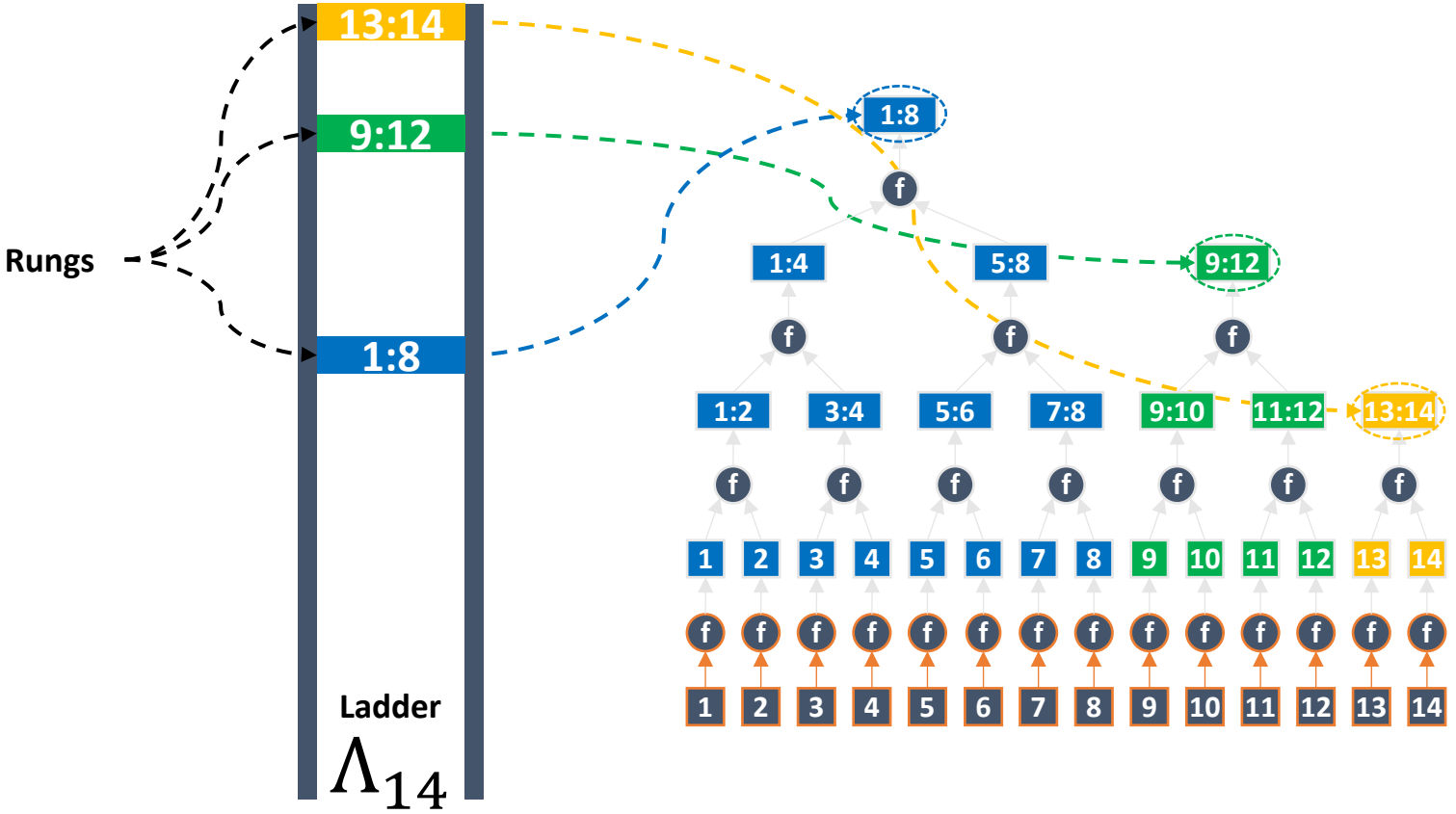
Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC

Andrew Fregly
afregly@verisign.com
IETF-120

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

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 potentially verify Merkle proofs constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time. (DNSSEC, OCSP, etc…)

Trade-offs for MTL Mode for DNSSEC

- Benefits
  - Condensed signatures address size issues current NIST PQC signature algorithms present to DNSSEC: A condensed signature in an RRSIG can be comprised of a Merkle proof + reference to signed ladder
    - Limitations related to transmitting large DNSSEC responses over UDP
    - Memory footprint for large zones in authoritative name servers and resolver caches
    - Signing CPU load imposed by some signature schemes (SLH-DSA!)
  - Per our draft for CFRG, "Merkle Tree Ladder (MTL) Mode Signatures" (https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/), MTL mode operations can be aligned with the underlying signature scheme to ensure proper cryptographic separation
  - Hash-based scheme ➔ quantum-safe design
    - "Stateful" hash-based (if evolving Merkle tree is considered to be state), but graceful degradation of security instead of key compromise if state is reused
  - Hash functions are already available in many hardware platforms, making MTL mode performant
  - Incremental zone signing of RRset batches can significantly reduce CPU requirements. Only one ladder per batch needs to be signed with the underlying signature scheme.
  - Impact of hybrid signatures schemes is minimized as they are applied to signed ladders rather than RRSIGs comprised of condensed signatures
- Drawbacks
  - Requires a protocol update to support retrieving signed ladders
  - Resolver changes to handle signed ladder caching and full signature production

Overview of draft-fregly-dnsop-slh-dsa-mtl-dnssec-01

- Defines signature formats for both “condensed” signatures and “full” signatures
- Defines the public key format as an SLH-DSA (SPHINCS+) public key.
- Defines the use of EDNS(0) as the means to request full signatures containing signed ladders
- A detailed example containing condensed and full signatures for a signed zone is provided.

Intellectual Property

- Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Draft
- IPR declarations [6240-6242] give the official language (https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-fregly-dnsop-slh-dsa-mtl-dnssec)

Next Steps

- Please review the draft and provide feedback
- We are looking for partners to participate in interoperability testing
- We anticipate using testbeds such as SIDN Labs “A quantum-safe cryptography DNSSEC testbed” (https://www.sidnlabs.nl/en/news-and-blogs/a-quantum-safe-cryptography-dnssec-testbed) for SLH-DSA-MTL for DNSSEC related research