Post-Quantum DNSSEC with FALCON-512 and PowerDNS

Matthieu Grillere · Nils Wisiol
Technische Universität Berlin

Peter Thomassen
SSE Secure Systems Engineering GmbH

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 available ~~"within the next decade"™~~ maybe sometime (thanks, Paul Hofmann)
  - New signature scheme required
  - DoH, DoT only provide transport security
- DNSSEC requirements
  - Fast validation
  - Short signatures
  - Short-ish public keys
- Why FALCON-512?
  - Best fit among NIST candidates ("Retrofitting" paper by Müller et al. 2020)
  - Security equivalent to 256-bit ECDSA
  - Security stronger than RSA-2048
- No PQ-DNSSEC implementation available*

* when we started the project

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

The Mission

Create Real-World Experimental Setup

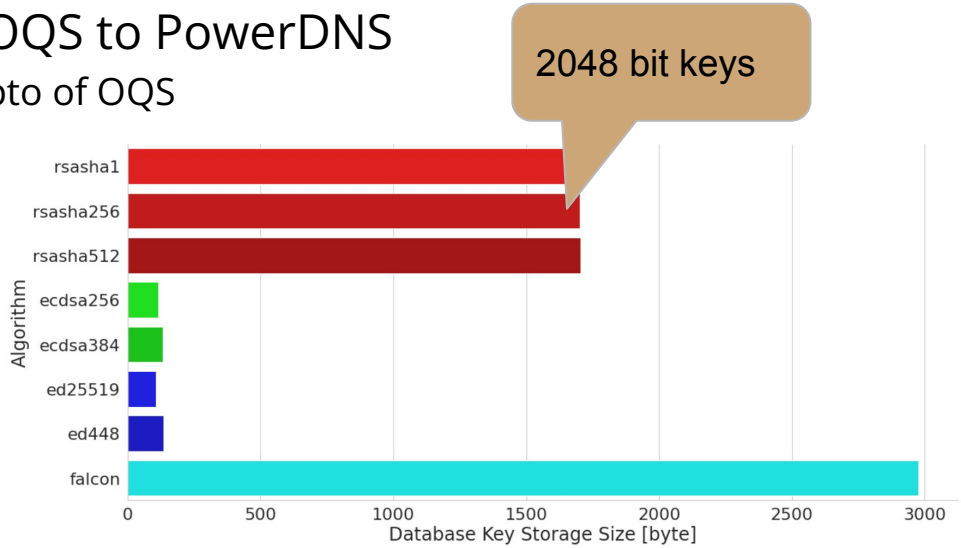
- **Storage:** Required key storage
- **Performance:** Key generation, signing, and validation performance
- **Compatibility:** Measure adoption problems in the real world
  - Packet sizes

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

FALCON-512 in PowerDNS

- Using OpenSSL fork of Open Quantum Safe (OQS)
  - Added high-level/EVP API for FALCON-512 OQS OpenSSL
  - (Not yet merged upstream)
- Added a `CryptoKeyEngine` for OQS to PowerDNS
  - Suitable for other post-quantum crypto of OQS

