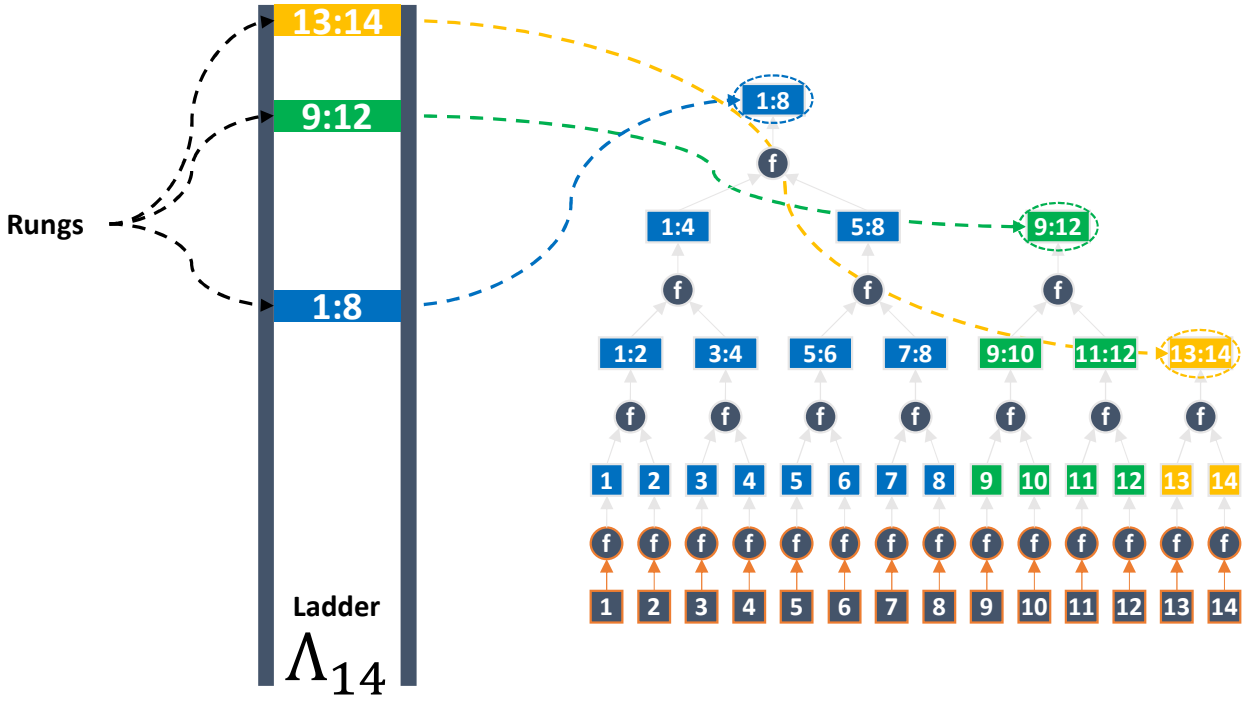
draft-harvey-cfrg-mtl-mode Merkle Tree Ladder (MTL) Mode Signatures

Burt Kaliski
bkaliski@verisign.com
IETF-120

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…)

IETF-117 MTL Mode Next Steps

- Please review the draft and provide feedback (is CFRG mailing list the right place?)
- We plan to release an open-source library that combines MTL Mode with SPHINCS+
- We also plan to publish an I-D on using MTL Mode with DNSSEC (DNSOP?).

Update since IETF-117

- MTL Mode Draft has been updated based on feedback and evolution of PQ standards from NIST.
  - Topic of the IETF-118 Hackathon “Introduction to the MTL Mode Open Source Library” https://wiki.ietf.org/en/meeting/118/hackathon
  - Version 03 now aligns with the NIST FIPS signature guidelines that include a pre-hashing separator.
    - NIST defines pure hashing as prefixed with a 0x00 byte
    - NIST defines pre-hashing as prefixed with a 0x01 byte
    - Should other prefix flags be defined for other modes of operation?
      - MTL Mode defines a prefixes of 0x80 and 0x81 for further separation of hashing operations.
- MTL Mode Open Source Software has been released
  - License Terms - https://github.com/verisign/MTL/blob/main/LICENSE.md
  - Source Code - https://github.com/verisign/MTL

Update since IETF-117 (Continued)

- I-D on using MTL Mode with DNSSEC has been published for discussion at DNSOP
  https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/
  - Version 02 demonstrates how the MTL signatures work with DNS RRSIG records
  - Topic of the IETF-120 Hackathon “Exploring Implementation Approaches for Merkle Tree Ladder Mode Signatures for DNSSEC” https://wiki.ietf.org/en/meeting/120/hackathon

Intellectual Property

- Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Draft
- IPR declarations 6174-6176 give the official language
  https://datatracker.ietf.org/ipr/search/?draft=draft-harvey-cfrg-mtl-mode&rfc=&doctitle=&group=&holder=VeriSign%2C+Inc.&iprtitle=&patent=&submit=draft

Next Steps

- Request that CFRG take up MTL Mode as part of researching “modes of operation” for digital signatures, including guidance to applications on domain separation between pure signing, pre-hash signing and other ways of processing message inputs to a signature scheme.
- Work with the DNS community to evaluate MTL Mode DNSSEC and the operational considerations.