NIST Workshop on Elliptic Curve Cryptography Standards

June 11 – June 12, 2015

NIST solicits papers, presentations, case studies, panel proposals, and participation from any interested parties, including researchers, systems architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site and include these in a workshop handout. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. Topics for submissions should include, but are not limited to, the following:

Security of Elliptic Curves

- Are there any attacks of cryptographic significance that affect the claimed security of the NIST-recommended curves?
- Is there confidence in the security of the NIST-recommended curves?

Elliptic Curve Specifications and Criteria

- Is there a need for new elliptic curves to be considered for standardization?
- Which of the new elliptic curves that have been proposed in the literature or standards should NIST consider?
- What criteria should NIST use to evaluate any curves to be considered for inclusion?

Interoperability

- Which of the NIST-recommended curves have been used in practice?
- If new curves are to be standardized, what would be the impact of changing existing implementations to allow for the new curves?
- Does having a large number of recommended curves hinder interoperability?
- What are the advantages or disadvantages of allowing users/applications to generate their own elliptic curves, instead of using the NIST-recommended curves?

Performance

- Is the performance of existing implementations of elliptic curve cryptography inhibiting more widespread adoption?

Intellectual Property

- What are the desired intellectual property requirements for any new curves or schemes that could potentially be included in a standard?
- Are intellectual property requirements inhibiting more widespread adoption of elliptic curve cryptography?

Deadlines for submissions are:

- ***Papers, Presentations and Proposals Due: March 15, 2015***
- ***Authors Notified: April 10, 2015***

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). ***Paper submissions*** must not exceed 15 pages (single space, two column format with 1" margins using a 10 pt or larger font) and have no header or footer text (e.g., no page numbers). ***Proposals for presentations or panels*** should be no longer than five pages; panel proposals should include possible panelists and an indication of which panelists have confirmed participation.

Please submit the following information to EllipticCurves@nist.gov:

- Name, affiliation, email, phone, postal address for the primary contact author
- First name, last name, and affiliation of each co-author
- The finished paper, presentation or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.