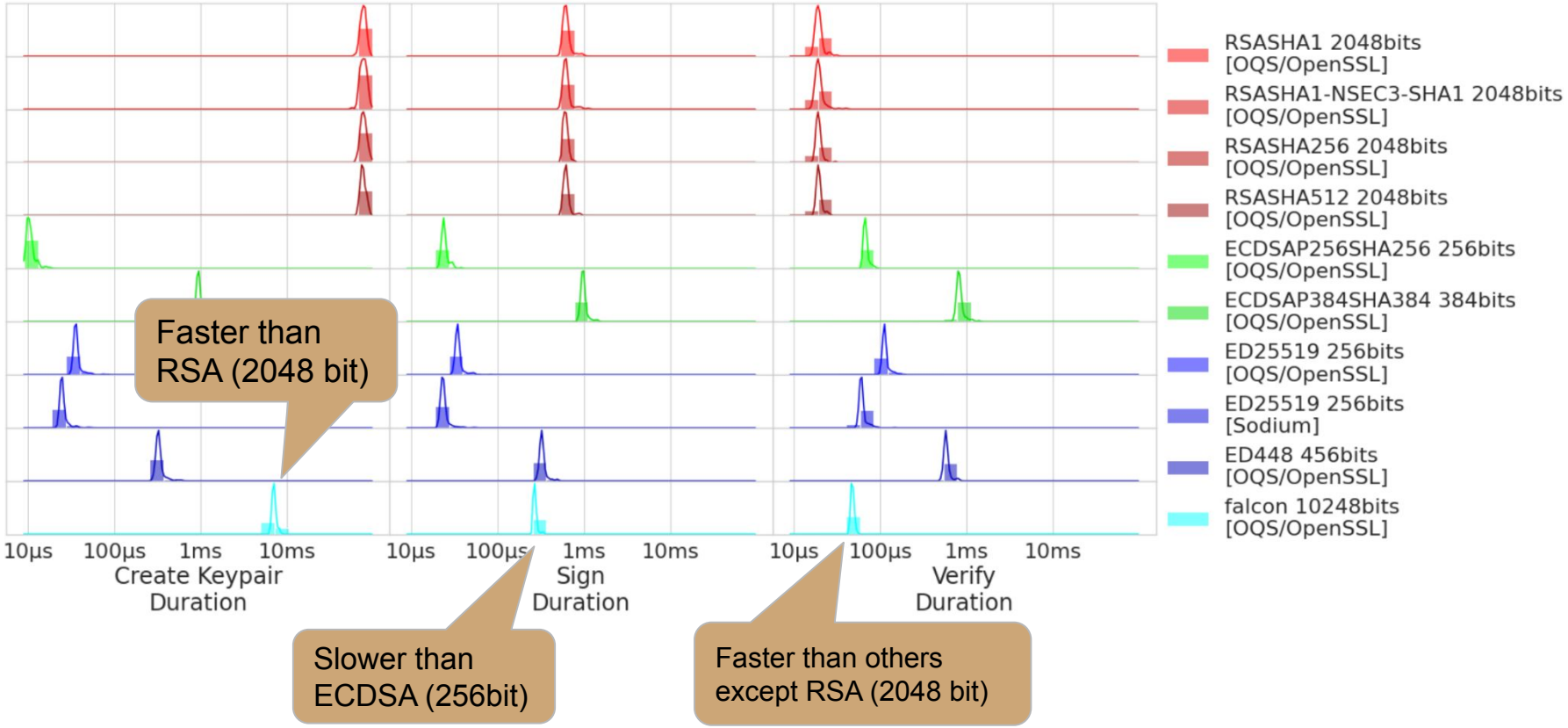
- Database Storage
  - Secret key size: 1281 byte
  - Public key size: 897 byte
  - **Total database storage size: 2976 byte**
    (including base64 and 72 byte formatting overhead)



