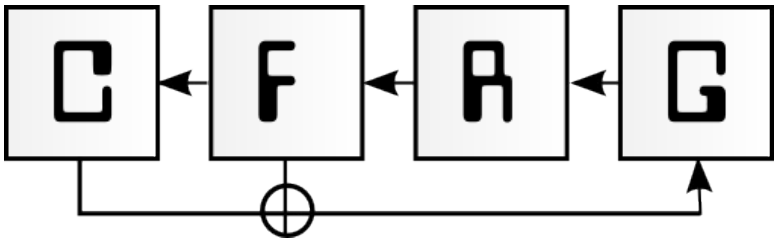
Internet Research Task Force
Crypto Forum Research Group

IETF 87 Berlin
July 29, 2013



Agenda

- **Agenda Bashing**
- **Note Well**
- **Randomized Hashing** (NIST SP-800-106/107) - **Dang**
- **Quick updates on active drafts**
  - OCB Mode of Operation, `draft-irtf-cfrg-ocb-03`
  - Dragonfly Key Exchange, `draft-irtf-cfrg-dragonfly-01`
  - Hash-Based Signatures, `draft-mcgrew-hash-sigs-00`
  - Ciphers in Use in the Internet `draft-irtf-cfrg-cipher-catalog-01`
- **SM2 Digital Signature Algorithm**, `draft-shen-sm2-ecdsa-01` – **Shen**, Lee
- **Selection of Future Cryptographic Standards**, `draft-mcgrew-standby-cipher-00` – **McGrew**, Sheffer, Grieco
- **Discussion on other crypto work**
  - DTLS In Constrained Environments (DICE) BoF
  - Salsa20
  - CAESER

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
  - Any IETF working group or portion thereof
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.
- Please consult RFC 5378 and RFC 3979 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Discussion: Other Crypto Work

- DTLS In Constrained Environments (DICE) BoF
  - http://datatracker.ietf.org/wg/dice/charter/
- Salsa20
  - `draft-josefsson-salsa20-tls-01`
- CAESER
  - http://competitions.cr.yp.to/caesar.html
  - Directions in Authenticated Ciphers (DIACs), August 11–13, 2013 Chicago, USA
- Others