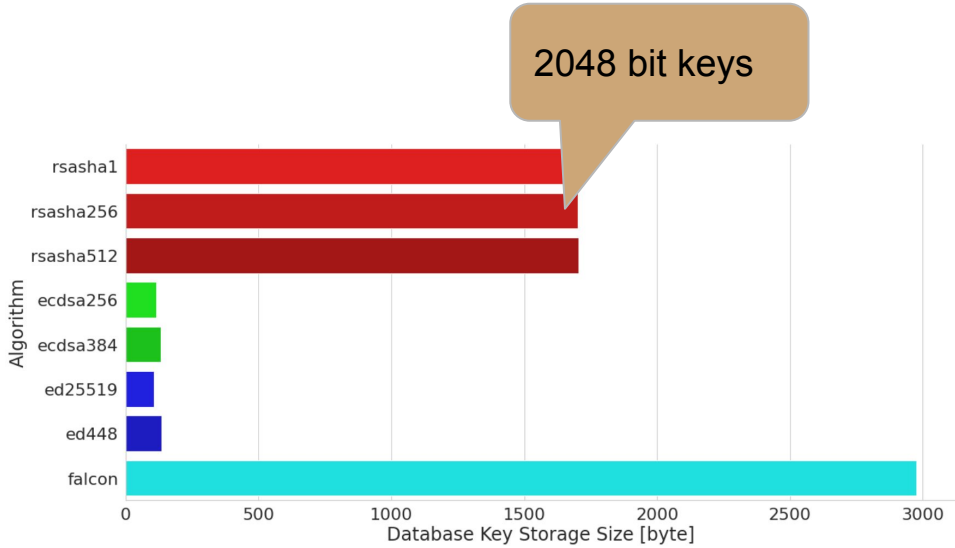
Algorithm	SL	Pub size (in B)	Sign size (in B)	sign/s	verify/s	Priv size (in B)
EdDSA-Ed22519	-	32	64	26k	8k	64
Falcon-512	I	897	666	6k	28k	1280
Falcon-1024	V	1793	1280	3k	13k	2310
qTESLA-p-I	I	15k	2592	1k	1k	5k
qTESLA-p-III	III	46	28k	500	500	16
MQDSS-31-48	I/II	46	28k	36	50	16
MQDSS-31-64	III/IV	64	60k	11	15	24
LUOV-7-57-197	I	11,5k	239	3k	8k	32
LUOV-7-83-283	III	35,4k	337	1k	2k	32
BLISS-BII	I	875	625	5,5k	33k	250
BLISS-BIV	III	875	813	6k	33k	375
SQISign	I	64	204	0.4	20	16

Red meaning, that the value exceeds the requirement. Orange that the hard requirement is not met but within the soft requirement boundary. Pink denoting non-safe algorithm