Performance I

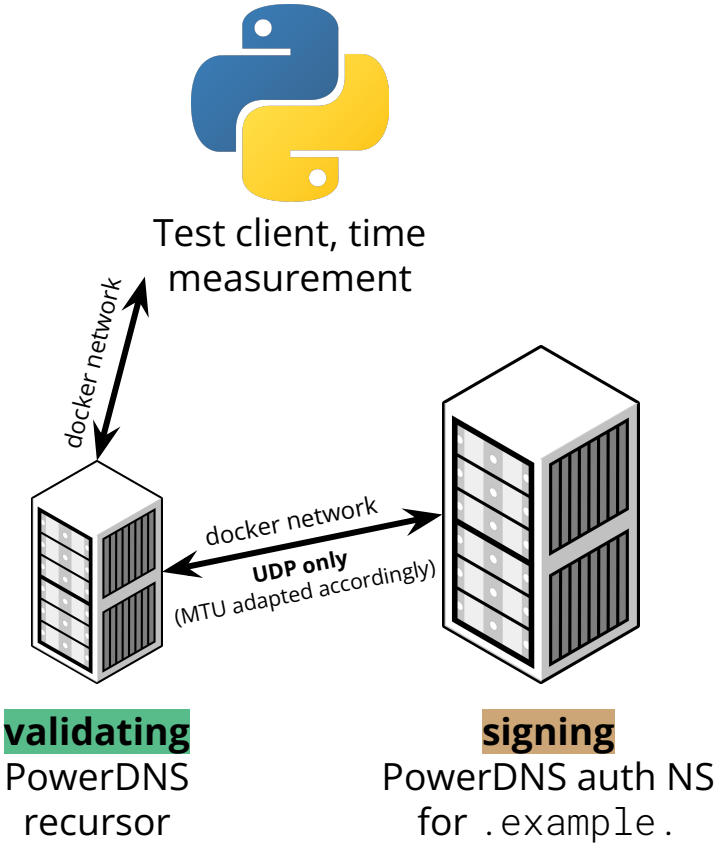
- PowerDNS ships performance test:
  `pdnsutil test-algorithms` (mean of 100 samples)
- Run many times on my Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz

