Randomized Evaluation of SLH-DSA-MTL's Impact on Reducing PQ-DNSSEC Signature Sizes

Minh Hoang Tran
tran189@vt.edu

Dr. Tijay Chung
tijay@vt.edu

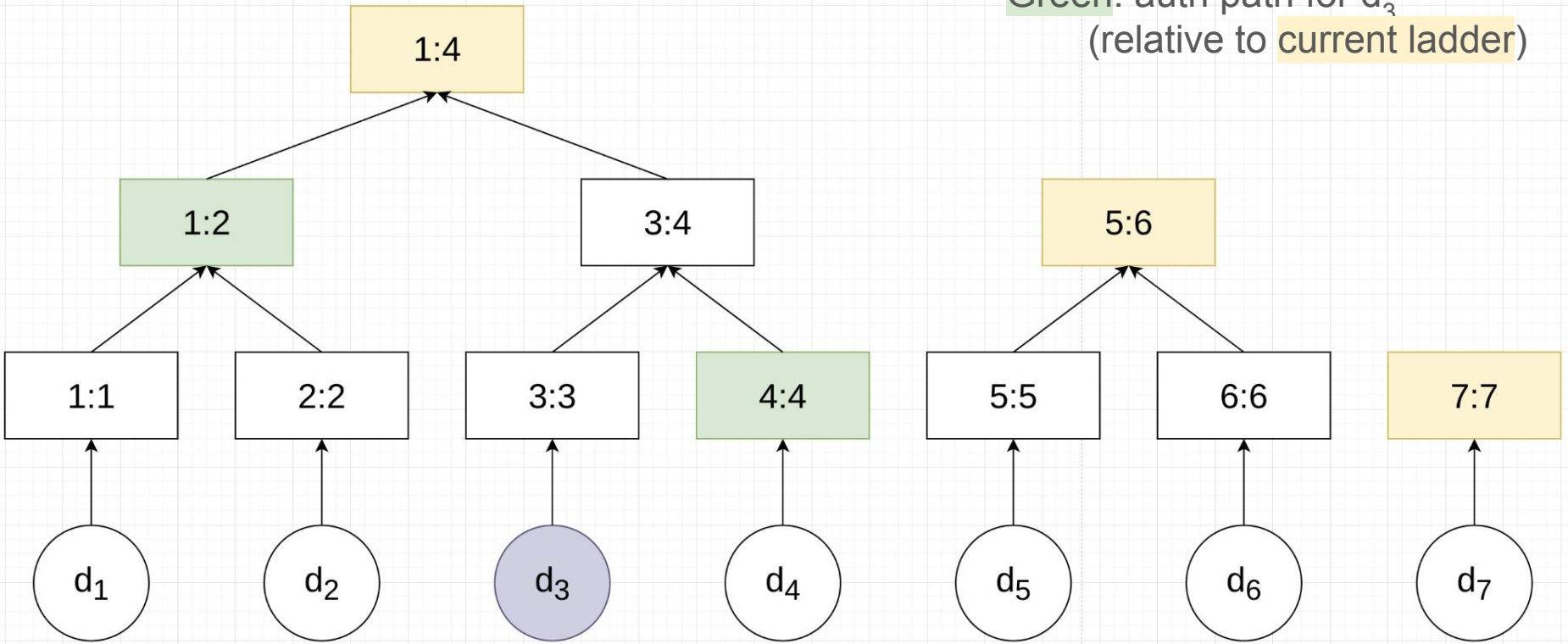
Presentation structure

1. MTL-mode overview
   - signature “backwards compatibility”
2. Zone signing strategies
   - .com RRSIG inception times
3. Ladder endurance “simulation” (evaluation)

