From: Moody, Dustin (Fed)
To: Davidson, Michael S. (Fed)
Subject: Re: Standard curves for Schnorr/EdDSA
Date: Friday, August 27, 2021 10:01:39 AM

Yes, DSA over finite fields is deprecated

From: Davidson, Michael S. (Fed) <michael.davidson@nist.gov>
Sent: Friday, August 27, 2021 10:01 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Standard curves for Schnorr/EdDSA

Thanks Dustin. And if I understand correctly, have we deprecated the use of discrete-log-based signatures in non-ECC fields?

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Friday, August 27, 2021 9:57 AM
To: Davidson, Michael S. (Fed) <michael.davidson@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Standard curves for Schnorr/EdDSA

Michael,

Here's a quick answer. Lily can add her thoughts.

I think you certainly could define Schnorr-type signatures over non-Edwards curves, but you are correct that this is not currently in FIPS 186-5 (or SP 800-186). We're on the verge of publishing the FIPS, so it won't be included in it for now. The only approved signatures over elliptic curves are ECDSA (including the deterministic version added in FIPS 186-5), and EdDSA for the two curves you noted.

One of the challenges is balancing standardizing new algorithms/curves with not having too many options for implementers to implement. With ECC, this has been an ongoing concern since NIST first standardized 15 curves for ECC.

In addition, we will likely soon be transitioning to new PQC signatures.

Dustin

From: Davidson, Michael S. (Fed) <michael.davidson@nist.gov>
Sent: Friday, August 27, 2021 9:51 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Standard curves for Schnorr/EdDSA

Hi guys,

I was wondering if we have standardized or plan to standardize Schnorr-type signatures over non-Edwards curves. I get the impression that we've only standardized EdDSA with ed25519 and ed448 curves, and while I have not fully read through FIPS 186-5 and SP 800-186, what I've seen so far is ambiguous.

FIPS 186-5 says: "The Edwards-curve Digital Signature Algorithm (EdDSA) is a digital signature scheme using a variant of a Schnorr signature based on twisted Edwards curves. See SP 800-186 for details on curves approved for use with EdDSA." The executive summary of SP 800-186 says: "Specification of new Montgomery and Edwards curves, which are detailed in Elliptic Curves for Security [RFC 7748]. These curves are only to be used with the EdDSA digital signature scheme in FIPS 186-5." Then, in section 3.1.3, it says: "An Edwards curve is a twisted Edwards curve with a=1. Edwards curves are to be used with the EdDSA digital signature scheme [FIPS 186-5]."

SP 800-186 does not appear to say that other curves are explicitly forbidden, though it seems implied.

I've also noticed that Ed25519 has a= -1, rather than a=1, so section 3.1.3 is inconsistent; this isn't an issue with Ed448.

In any case, I apologize if this is already well-known or has been documented already, but is there a reason to restrict the standard to these particular curves?

Thanks,
Michael