

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

Joe Harvey

jsharvey@verisign.com

IETF-117

What is MTL Mode?

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

- MTL mode is a technique for using a signature scheme to authenticate an evolving series of messages
- Rather than signing individual messages, MTL mode signs Merkle Tree Ladders
- Ladder = subset of nodes or “rungs” in generalized Merkle tree construction (not just a single root)
- 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
- Signature on message can be just Merkle proof + reference to signed ladder
- MTL mode operations can be aligned with the underlying signature scheme to ensure proper cryptographic separation (I-D proposes alignment with SPHINCS+)
- Presented by Burt Kaliski (Verisign) at NIST 4th PQC Standardization Conference and CT-RSA 2023

Benefits of MTL Mode

- 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
- Merkle proofs are typically much shorter than PQC signatures → reduces size of messages that are transmitted across the wire or stored in memory/cache
- Batching can reduce the number of underlying signatures computed
- Hybrid signatures can be applied to ladders rather than individual messages

Outline of draft-harvey-cfrg-mtl-mode

1. Introduction Introduces MTL Mode.
2. Preliminaries Gives preliminaries including definitions, operators, functions and algorithm style.
3. General Model Presents the general model for authenticating messages in MTL mode.
4. Security Parameter, Cryptographic Functions, Address Scheme Introduces the security parameter, abstract cryptographic functions and address scheme used in the document, which are based on SPHINCS+.
5. Computing Data Values from Messages Shows how to compute data values for the Merkle node set from messages.
6. MTL Node Sets Describes the various concepts behind MTL mode operations including seeds and series identifiers, node sets, leaf nodes, internal nodes, ladders, authentication paths and backward compatibility.
7. Data Structures Defines the data structures for ladders, rungs and authentication paths.
8. MTL Node Set Operations Provides interoperable specifications for MTL node set operations.
9. Signing and Verifying Messages in MTL Mode Discusses how to sign and verify messages in MTL mode, including the concepts of "full" and "condensed" signatures.
10. SPHINCS+ in MTL Mode Proposes instantiations of SPHINCS+ in MTL mode using the SHAKE and SHA2 hash function families.
11. Related Work Discussion on related work.
12. IANA Considerations Comments on IANA considerations.
13. Security Considerations Covers the security considerations.
14. References Lists the references.

Intellectual Property

- Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Draft
- The license provides a “Standards Development Grant” for the purpose of facilitating standardization of the Internet-Draft
- IPR declarations 6072-6078 give the official language ([datatracker link](#))

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?).
- Pseudo-code for data structures and algorithms in current draft is runnable Python code (see Appendix A).
 - Test code (see Appendix B) shows examples of how to do operations like sign or verify a message.