State: N = 7

(Verisign Labs') MTL-mode

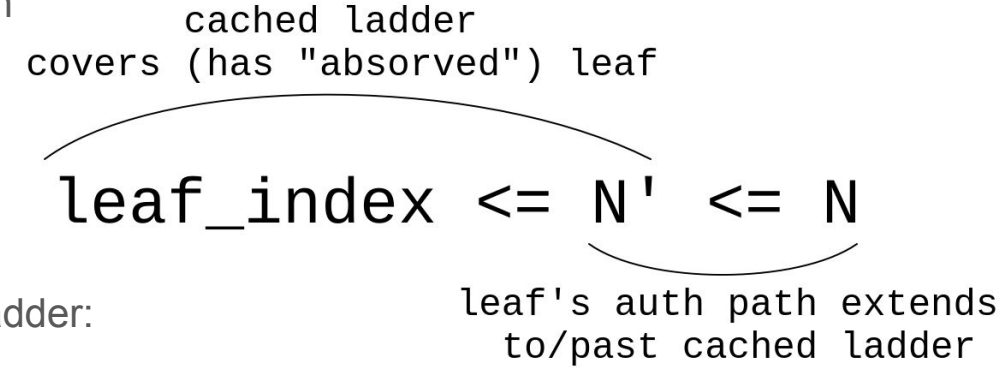
Yellow: ladder
Purple: element d_3 to be verified
Green: auth path for d_3
(relative to current ladder)



MTL mode backwards compatibility requirements

MTL mode signature types:

- Full sig: (PQC-signed-)ladder, auth path
- Condensed sig: auth path



Signatures (auth paths) in MTL are **relative** to a ladder:

- leaf_index: index of item being verified
- N: ladder state to which leaf_index's signature is relative
- N': verifier's cached ladder state

Zone signing strategies

How a zone is signed has a large impact on MTL-mode performance characteristics

There are various ways to sign a (large) DNS zone:

- All-at-once
  - The entire zone is signed at once
  - Signatures have same inception time (+/- random offset)
  - Impractical for very large zones (TLDs), least responsive
- As-needed
  - New signatures signed as records added/changed or old signatures (about to) expire
  - Spreads signing resource consumption across time
  - Most responsive, allows for immediate changes to zone
- Batched
  - Signatures signed in batches
    - Fixed batch size or
    - Percentage of zone or
    - Time interval
  - Tradeoff between zone-responsiveness and signing-spike

Effect of zone signing on MTL mode

- All-at-once
  - Best for MTL mode, all condensed signatures share a single ladder
  - *Impractical for large zones* (TLDs), least responsive
- As-needed
  - Worst for MTL mode, each condensed signature has its own ladder
    - Nameserver: (extremely) large zone size
    - Resolver: more frequent fetching of full signatures
- Batched
  - Tradeoff between batch size and full signature count
  - Condensed signatures within a batch share the same ladder
  - More batches: **more responsive**, **lower signing-spike**, but **more full signatures**
  - Fewer batches: **less responsive**, **higher signing spike**, but **fewer full signatures**

