Revocation Status with MTL Mode

November 6, 2024

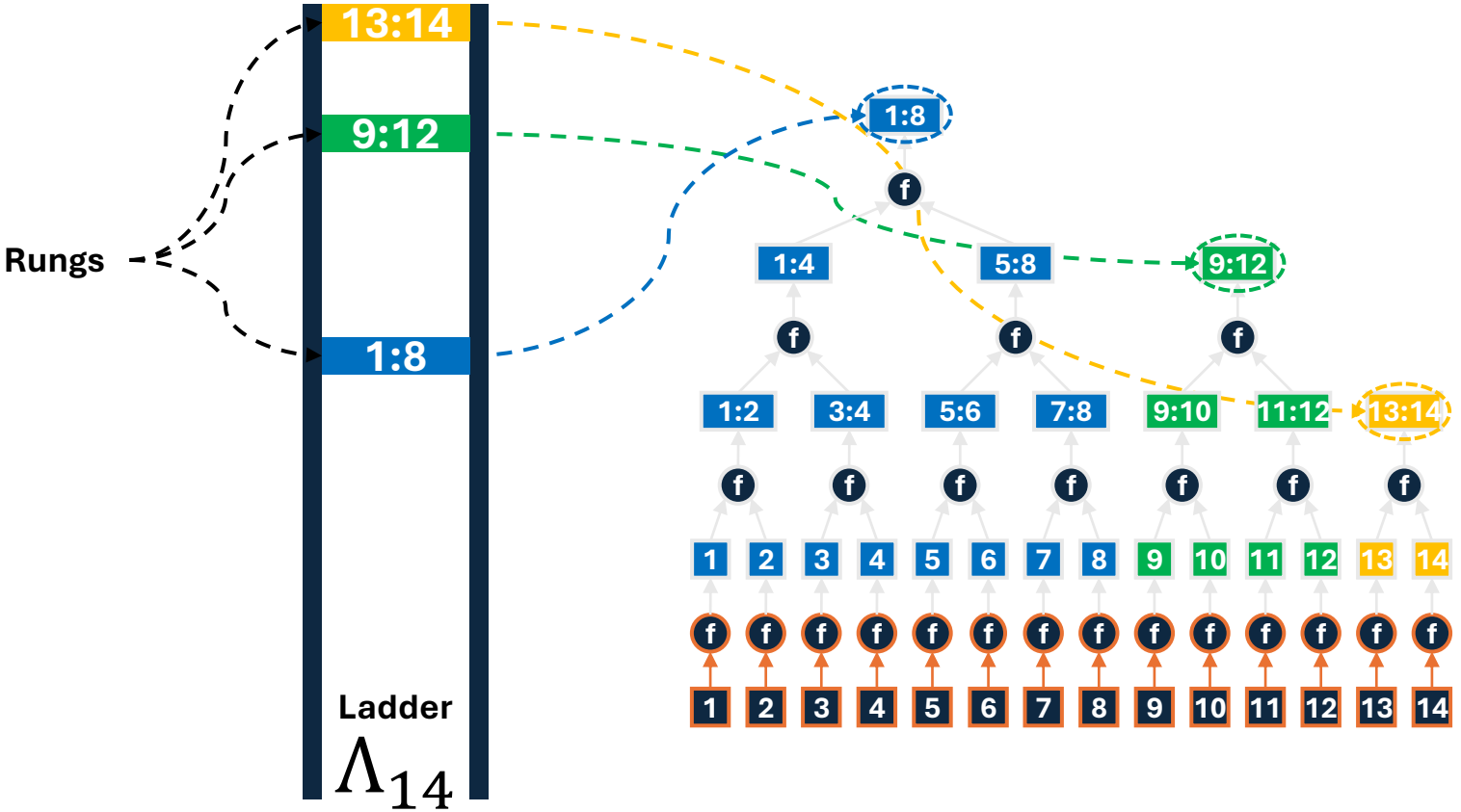
John Gray – John.Gray@entrust.com

Joe Harvey – jsharvey@verisign.com

Foundation

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 an evolving series of ladders
- Ladders provide backward compatibility since they can verify Merkle proofs for the same leaves constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time and over 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 the things to consider 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 public, royalty-free licenses 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

Application

Motivation for Exploring MTL mode

Post-quantum cryptographic signatures may have a significant operational impact in protocols that have a large number of signatures.

