In SP 800-208, "**Recommendation** for Stateful Hash-Based Signature Schemes",

NIST has already specified two Post-Quantum resilient digital signature algorithms.

We do not see those in the Selected Algorithms.

So does it mean that NIST retracts her previous recommendation?

Uri Kaluzhny, PhD

Senior Security Architect

Winbond Israel

From:	Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To:	ukaluzhn@winbond.com
CC:	pqc-forum <pqc-forum@list.nist.gov>
Subject:	[pqc-forum] RE: Selected Algorithm 2022 OFFICIAL COMMENT: SPHINCS+
Date:	Thursday, July 07, 2022 01:52:45 PM ET
Attachments:	image001.jpg

Uri,

NIST has not retracted SP 800-208, "Recommendation for Stateful Hash-Based Signature Schemes," which specifies two stateful hash-based signatures as you noted. SP 800-208 is considered as a post-quantum cryptography standard, and the two algorithms XMSS and LMS are intended to provide resistance to attacks from quantum computers. However, stateful hash-based signature schemes are not suitable for general use because they require careful state management. As such, stateful hash-based signatures were not in the scope of the NIST Call for Proposals for the PQC Standardization Process. That is why you did not see them in the selected algorithms.

Dustin

From: ukaluzhn@winbond.com <ukaluzhn@winbond.com>
Sent: Thursday, July 7, 2022 8:38 AM
To: pqc-comments <pqc-comments@nist.gov>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Selected Algorithm 2022 OFFICIAL COMMENT: SPHINCS+

In SP 800-208, "**Recommendation** for Stateful Hash-Based Signature Schemes",

NIST has already specified two Post-Quantum resilient digital signature algorithms.

We do not see those in the Selected Algorithms.

So does it mean that NIST retracts her previous recommendation?

Uri Kaluzhny, PhD

Senior Security Architect

Winbond Israel