From: Moody, Dustin (Fed)
To: Moody, Dustin (Fed)
Subject: RE: Any approved hash function to substitute SHA-512 in EdDSA with 25519.
Date: Monday, November 27, 2017 1:58:43 PM

Qunhy also notes no key gen algorithm. And to allow other pre-hashes.

From: Dang, Quynh (Fed)
Sent: Wednesday, November 15, 2017 6:26 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Any approved hash function to substitute SHA-512 in EdDSA with 25519.

Right.

It would not make any implementations non-conformant if you decide to say that an approved hash function with at least 128-bit of security is required. From our perspective, I think we should not say SHAKE128/512 or SHAKE256/512 (output length: 512) or SHA-512 should be used.

Our hash policy does not prefer SHA2s over SHAKEs.

Quynh.

From: Moody, Dustin (Fed)
Sent: Wednesday, November 15, 2017 4:31:15 PM
To: Dang, Quynh (Fed)
Subject: Re: Any approved hash function to substitute SHA-512 in EdDSA with 25519.

Quynh,

Although SHA-512 isn't required in order for EdDSA to work, it is defined with SHA-512. That is, in order to be the same as existing implementations, then SHA-512 should be used. The RFC does define it more generally in terms of a hash function H, and then says for 25519 H is SHA-512 (as you know). I'll talk it over with Andy, Lily, and Scott at our next FIPS 186 meeting (on Monday).

On another note, the CFRG email said:

Transition from classical to Post-Quantum Cryptography, Paul Hoffman

(Last time Kenny spoke, Paul wasn?t present; this time Paul?s present and Kenny isn?t. Hmm)

Helping people who like to make predictions, make predictions

Proposed CFRG adoption. Consensus in room was strongly in favor, some need more info. To be confirmed on the list.

Q&A about num of qubits needed for 2K RSA, possibility of multiple smaller-sized machines, and practicality of using (much) larger curves with existing algorithms

Get your friends to help review and/or provide content!

Can you tell me more about this?

From: Dang, Quynh (Fed)
Sent: Wednesday, November 15, 2017 4:00:12 PM
To: Moody, Dustin (Fed)
Subject: Re: Any approved hash function to substitute SHA-512 in EdDSA with 25519.

A well known guy here: Robert Moskowitz is working on constrained crypto and he is promoting Keccak and 25519.

I read the CFRG RFC with Ed25519, it does not require SHA-512 to be the hash function H. H just needs to produce 512-bit outputs.

Quynh.

From: Moody, Dustin (Fed)
Sent: Wednesday, November 15, 2017 8:43:20 AM
To: Dang, Quynh (Fed)
Subject: Re: Any approved hash function to substitute SHA-512 in EdDSA with 25519.

Good to know. When you say "there is interest", who specifically do you mean?

From: Dang, Quynh (Fed)
Sent: Tuesday, November 14, 2017 8:35:54 PM
To: Moody, Dustin (Fed)
Subject: Any approved hash function to substitute SHA-512 in EdDSA with 25519.

Hi Dustin,

There is interest in using a SHA3 hash function (including a possible new one in the future) to substitute SHA-512 which is built in Ed25519.

A constrained environment using Keccak for all symmetric crypto functions would not be happy if SHA-512 is required for doing a digital signature function with curve 25519.

Quynh.