Performance I

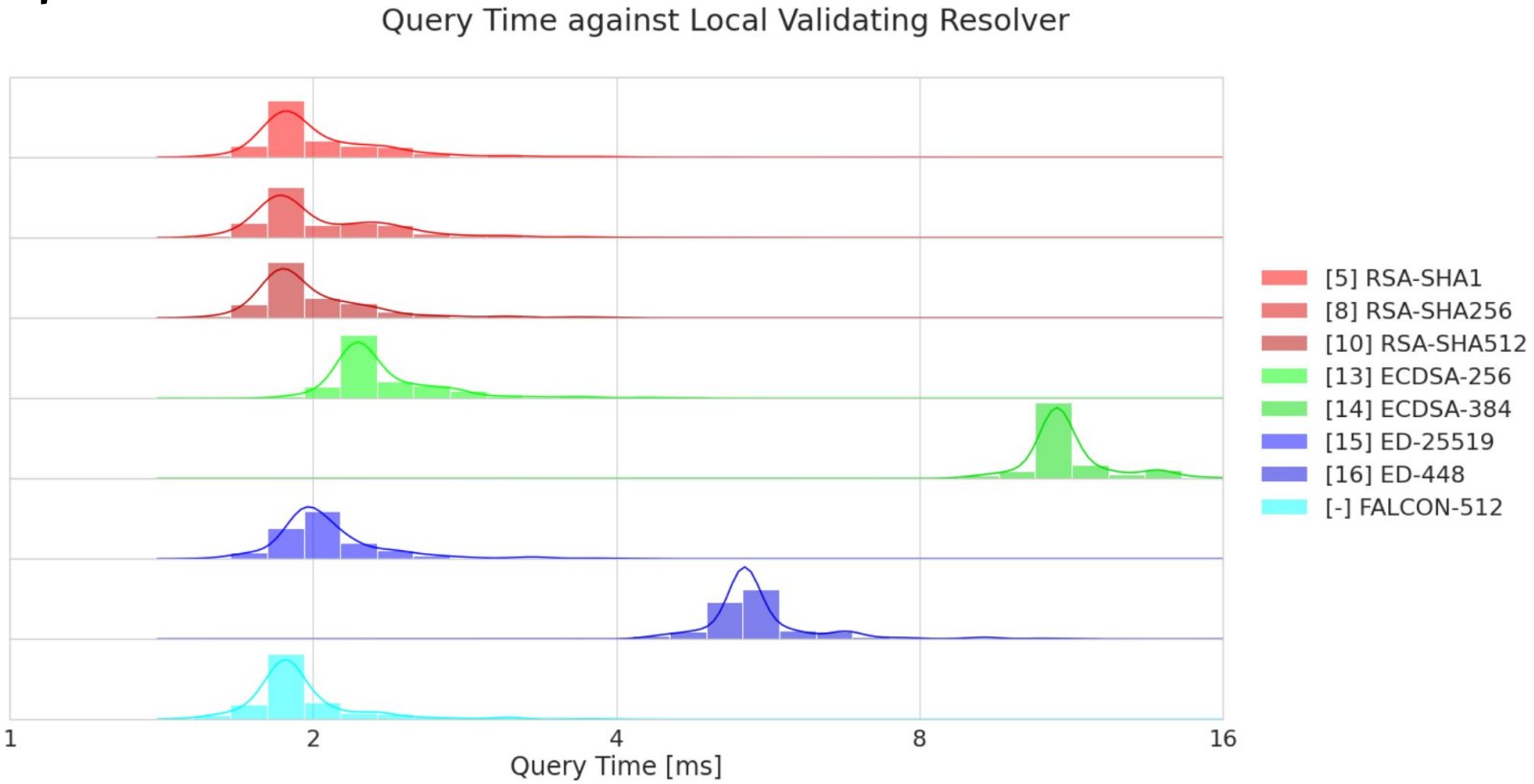


Performance II

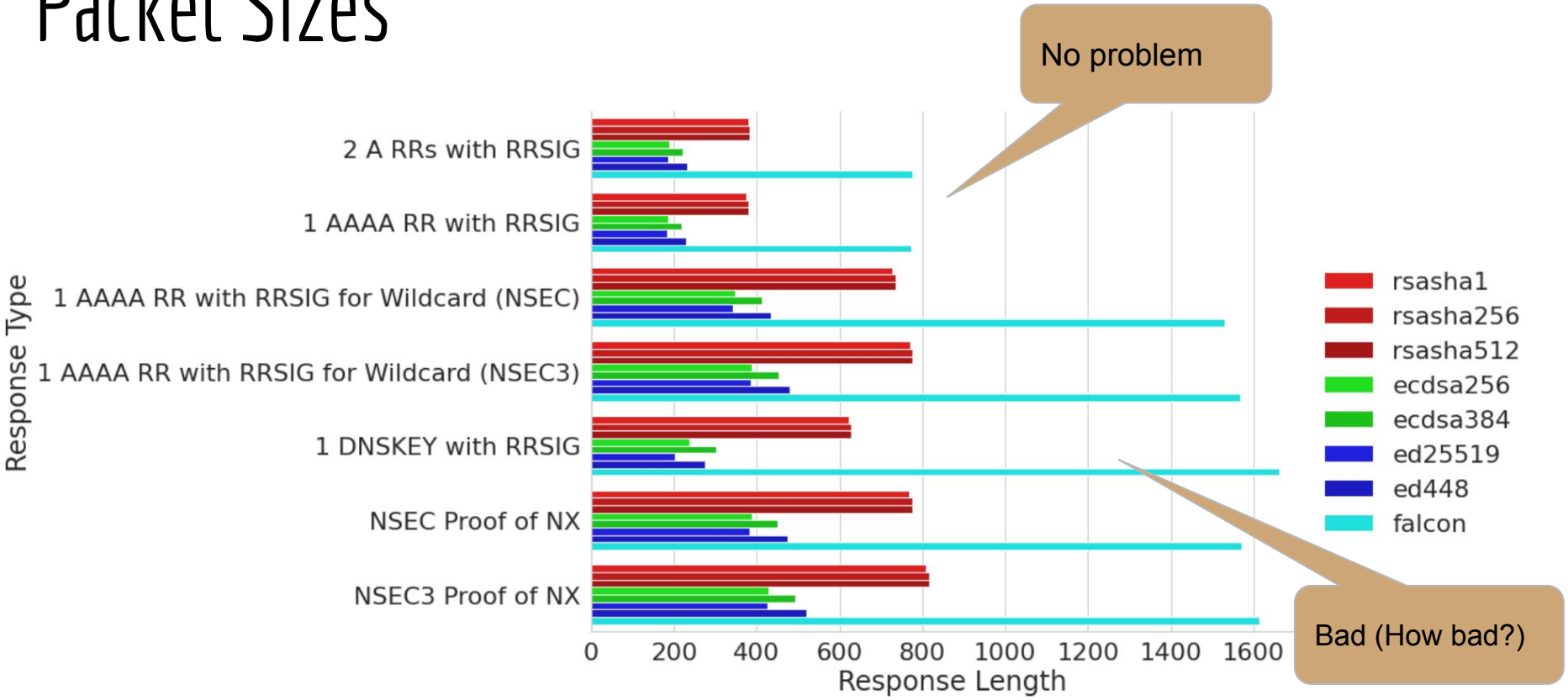
- Recursor has classical trust root for `.example` manually configured
- Recursor cache configured such that each query will be validated
- Sequentially query zones with different crypto config
- [complete setup on GitHub]