Examples:

- DNSSEC
- OCSP

MTL mode can help mitigate the operational impact in these use cases because verifiers are verifying signatures on a sub-set of a common message series.

Motivation for Status and Revocation with MTL Mode

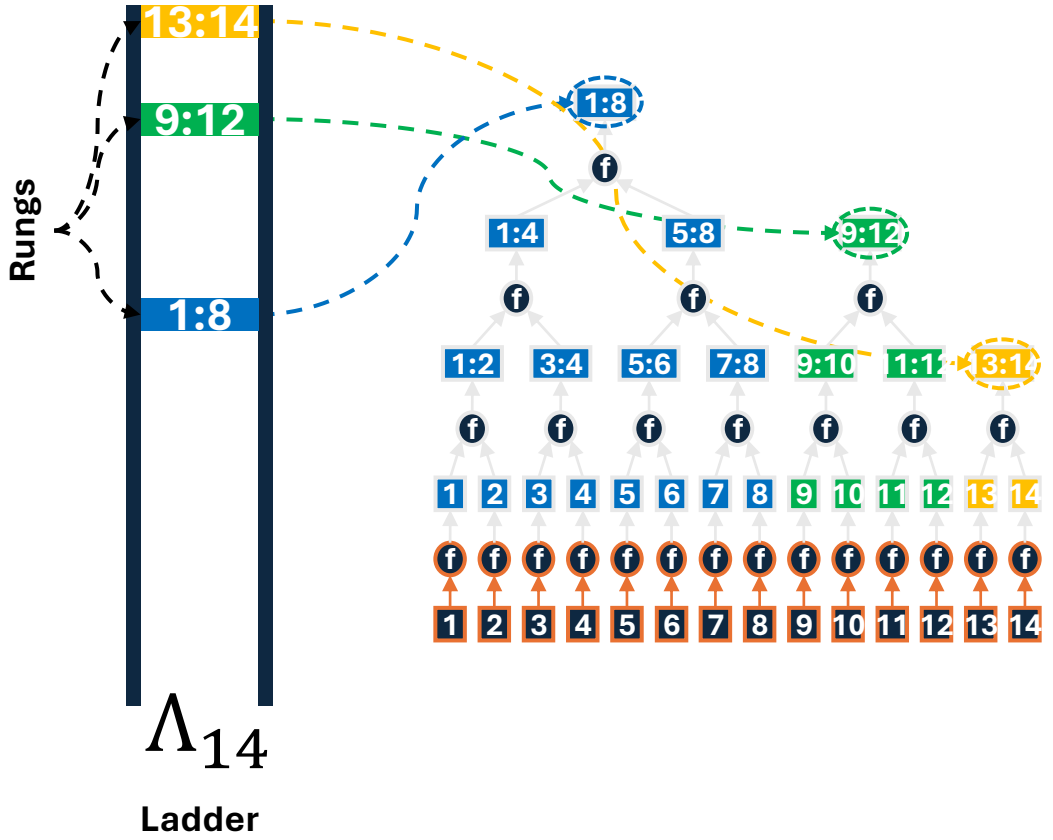
OCSP

• Replaces a list of revocations with individual OCSP status responses
• A signature is required for every response
  • Every certificate issued must have a corresponding revocation status
  • The revocation status of a particular certificate can change at any time
• Responders are basically big caches that periodically update responses (once a day, hour or x minutes)
  • Real-time responses can be enabled by use of a nonce but in practice it isn't used much

It is desirable to minimize the growth of the PQC signature size and resource consumption when adding PQC security to these protocols.

