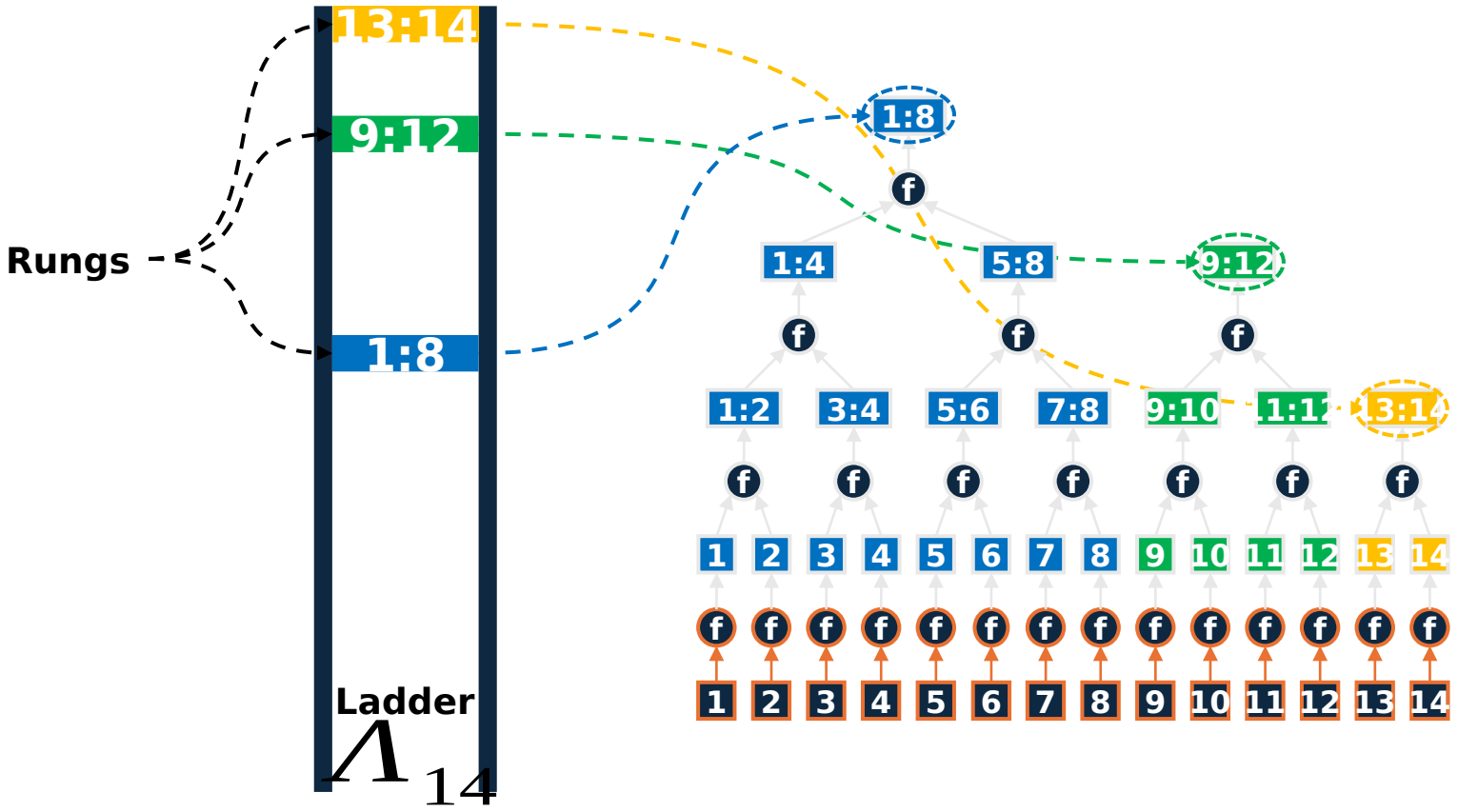
Experiments with MTL Mode in DNS Resolvers

Joe Harvey (jsharvey@verisign.com)
Swapneel Sheth (ssheth@verisign.com)
Willem Toorop (willem@nlnetlabs.nl)

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 DNSSEC

Draft Specifications

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

Open source code that implements MTL mode:

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

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

IETF Hackathon Efforts

- IETF-118
  - Introduced MTL mode open source library
- IETF-120
  - Demonstrated SLH-DSA-MTL signatures on zone file
- IETF-121
  - Implemented draft-fregly-dnsop-slh-dsa-mtl-dnssec
    - NSD providing full and condensed signatures based on EDNS option flag
    - Unbound providing verification of SLH-DSA-MTL signatures
      - Verifies condensed signatures from cached ladders
      - Requests full signatures for records that do not have a cached ladder

IETF-121 NSD & Unbound Testing Results

SUCCESS!

Unbound Config

```
server:
    trust-anchor: ". DS 20326 8 2
e06d44b80b8f1d39a95c0b0d7c65d08458e880409
bbc683457104237c7f8ec8d"
    trust-anchor: "example.com. DS 42788 248 2
d66cf16674c72d32341e0d0781a20819352be3e57
7d8082d2df2bcc2a8394a61"


stub-zone:
    name: example.com
    stub-host: stub.example
    stub-addr: 206.189.116.190
```

Unbound Log

```
libunbound[178913:0] info: MTL signature (248) - Full Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - Full Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com has address 192.0.2.1
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com has IPv6 address 2001:db8::1
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com mail is handled by 10 mail.example.net.
```

Next Steps

- Will be discussing this and more at the PQ DNSSEC side meeting
  - Thursday, November 7, 2024
  - 10:00-11:30 (local Dublin time)
  - Wicklow Hall 2A