Implementation and Key Storage

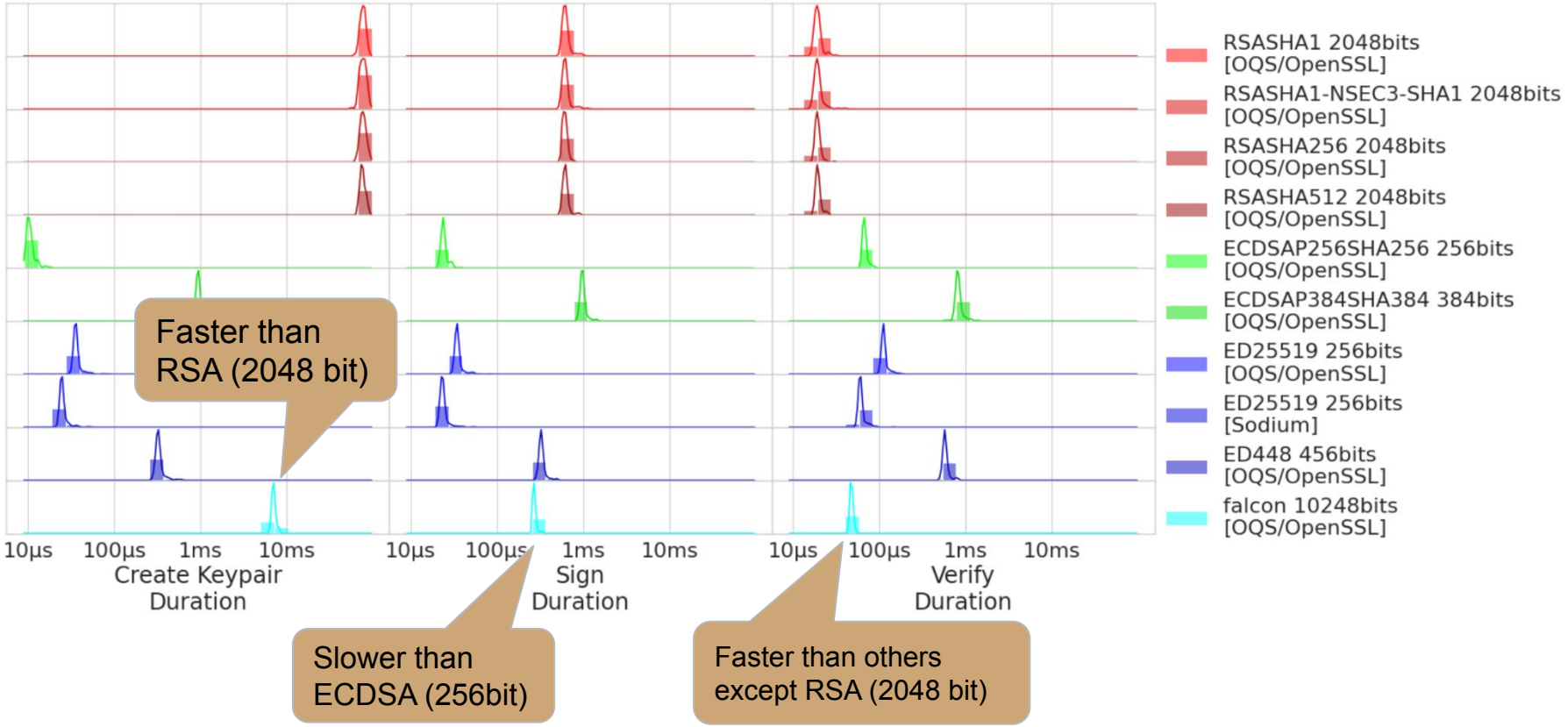
- Using OpenSSL fork of Open Quantum Safe (OQS)

- Database Storage
  - Secret key size: 1281 byte
  - Public key size: 897 byte
  - **Total database storage size: 2976 byte**
    (including base64 and 72 byte formatting overhead)