Performance II



Packet Sizes



(vary slightly with involved (query) names)

Try it yourself!

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!

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

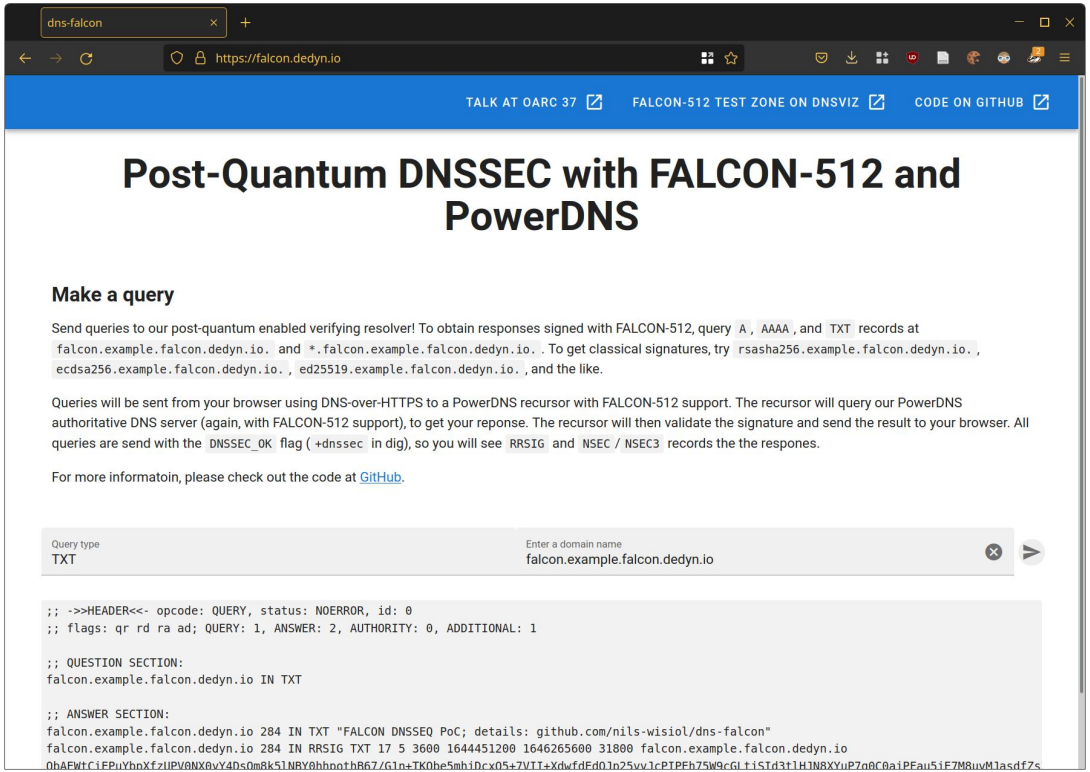
```
;; <<>> DiG 9.16.1-Ubuntu <<>> TXT falcon.example.falcon.dedyn.io +dnssec @falcon.dedyn.io -p 5302
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46685
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; 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
- **Compatibility:**
  - Paket Sizes: Prone for TCP fallback
    - DoT, DoH have no such limitation (but still not a fit)
  - Future work!
- **Online PoC and Playground**

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 BIND implementation of FALCON 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