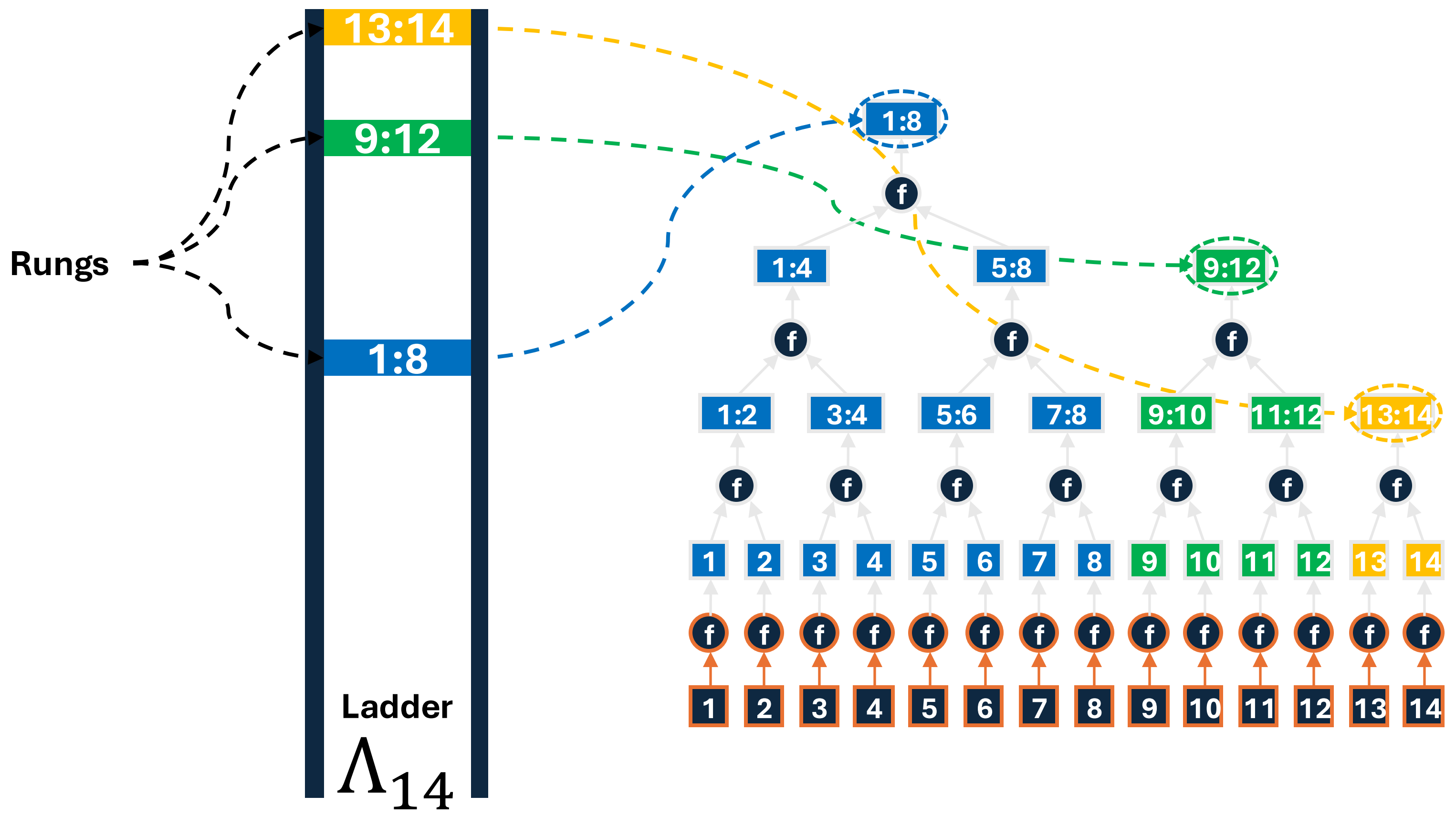
PQ DNSSEC with MTL Mode

Joe Harvey (jsharvey@verisign.com)

Swapneel Sheth (ssheth@verisign.com)

What is MTL Mode?

MTL mode is a method for reducing a signature scheme's operational impact on an expanding message series.



- Rather than signing individual messages, MTL mode signs Merkle Tree Ladders
- Messages are authenticated with Merkle proofs relative to ladders
- Ladders provide backward compatibility since they can verify Merkle proofs constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time. (DNSSEC, OCSP, etc.)

MTL Mode Specification

MTL mode originates in two documents:

Document	Purpose
draft-harvey-cfrg-mtl-mode	Specification which defines how MTL mode is constructed and works.
URL: https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/	
draft-harvey-cfrg-mtl-mode-considerations	Document that describes considerations when integrating MTL mode into an application
URL: https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode-considerations/	

MTL mode open source library implementation:

URL: https://github.com/verisign/MTL

Intellectual Property

- Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Drafts
- IPR declarations 6174-6176 and 6501 give the official language

https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-harvey-cfrg-mtl-mode
https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-harvey-cfrg-mtl-mode-considerations
https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-fregly-dnsop-slh-dsa-mtl-dnssec

What is SLH-DSA-MTL-DNSSEC?

draft-fregly-dnsop-slh-dsa-mtl-dnssec describes the application of MTL mode to DNSSEC.

https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/

This draft defines how to use MTL mode with DNSSEC leveraging SLH-DSA (as defined in FIPS 205) as the underlying signature scheme.

Reference Open Source Implementations	Link
NSD [authoritative resolver]	https://github.com/NLnetLabs/nsd/pull/397
Unbound [recursive resolver]	https://github.com/verisign/mtl-mode-unbound

Zone Signing

At IETF-120 we hosted a Hackathon where we demonstrated NSD serving a zone signed per the SLH-DSA-MTL-DNSSEC draft.

Results: Created a signed zone – can verify it with the open source MTL library.

- The PQC signed zone footprint is larger than a zone signed with RSA or Elliptic Curve algorithms.
- Signing batches of records aligns with the zone signing model well.
- Signing requires a modification to the typical zone signing workflow, with two passes over the RRSets.
  - Pass one adds the records to the message series (requires only hashing operations).
  - Pass two gets the authentication paths and fetches/signs the current ladder (requires fetching hashes and signing with the PQC algorithm).

Zone Verification

At IETF-121 we hosted a Hackathon where we demonstrated the unbound recursive resolver verifying DNSSEC including records that were signed as described in the SLH-DSA-MTL-DNSSEC specification.

Results: Verified DNSSEC signatures produced with SLH-DSA-MTL-DNSSEC

- This POC confirms the query and retry methods in the draft are sufficient.
- Can start validating MTL mode with DNSSEC
  - Ladder Endurance
  - Response sizes
  - Cache memory footprint
- SOA Method has some limitations that the EDNS option method will resolve.
  - Validation requires a little extra work
  - Backward compatibility is limited
  - Client responses are more challenging due to not knowing if the client wants the AD bit or a full/condensed signature.

Interoperability

As the SLH-DSA-MTL-DNSSEC draft specification is verified, we will need to expand metrics collection and interoperability testing.

- Goals
  - Study interoperability with other proof-of-concept implementations in other code bases.
  - Collect further feedback from the resolver community on overall application and operational experience.

Next Steps

- Test incrementally signed zones
- Collect metrics on DNSSEC with MTL mode
- Expand the POC and test interoperability