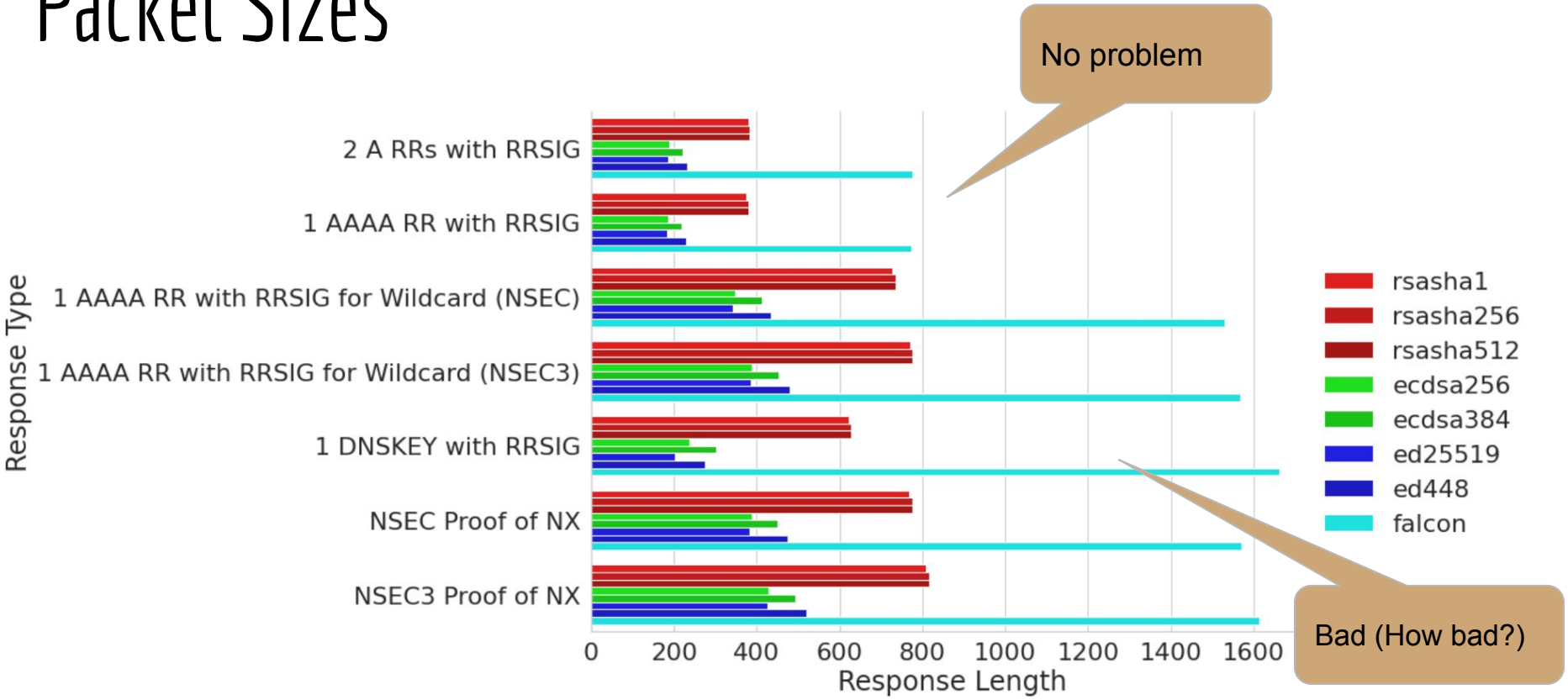


Performance

- PowerDNS ships performance test: `pdnsutil test-algorithms` (mean of 100 samples)
- Run many times on my Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz



Packet Sizes



(vary slightly with involved (query) names)

Try it yourself: Query Using an Unaware Resolver

dig TXT falcon.example.falcon.dedyn.io @8.8.8.8 +dnssec

```
;; <<>> DiG 9.16.1-Ubuntu <<>> TXT falcon.example.falcon.dedyn.io @8.8.8.8 +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62998
;; 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.falcon.dedyn.io.    IN    TXT

;; ANSWER SECTION:
falcon.example.falcon.dedyn.io.    3600 IN    RRSIG    TXT 17 5 3600 20220303000000 20220210000000 31800
falcon.example.falcon.dedyn.io. ObAEWtCiEPuYbpXfzUPV0NX0yY4DsOm8k5lNBY0hhpothB67/G1n+TKQ
... (shortened) ...
Fvy5TiGiKyD8/v909FEqUyEOPFk1K0wyLSHgtYnHEXlJf3jnrOsp998M 9nTaHRMtmiS5lLa4ntCjuQaZIvx931OTp5/b+6g=
falcon.example.falcon.dedyn.io.    3600 IN    TXT    "FALCON DNSSEQ PoC; details: github.com/nils-wisiol/dns-falcon"

;; Query time: 188 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Feb 17 16:44:13 CET 2022
;; MSG SIZE  rcvd: 854
```

