NIST Update: Elliptic Curves and More!

Andrew Regenscheid

Crypto Rump Session

August 19, 2014

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NIST Curves

- NIST-recommended curves specified in FIPS 186
- 10 of the curves are *pseudo-random* curves
  - Prime fields: $y^2 = x^3 - 3x + b$
  - Binary fields: $y^2 + xy = x^3 + x^2 + b$
- In general, a pseudorandom curve was chosen by:
  1) *Select a seed and hash it to generate the elliptic curve parameters*
  2) *Check if the curve has a large prime order subgroup such that the order satisfies certain conditions. If not, go to step 1 and repeat.*

  Note: Very likely need to choose many seeds

- The curves were generated by the NSA
- The seeds and curve parameters are published, but provenance not described

Current Understanding

- There are no known attacks of cryptographic significance on the NIST curves when implemented as described in our standards
- Lots of research in past 15 years on ECC
  - Newer curves proposed
    - Better performance
    - More resistance to side-channel attacks
- ECC critical for higher security strengths

Future Plans

- NIST seeks to promote adoption of secure, interoperable, and efficient elliptic curve cryptography

- NIST is re-examining its current ECC mechanisms
  - Will solicit comments on FIPS 186 and elliptic curves
  - We plan to host a workshop to discuss these issues

Comments

- We want to hear from you:
  - Concerns with NIST curves
  - Criteria to evaluate curves
  - Strategies to promote adoption of ECC
  - Deployment situation of the current curves
  - Approaches to resolve interoperability issues
  - Impacts to industry and users of any changes

- Send comments to: EllipticCurves@nist.gov

- Dustin Moody, ECC Lead, Dustin.Moody@nist.gov

NIST Publications

- **SHA-3**
  - Draft FIPS 202 comment period closes Aug. 26
  - Plans on authenticated encryption, message authentication, parallel hashing, and SHAKE functions to be discussed at SHA-3 workshop
- **Random Number Generation**
  - New draft of SP 800-90A expected soon
  - SP 800-90B/C on entropy sources and RBG constructions in development
- **Key Establishment**
  - SP 800-56B rev1 will be finalized soon

Available at: http://csrc.nist.gov/

Upcoming Workshops

- **SHA-3 2014 Workshop,** *Aug. 22. UCSB*
- **2nd Privacy Engineering Workshop**, *Sept. 15-16, San Jose, CA*
- **6th Cybersecurity Framework Workshop** *Oct. 29-30, Tampa, FL*
- **Workshop on Cybersecurity in a Post-Quantum World**, *April 2-3, NIST-Gaithersburg, MD*
  - Co-located with IACR's PKC 2015

Events: http://csrc.nist.gov/news_events/events.html