.com zone signing strategy

Data obtained from CZDS

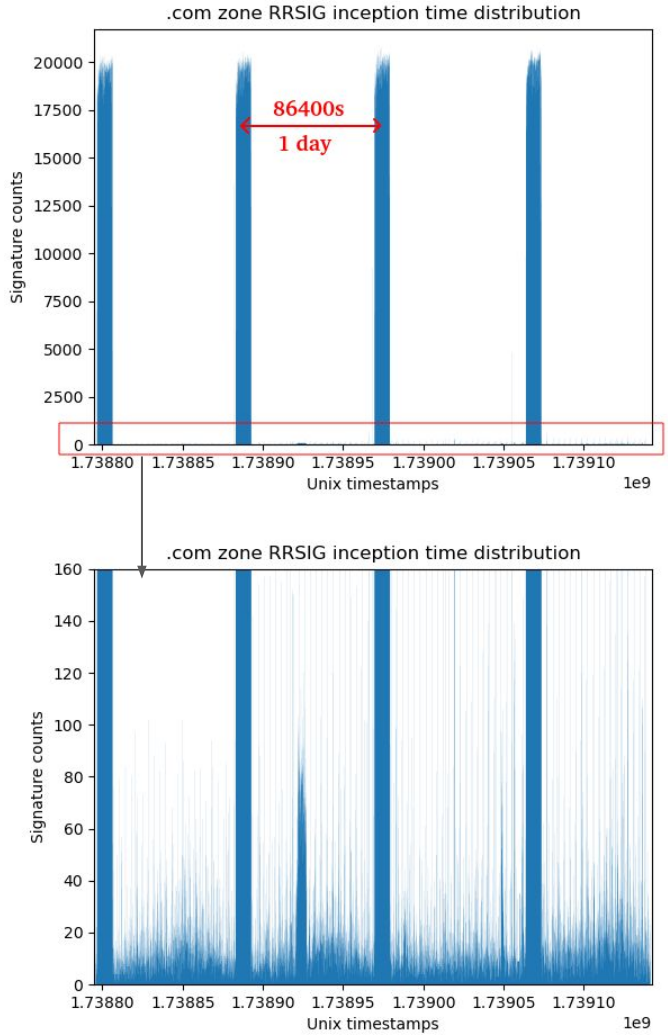
TLDR: Versign signs .com in 4 batches

- 1 batch a day
- 25% of zone per batch

(Comparatively) small number of unbatched RRSIGs

=> Evaluated MTL mode querying on .com zone

- RRSIG inception time used as proxy for ladder state



Evaluation parameters

Uniformly random distribution

of RRSIGs returned

from nameserver to resolver

Query count: 1 000 000 queries

(towards DNSSEC-signed records)

Duration: 1 000 s

=> 1 000 qps

Simulated temporal batching

- per-second
- per-minute
- per-hour
- per-day

100 iterations each

Simulation output:

- number of full signatures required
- (max) ladder cache size
- average queries between full signatures

Eval Result: full signature count

Per-second batching:

- mean: 14.34 full signatures
- median: 14

Per-minute batching:

