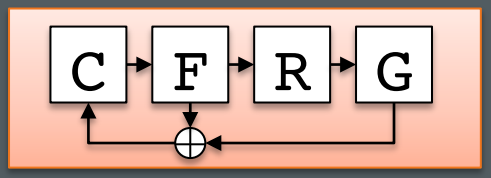


Crypto Forum Research Group @EUROCRYPT 2016

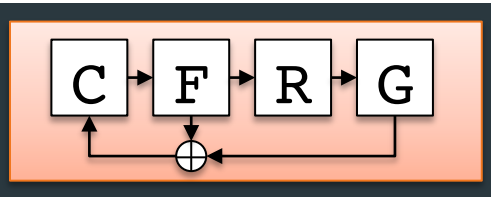
Kenny Paterson

Information Security Group

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

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda



13:30 - Chairs' welcome and document status update (10 mins)

13:40 - Shay Gueron/Adam Langley/Yehuda Lindell (30 mins + 10 mins discussion): AES-GCM-SIV
https://tools.ietf.org/html/draft-irtf-cfrg-gcmsiv-01

14:20 - Joel Alwen (30 mins + 10 mins discussion): Memory-Hard Functions

https://www.ietf.org/proceedings/interim/2016/05/12/cfrg/slides/slides-interim-2016-cfrg-1-1.pdf

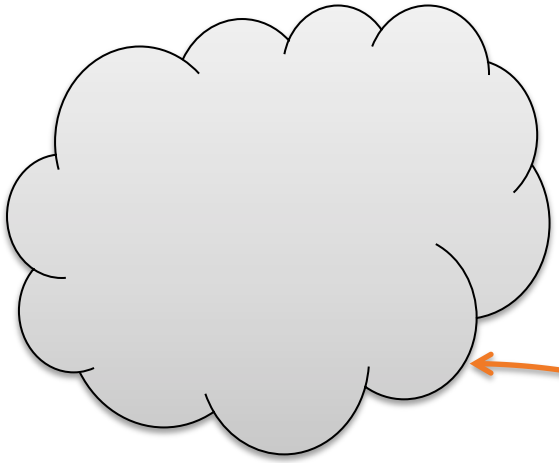
15:00 - Andreas Huelsing (10 mins update + 10 mins disucssion) XMSS: Extended Hash-Based Signatures

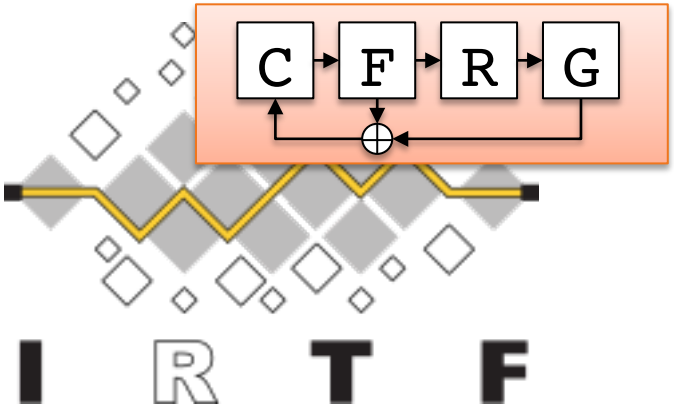
https://www.ietf.org/id/draft-irtf-cfrg-xmss-hash-based-signatures-03.txt

15:20 - AOB (10 mins)

15:30 - Meeting ends

Introducing IETF/IRTF/CFRG

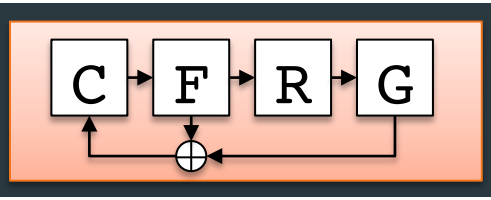




Objective:

make this work!

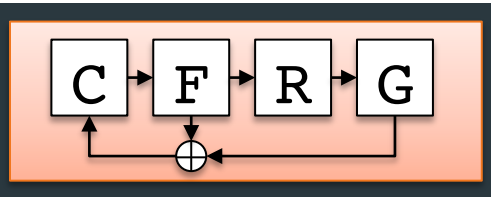
CFRG Charter (extract)



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.

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.

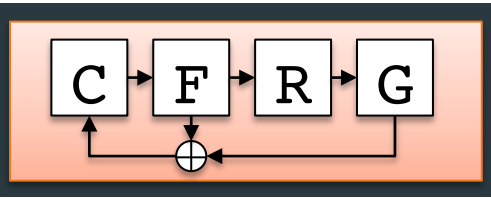
This Meeting



- CFRG normally meets physically at IETF meetings, held three times per year (see ietf.org for schedule).
  - Much work is also carried out on the CFRG mailing list.
- This is formally an *interim* meeting.
- It is an experiment, designed to increase academic engagement in CFRG.

- Please "sign in" on the circulating sheet – name and organisation only.

Document Status



- All documents at: https://datatracker.ietf.org/rg/cfrg/documents/

- A selection of active drafts adopted by CFRG:

  draft-irtf-cfrg-gcmsiv-01 – AES-GCM-SIV

  draft-irtf-cfrg-eddsa-05 - EdDSA signature scheme

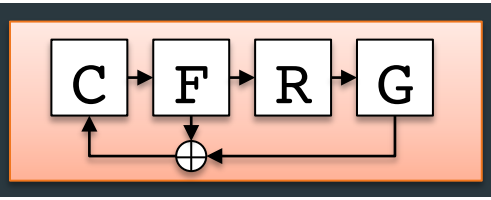
  draft-irtf-cfrg-pake-reqs-03 – PAKE requirements document

  draft-irtf-cfrg-xmss-hash-based-signatures-03 – Hash based signatures

- Recently published:

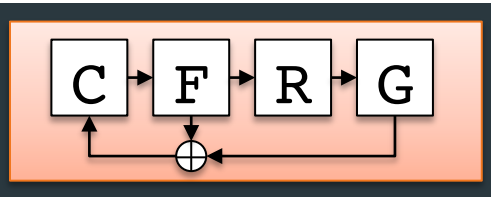
  RFC 7748 (was draft-irtf-cfrg-curves) - Elliptic Curves for Security

CFRG Review Panel



- Proposal from the CFRG chairs, intended to supplement normal CFRG processes with more formal reviews of documents.
- Idea under discussion on CFRG mailing list.
- Expected workload: review one or two documents per year, produce short report with recommendations.
- Chairs now looking for volunteers/nominations to join the panel.
- Talk to me if you are interested.

Agenda



13:30 - Chairs' welcome and document status update (10 mins)

13:40 - **Shay Gueron**/Adam Langley/Yehuda Lindell (30 mins + 10 mins discussion): AES-GCM-SIV
https://tools.ietf.org/html/draft-irtf-cfrg-gcmsiv-01

14:20 - Joel Alwen (30 mins + 10 mins discussion): Memory-Hard Functions

https://www.ietf.org/proceedings/interim/2016/05/12/cfrg/slides/slides-interim-2016-cfrg-1-1.pdf

15:00 - Andreas Huelsing (10 mins update + 10 mins disucssion) XMSS: Extended Hash-Based Signatures

https://www.ietf.org/id/draft-irtf-cfrg-xmss-hash-based-signatures-03.txt

15:20 - AOB (10 mins)

15:30 - Meeting ends