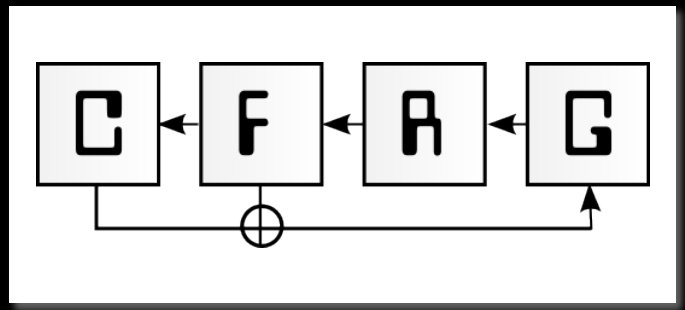


Internet Research Task Force
Crypto Forum Research Group
IETF 89

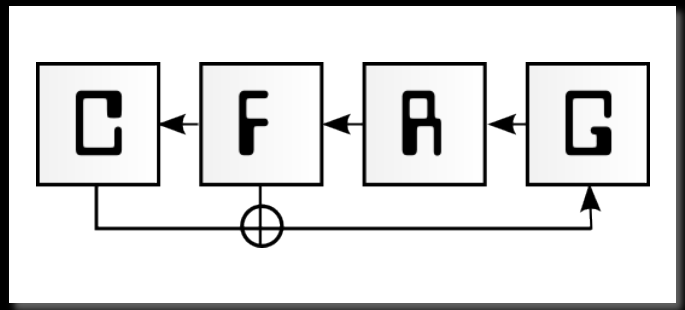
March 3, 2014 London

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

- Agenda Bashing (5 min)
- Document Status (10 min)
- Password Authenticated Key Exchange
  - Presentation on AugPAKE seonghan.shin@aist.go.jp (25 min)
  - DragonFly quick status update
- New Authenticated Encryption Mechanisms
  - Presentation and DISCUSSION on ChaCha+Poly1305 - ynir@checkpoint.com (25 min)
  - Presentation on Authenticated Encryption using Replay Protection (AERO) draft-mcgrew-srtp-aero-01 mcgrew@cisco.com (25 min)
- New Elliptic Curve Crypto
  - Status and DISCUSSION of non-standard curves (15 min)
- Consideration of new topics (15 min)

Status of Documents

- RFCs published: OCB
- CFRG drafts
  - draft-irtf-cfrg-augpake-01, *Augmented Password-Authenticated Key Exchange (AugPAKE)*
  - draft-irtf-cfrg-dragonfly-03, *Dragonfly Key Exchange*
  - draft-irtf-cfrg-zss-02, *ZSS Short Signature Scheme for Supersingular and BN Curves*
  - draft-irtf-cfrg-zssbn-01, *ZSS Short Signature Scheme for BN Curves*
  - draft-irtf-cfrg-cipher-catalog-01, *Ciphers in Use in the Internet*

Review Requested by IETF

- draft-nir-cfrg-chacha20-poly1305-01, *ChaCha20 and Poly1305 for IETF protocols*
- draft-shen-sm2-ecdsa-02, *SM2 Digital Signature Algorithm*
- draft-shen-sm3-hash-01, *SM3 Hash Function*

Other drafts of interest to the RG

- draft-ladd-safecurves-03, *Additional Elliptic Curves for IETF protocols*
- draft-mcgrew-aero-01, *Authenticated Encryption with Replay prOtection (AERO)*
- draft-urien-cfrg-cose-00, *Cloud of Secure Elements(CoSE*)

Password Authenticated Key Exchange

- Presentation on AugPAKE
  - seonghan.shin@aist.go.jp
- DragonFly quick status update
- QUESTIONS:
  - Would you support additional work on PAKE?
  - What does password-based security mean?
  - Usage and applicability?

New Auth Enc Mechanisms

- Presentation on ChaCha+Poly1305
  - ynir@checkpoint.com
- DISCUSSION: feedback on ChaCha+Poly1305 requested by TLS WG
  - QUESTION: do you think this function is adequately secure to be used in TLS ciphersuites?
- Presentation on Authenticated Encryption using Replay Protection (AERO) draft-mcgrew-srtp-aero-01
  - mcgrew@cisco.com

New Elliptic Curve Crypto

- Status of non-standard curves
  - DISCUSSION: feedback on non-standard curves requested by TLS WG
  - QUESTIONS:
    - How many have reviewed safecurves draft?
    - How many have reviewed Curve25519?
    - What constitutes proper documentation?
    - Do you think Curve25519 is secure enough to be included in TLS ciphersuites?
    - Interim meeting?

Consideration of New Topics

- Post-quantum crypto?
  - draft-mcgrew-hash-sigs-01
  - Do we have expertise in quantum cryptanalysis?
- Key-centric architectures?
  - IETF 90 paul@marvell.com
- STRINT (Strengthening the Internet) topics?
- Documenting security models used in security proofs?
- Proofs of correctness and simple protocols?
- Other?