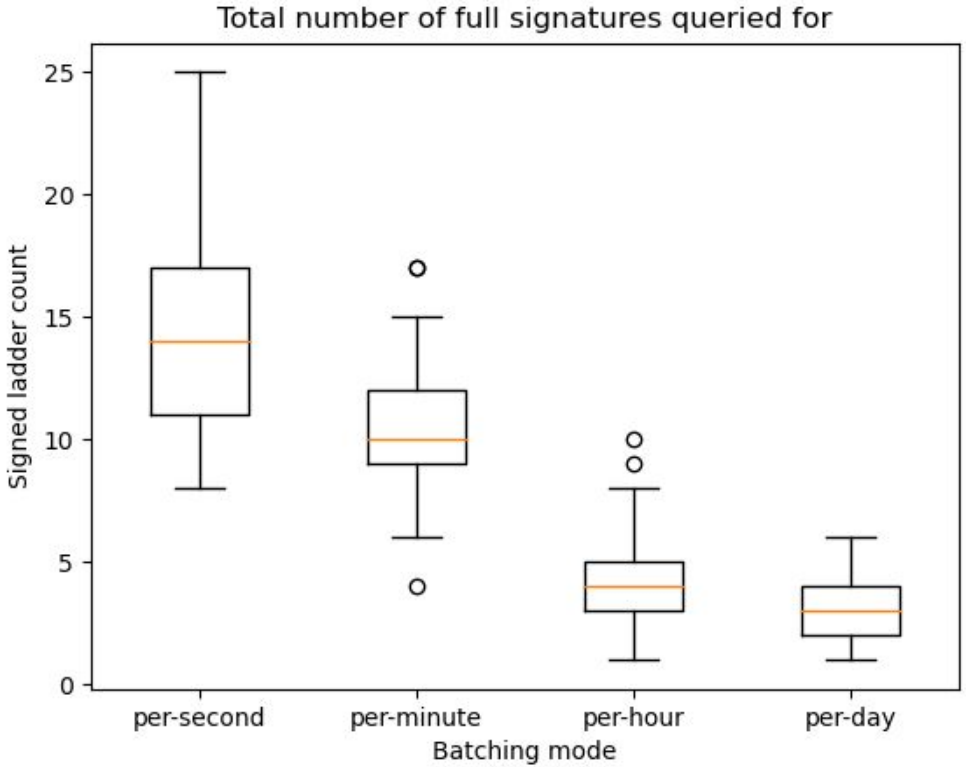
- mean: 10.57
- median: 10

Per-hour batching:

- mean: 4.38
- median: 4

Per-day batching:

- mean: 2.88
- median: 3



Eval result: ladder endurance

Average number of condensed signature served per signed ladder:

- per-second: 74 253.90
- per-minute: 101 204.41
- per-hour: 279 230.16
- per-day: 471 000

Assuming signature sizes (b64 encoded):

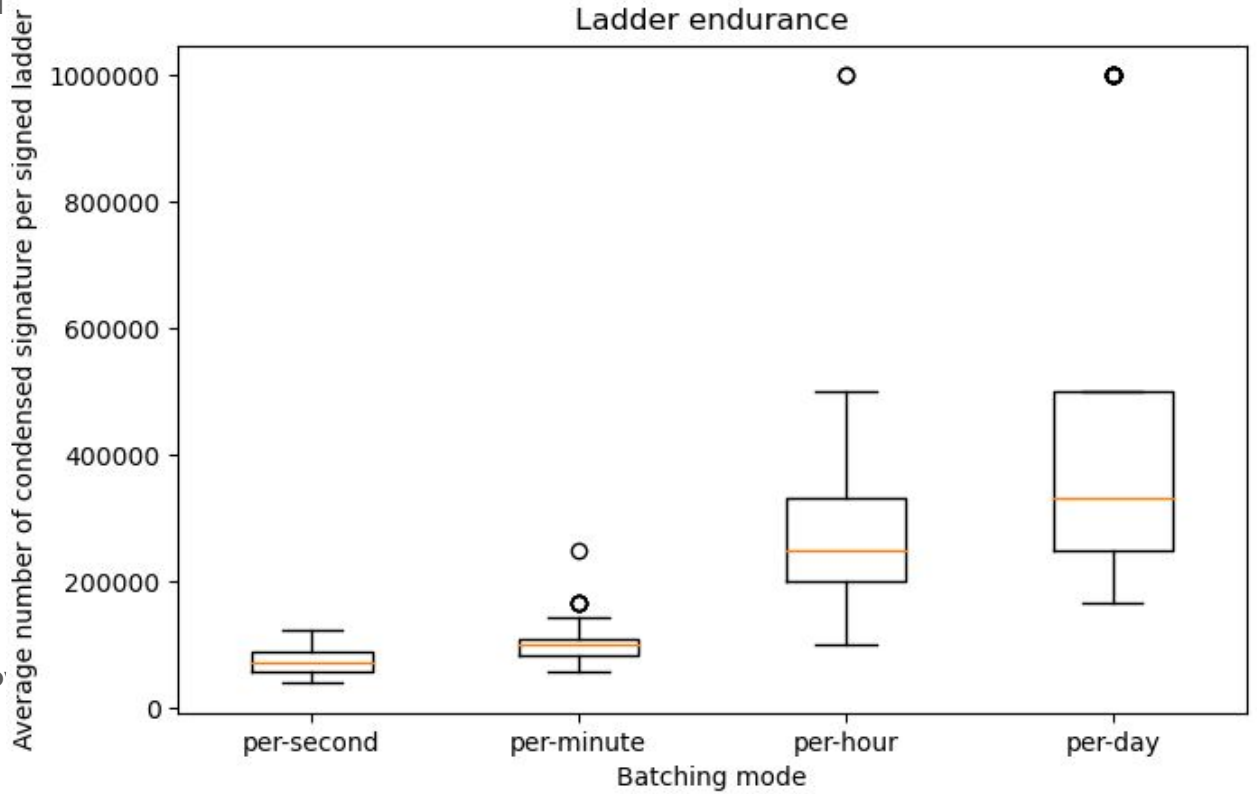
- full sig: 10.68 KB (SLH-DSA-128s)
- condensed sig: 120 B