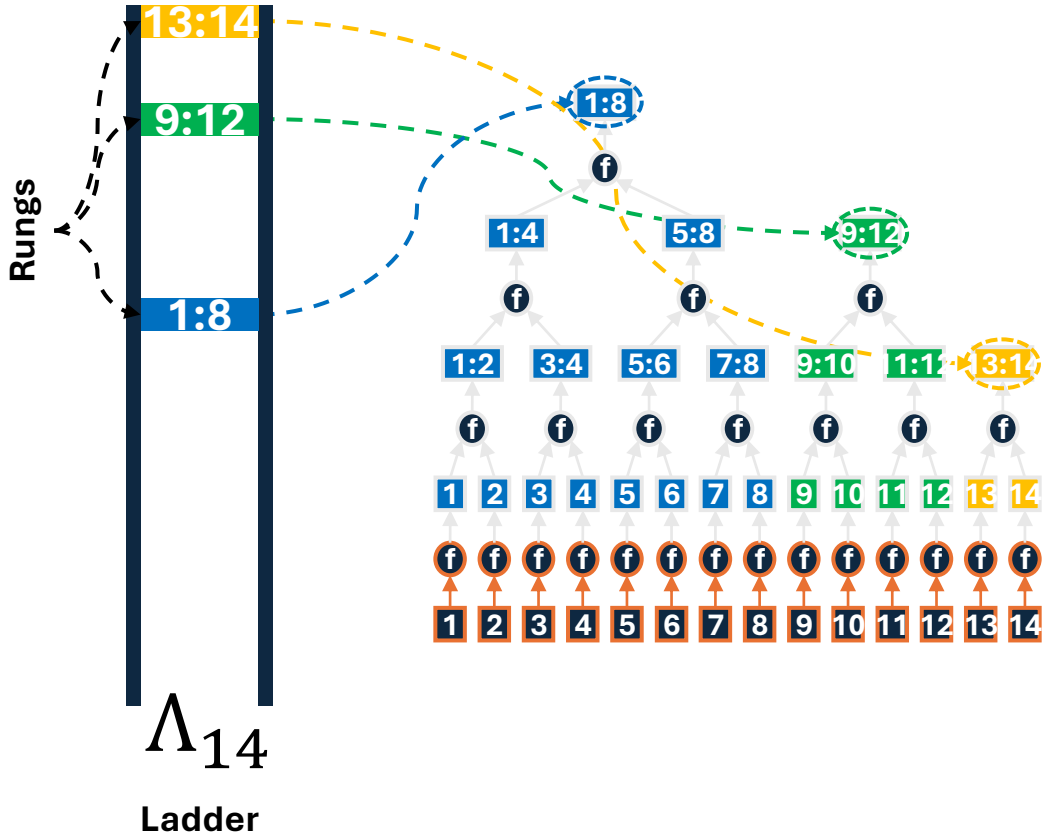
How Could It Work - OCSP?

- In MTL mode, Merkle trees are formed from a collection of data values to be signed
  - In OCSP each data value can be the hash of a to-be-signed OCSP response
- The signature has two forms, condensed and full
  - A condensed signature – the Merkle tree authentication path to one of the ladder rungs
  - A full signature - the condensed signature, the associated ladder, and a signature on the associated ladder



How Could It Work - OCSP?