Try it yourself: Query Using a FALCON-512 Resolver

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

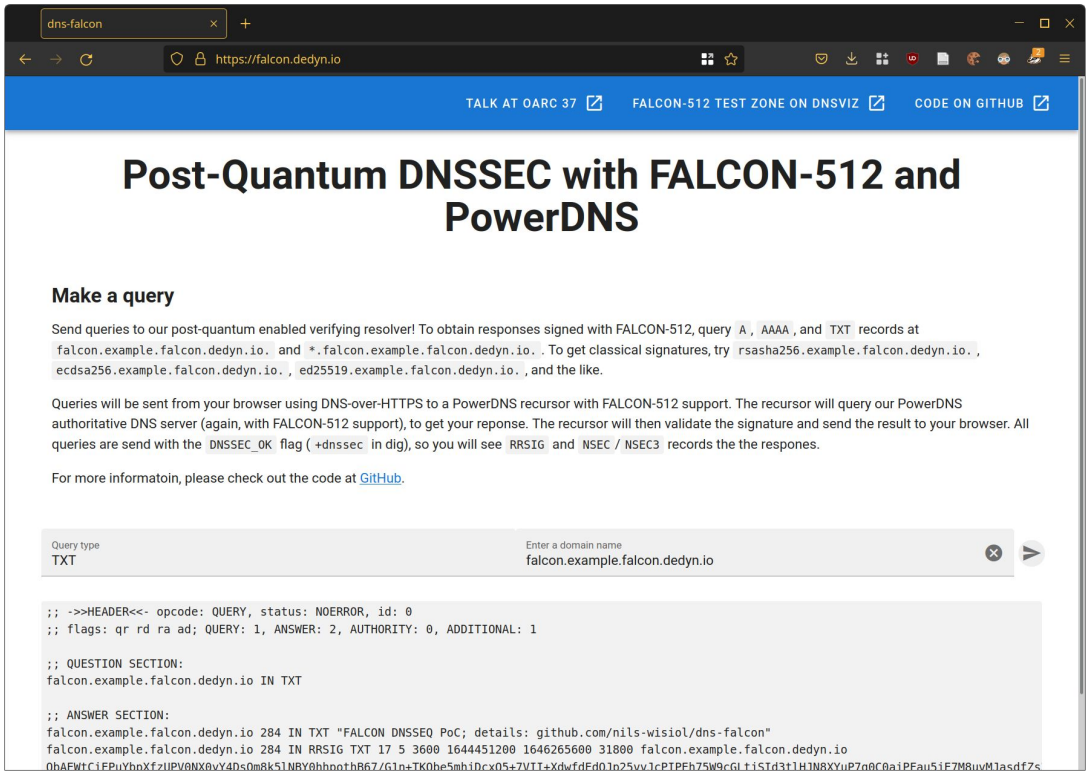
```
;; <<>> DiG 9.16.1-Ubuntu <<>> TXT falcon.example.falcon.dedyn.io +dnssec @falcon.dedyn.io -p 5302
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46685
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
falcon.example.falcon.dedyn.io.    380 IN    TXT    "FALCON DNSSEQ PoC; details: github.com/nils-wisiol/dns-falcon"
falcon.example.falcon.dedyn.io.    380 IN    RRSIG    TXT 17 5 3600 20220303000000 20220210000000 31800
falcon.example.falcon.dedyn.io. ObAEWtCiEPuYbpXfzUPV0NX0yY4DsOm8k5lNBY0hhpothB67/G1n+TKQ
... (shortened) ...
Fvy5TiGiKyD8/v909FEqUyEOPFk1K0wyLSHgtYnHEXlJf3jnrOsp998M 9nTaHRMtmiS5lLa4ntCjuQaZIvx931OTp5/b+6g=

;; Query time: 24 msec
;; SERVER: 130.149.230.84#5302(130.149.230.84)
;; WHEN: Thu Feb 17 16:47:39 CET 2022
;; MSG SIZE  rcvd: 854
```