[draft-fregly-dnsop-slh-dsa-mtl-dnssec-03]

=> Amortized signature size:

- per-second: 120.144 B
- per-minute: 120.106 B
- per-hour: 120.038 B
- per-day: 120.023 B

Note: number assumes resolver **does not remo** previous obtained signed ladders **from cache** (unless TTL or expiration runs out)



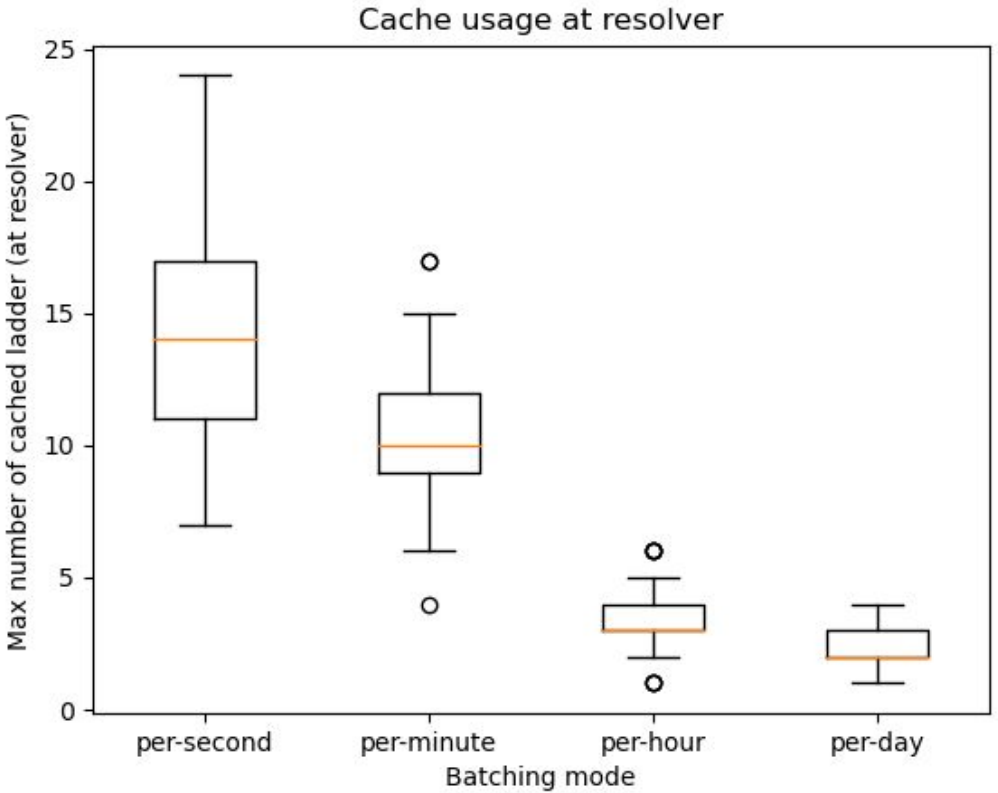
Eval result: resolver cache use

More batching requires the resolver to cache fewer (expensive) signed ladders.

Mean:

- per-second: 14.06 ladders (150.16 KB)
- per-minute: 10.46 ladders (111.71 KB)
- per-hour: 3.46 ladders (36.95 KB)
- per-day:2.23 ladders (23.82 KB)

Note: still assuming 10.68 KB full sig per [draft-fregly-dnsop-slh-dsa-mtl-dnssec-03]



Thank you

Q&A?

Minh Hoang Tran
tran189@vt.edu