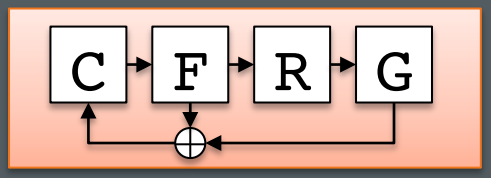


Crypto Forum Research Group

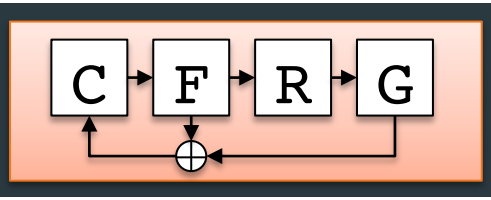
Kenny Paterson

Information Security Group

@kennyog; www.isg.rhul.ac.uk/~kp

ROYAL HOLLOWAY UNIVERSITY OF LONDON

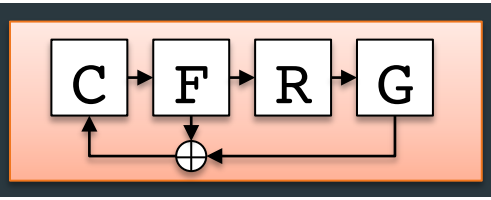
CFRG Charter



The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.

The CFRG 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 via Informational RFCs.

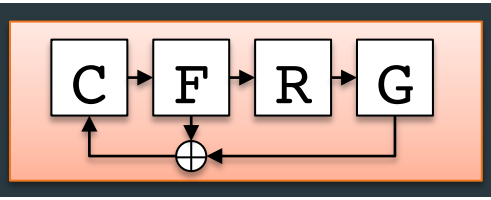
CFRG Charter (continued)



Our goal is to provide a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the use of emerging mechanisms and new uses of existing mechanisms.

IETF working groups developing protocols that include cryptographic elements are welcome to bring questions concerning the protocols to the CFRG for advice.

CFRG Processes



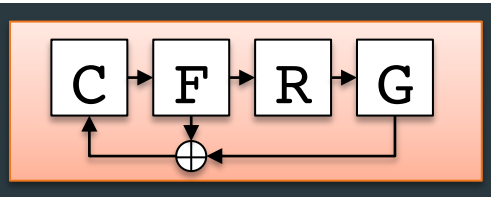
ID (Internet Draft): a raw text document describing an algorithm, protocol or idea.

CFRG process

RFC (Request for Comments): *de facto* an Internet standard*.

Main CFRG objective: turn useful-looking IDs into complete, clear, well-specified RFCs by tapping into expertise of the community.

CFRG Chairs and Their Roles



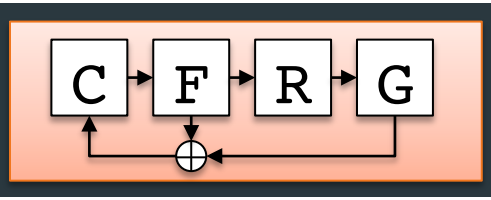
Current chairs of CFRG:

- **Alexey Melnikov**
- **Kenny Paterson**

Role of chairs:

- Ideally processes are consensus-based, and the chairs' job is to guide group towards consensus.
- In IETF, achieving at least rough consensus is required.
- In IRTF, rough consensus is preferred but not required and decision-making ultimately resides with the chairs.

CFRG Resources

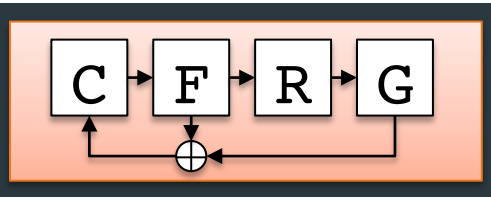


- CFRG is resource-limited and the problem of "making crypto for the Internet" is large and complicated.
- The work is volunteer-driven.
- Cf. dedicated staff running NIST AES and SHA-3 competitions.

- CFRG review panel: a circle of experts who can be called upon to review drafts and make recommendations.

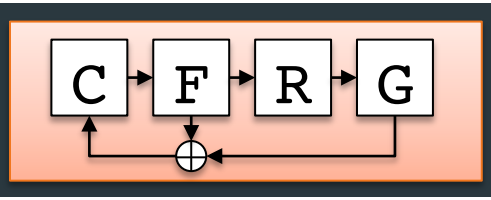
Scott Fluhrer	Yaron Sheffer
Pierre-Alain Fouque	Stanislav Smyshlyaev
Russ Housley	Bjoern Tackmann
Tibor Jager	

Current CFRG Work



- **Requirements for PAKE protocols**: published as RFC 8125, April 2017.
- **Hash-based signatures**: draft-irtf-cfrg-xmss-hash-based-signatures-09 – last call completed, with IRTF chair for publication.
- **ChaCha20 and Poly1305 for IETF Protocols**: draft-nir-cfrg-rfc7539bis-01 –at last call.
- **AES-GCM-SIV**: draft-irtf-cfrg-gcmsiv-04 – needs further review.
- **Password hashing; adoption of Argon 2:** draft-irtf-cfrg-argon2-02 – under discussion today.
- **Re-keying Mechanisms for Symmetric Keys**: draft-irtf-cfrg-re-keying-01 – discussed extensively at IETF in Chicago.
- All drafts at: https://datatracker.ietf.org/rg/cfrg/documents/

Agenda



16:00 CFRG status update from CFRG chairs (10 mins; Kenny Paterson)

16:10 Argon 2 update https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/ (15+10 mins; Dmitry Khovratovich)

16:35 PKEX: A Password-Authenticated Public Key Exchange

https://datatracker.ietf.org/doc/draft-harkins-pkex/ (10+5 mins; Dan Harkins)

16:50 Caesar's Role in the Fall of AE Security (15+10 mins; Pooya Farshim)

17:15 BIP32-Ed25519 (15+10 mins; Dmitry Khovratovich)

17:40 Evaluation of secp256k1 as popular alternative curve (5+5 mins; Christopher Allen)

17:50 Ephemeral Diffie-Hellman Over COSE (EDHOC): https://tools.ietf.org/html/draft-selander-ace-cose-ecdhe-06 (5 mins; Göran Selander/Jim Schaad)

17:55 Open discussion

18:00 Finish