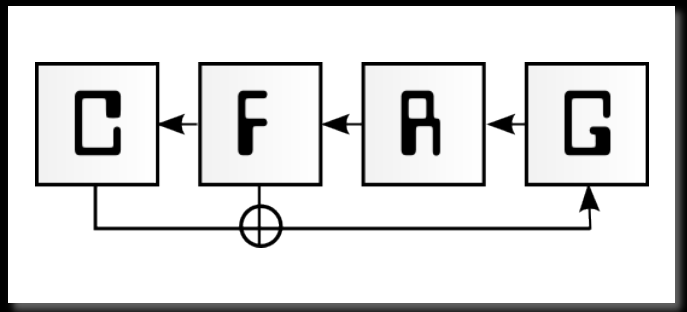


Internet Research Task Force
Crypto Forum Research Group
Interim Meeting on ECC

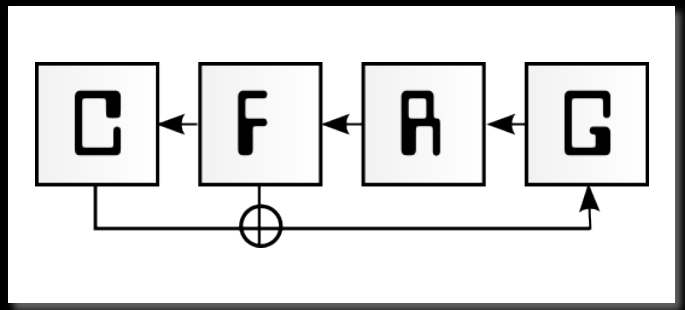
April 29, 2014

List: cfrg@irtf.org Chairs: mcgrew@cisco.com kmigoe@nsa.gov

https://datatracker.ietf.org/stream/irtf/

Internet Research Task Force

- Promotes research of importance to the evolution of the Internet by creating focused, long-term Research Groups
- Sister organization to the IETF



Crypto Forum Research Group

- Forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.
- Serves as a bridge between theory and practice, bringing new cryptographic techniques to the Internet community and promoting an understanding of the use and applicability of these mechanisms.

Note Well: IRTF IPR Disclosure Rules

- The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules. This is a summary of these rules as they relate to IRTF research group discussions, mailing lists and Internet Drafts:
  - If you include your own or your employer's IPR in a contribution to an IRTF research group, then you must file an IPR disclosure with the IETF.
  - If you recognize your own or your employer's IPR in someone else's contribution and you are participating in the discussions in the research group relating to that contribution, then you must file an IPR disclosure with the IETF. Even if you are not participating in the discussion, the IRTF still requests that you file an IPR disclosure with the IETF.
  - Finally, the IRTF requests that you file an IPR disclosure with the IETF if you recognize IPR owned by others in any IRTF contribution.
- The IRTF expects that you file IPR disclosures in a timely manner, i.e., in a period measured in days or weeks, not months. The IRTF prefers that the most liberal licensing terms possible are available for IRTF Stream documents, see RFC 5743. You may file an IPR disclosure here: http://www.ietf.org/ipr/file-disclosure
- See RFC 3979 (BCP 79) for definitions of "IPR" and "contribution" and for the detailed rules (substituting "IRTF" for "IETF").

Agenda

3:00 David McGrew: *Current ECC standards and problem statement*

3:15 Rene Struik: *Fixing the EC-DRBG*

3:35 Dan Brown: *Random curves: security benefits, generation methods, and Cheon attacks*

3:45 Watson Ladd: *On the security of twisted Edwards Curves*

4:05 Patrick Longa: *Selecting Elliptic Curves for Cryptography*

4:50 Discussion

1. What curves and algorithms are safe to use on the Internet?
2. What curves and algorithms are desirable to use in Internet protocols, considering criteria beyond just security, such implementation costs and interoperability?

5:30 Wrap up

CURRENT ECC STANDARDS AND PROBLEM STATEMENT

ECC on the Internet

- TLS
  - *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS),* RFC4492
    - 7% support on Internet
  - *Fundamental Algorithms of Elliptic Curve Cryptography,* RFC6090
  - *Curve25519 for ephemeral key exchange in Transport Layer Security (TLS),* draft-josefsson-tls-curve25519-05
- SSH
  - *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer,* RFC5656
    - 10% support on Internet
  - *Using ED25519 in SSHFP Resource Records,* draft-moonesamy-sshfp-ed25519-00

Bos et. al. Elliptic Curve Cryptography in Practice, 2013

Criteria for new ECC mechanisms

Simplicity

- R1. Desired: easy to understand and implement [1]

Efficiency

- R2. Required: amenable to compact implementations and fast implementations, across both small and large processors [1]
- R3. Desired: re-use components between signatures and key exchange algorithms [3]

Intellectual Property

- R4. Required: available worldwide under reasonable and well understood licensing terms [1]
- R5. Desired: available worldwide under royalty-free licensing terms [1]

Interoperability

- R6. Desired: can be used with current software implementations (using different curve parameters) of TLS, PKIX, SSH, and IKE [4]
- R7. Desired: can be used within current ECC standards of TLS, PKIX, SSH, and IKE[4]

Criteria for new ECC mechanisms

Security

- R8. Required: amenable to constant-time implementations, to avoid side channel attacks [2]
- R9. Required: resist twist attacks [2]
- R10. Required: curve parameters should have good provenance; random curves should be provably pseudorandom [5]
- R11. Desired for key exchange: resist invalid curve attacks [2]; note that complete addition laws help and are thus desirable [2]. (Note that the use of ephemeral keys also resist such attacks.)
- R12. Required for PAKE: indistinguishability of curve points from random strings [2]

Footnotes

[1] Original criteria set out for the Advanced Encryption Standard, which is equally applicable to ECC. National Institute of Standards and Technology (NIST) of the United States, 1998

[2] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. http://safecurves.cr.yp.to, accessed April 2014

[3] Criteria identified by David McGrew, 2014

[4] Criteria identified by Russ Housley, TLS WG meeting at IETF89

[5] Criteria widely acknowledged on CFRG email list during 2014

Discussion

1. What curves and algorithms are safe to use on the Internet?
2. What curves and algorithms are desirable to use in Internet protocols, considering criteria beyond just security, such implementation costs and interoperability?