- The ladder allows for validation of all of the leaf nodes in that series
- MTL parameters for each series are set up to a reasonable limit for entries in a PKI hierarchy (e.g., a few million at most)
- Adding more status responses (or resigning when the existing ones expire) just appends more leaf nodes to the tree



OCSP in MTL Mode vs Traditional OCSP

PROS

- Performance can benefit from pre-producing OCSP responses
- The cost for signing a message series with N messages goes from N signatures to B signatures + at most 2N-1 hashes where B is the number of batches
- Verification clients that verify a lot of certificates would see reduced bandwidth because one ladder covers many status responses
- Most of the time verification clients only have to verify a condensed signature
- Fetching the signed ladder may not compromise privacy since a ladder can cover many responses
  - Used with techniques like stapling for the condensed signatures can preserve privacy

More details on the considerations for MTL mode in OCSP:
https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode-considerations/

OCSP in MTL Mode vs Traditional OCSP

CONS

- Clients that infrequently perform revocation may have to download the signature on the ladder each time and won't see any improvement (and would have slightly larger data to download)
- Clients would need new logic to manage the ladders and signatures separately from the authentication paths

More details on the considerations for MTL mode in OCSP:
https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode-considerations/

Next Steps

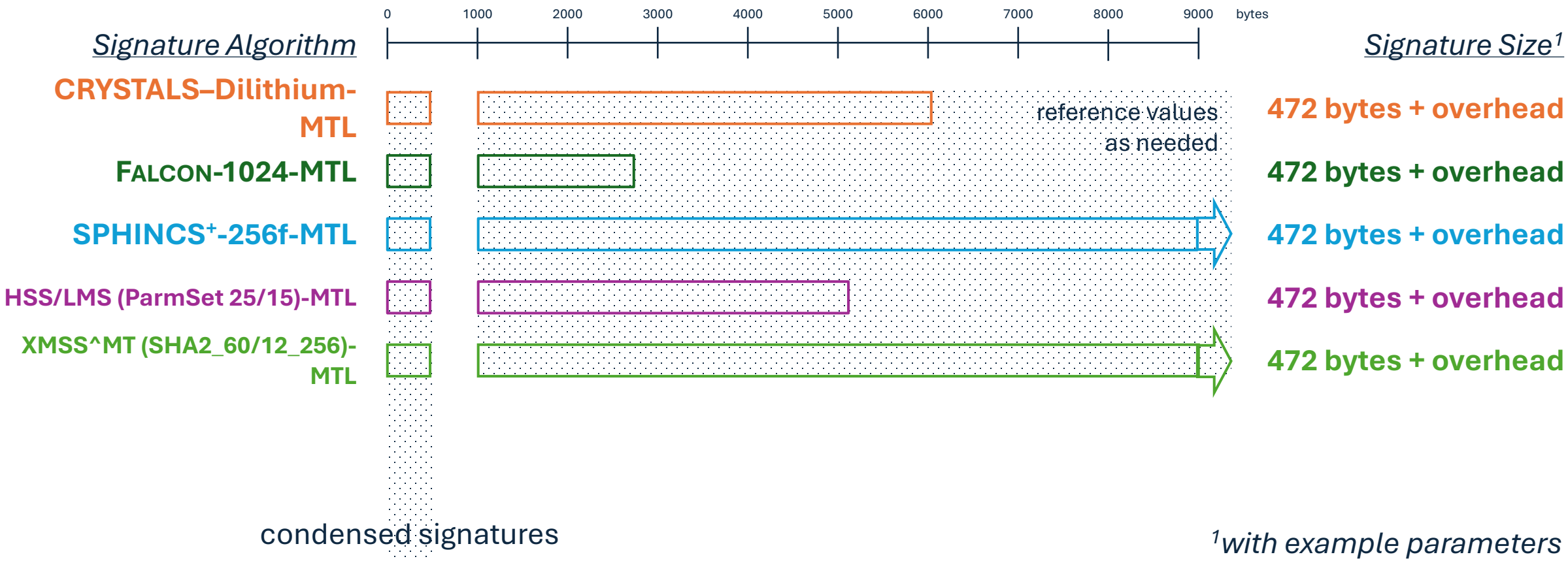
- Hackathon to prove out the concepts?
- An initial draft to describe the concept?

Thank You

Appendix

Reducing Effective Size Impact

Send Condensed Signatures, Look Up Reference Values



[1]*with example parameters*