PROJECTS

Elliptic Curve Cryptography ECC

PROJECT LINKS

Overview
News & Updates
Events
Publications

Project Overview

Elliptic curve cryptography is critical to the adoption of strong cryptography as we migrate to higher security strengths. NIST has standardized elliptic curve cryptography for digital signature algorithms in FIPS 186 and for key establishment schemes in SP 800-56A.

In FIPS 186-4, NIST recommends fifteen elliptic curves of varying security levels for use in these elliptic curve cryptographic standards. However, more than fifteen years have passed since these curves were first developed, and the community now knows more about the security of elliptic curve cryptography and practical implementation issues. Advances within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim to offer better performance and are easier to implement in a secure manner. Some of these curves are under consideration in voluntary, consensus-based Standards Developing Organizations.

In 2015, NIST hosted a Workshop on Elliptic Curve Cryptography Standards to discuss possible approaches to promote the adoption of secure, interoperable and efficient elliptic curve mechanisms. Workshop participants expressed significant interest in the development, standardization and adoption of new elliptic curves. In 2015, NIST solicited comments on possible improvements to FIPS 186-4. In particular, comments were requested on the possibility of adding new elliptic curves to the current recommended set, as well as on digital signature schemes. Throughout 2016, NIST began resolving the comments received and revising FIPS 186-4.

October 31, 2019

A Federal Register Notice (FRN) announces a **Request for Comments on Draft FIPS 186-5 and Draft NIST Special Publication (SP) 800-186.** The public comment period is closed.

Draft FIPS 186-5, *Digital Signature Standard (DSS)*
Draft NIST SP 800-186, *Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters*

- **April 7, 2020: Comments received** are available for each publication by selecting the respective pub above.

CONTACTS

Dr. Lily Chen
lily.chen@nist.gov

Dr. Dustin Moody

GROUP

Cryptographic Technology

TOPICS