Try it yourself at https://falcon.dedyn.io



Conclusion

- **Storage:**
  - okay, but 1.5 times 2048bit RSA
- **Performance:**
  - Key creation:
    - faster than 2048bit RSA
    - slower than others
  - Signing:
    - faster than 2048bit RSA
    - slower than 256bit ECDSA
  - Verification:
    - slower than 2048bit RSA
    - but faster than others
- **Online PoC and Playground**
- **Compatibility:**
  - Paket Sizes: Prone for TCP fallback
    - DoT, DoH have no such limitation
  - Future work!

Future Work

- How many *validating* resolvers do not support TCP?
  - Or have other issues with large responses
- Other PQ algorithms?
  - BLISS: similar key and signature size, but not part of NIST competition
  - Merkle Tree?
- What would it take to make the root PQ secure?
  - Root algo rollover
  - Root key rollover was quite a project
- Compatibility with FALCON-512 implementation in BIND of Jason Goertzen? https://github.com/Martyrshot/OQS-Bind-testing-env

Thank You!

Any Questions?

Post-Quantum DNSSEC with FALCON-512 and PowerDNS

Matthieu Grillere matgrillere@gmail.com
Technische Universität Berlin

Peter Thomassen peter.thomassen@securesystems.de
SSE Secure Systems Engineering GmbH, deSEC e.V.

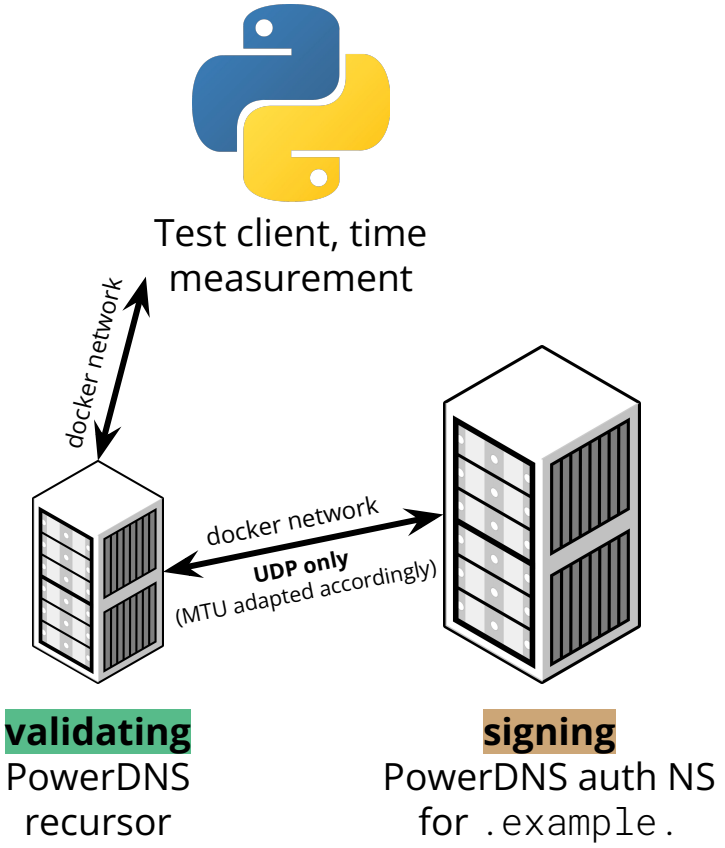
Nils Wisiol nils.wisiol@tu-berlin.de
Technische Universität Berlin, deSEC e.V.

https://github.com/nils-wisiol/dns-falcon
https://falcon.dedyn.io/

Backup

Performance II

- Recursor has classical trust root for `.example` manually configured
- Recursor cache configured such that each query will be validated
- Sequentially query zones with different crypto config
- [complete setup on GitHub]



Performance II