Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice

Andrew Fregly[1,2], Joseph Harvey[1], Burton S. Kaliski Jr.[1] and Swapneel Sheth[1]

[1] Verisign Labs, Reston, VA 20190, USA
[2] afregly@verisign.com

Abstract. We introduce the *Merkle Tree Ladder (MTL) mode of operation* for signature schemes. MTL mode signs messages using an underlying signature scheme in such a way that the resulting signatures are *condensable*: a set of MTL mode signatures can be conveyed from a signer to a verifier in fewer bits than if the MTL mode signatures were sent individually.

In brief, MTL mode constructs an evolving sequence of Merkle tree nodes, which we call *ladders*, from the sequence of messages being signed, then signs each ladder using the underlying signature scheme. An MTL mode signature has three parts: an authentication path from a message to a Merkle tree ladder node or "rung"; the ladder; and the signature on the ladder. A *condensed signature* conveys the authentication path; a *reference value* conveys a ladder and its signature. The signer sends the verifier a condensed signature and a handle pointing to a reference value; the verifier computes a *reconstituted signature* from the condensed signature and a suitable reference value, requesting a new reference value if needed, and then verifies the reconstituted signature. The condensation process evolves the authentication paths to maximize reuse of ladders and therefore minimize their size impact.

We show that in a practical scenario involving random access to an initial series of 10,000 signatures that expands gradually over time, MTL mode can reduce the size impact of the NIST PQC signature algorithms, which have signature sizes of 666 to 7856 bytes with example parameter sets, to a condensed signature size of 472 bytes per message. Even adding the overhead of the reference values, MTL mode signatures still reduce the overall signature size impact under a range of operational assumptions. Because MTL mode itself is quantum-safe, the mode can support long-term cryptographic resiliency in applications where signature size impact is a concern without limiting cryptographic diversity only to algorithms whose signatures are naturally short.

Keywords: Post-Quantum Cryptography, Digital Signatures, Merkle Trees, Modes of Operation.