CFRG

Crypto Forum Research Group

Kenny Paterson

Information Security Group

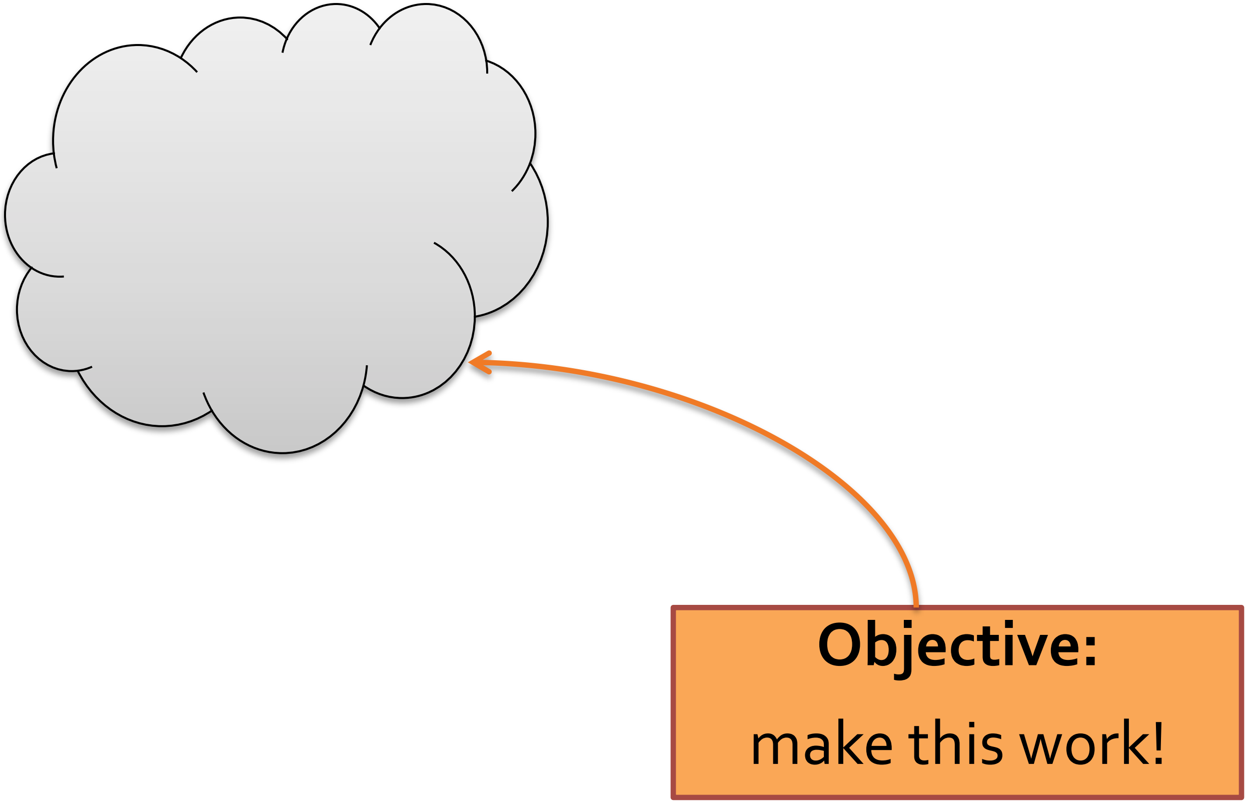
@kennyog; www.isg.rhul.ac.uk/~kp

ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

Overview

- IETF/IRTF
- CFRG charter
- CFRG processes
- Current work
- Getting involved

IETF/IRTF



Objective:

make this work!

IETF and IRTF

IETF: focus on engineering, standardisation of better protocols and new features.

IRTF: research-oriented, longer-term perspective.

IRTF is organised into Research Groups (RGs).

CFRG is the **Crypto Forum** Research Group.

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.

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.

CFRG Charter (continued)

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

Sometimes this does happen (but not always).

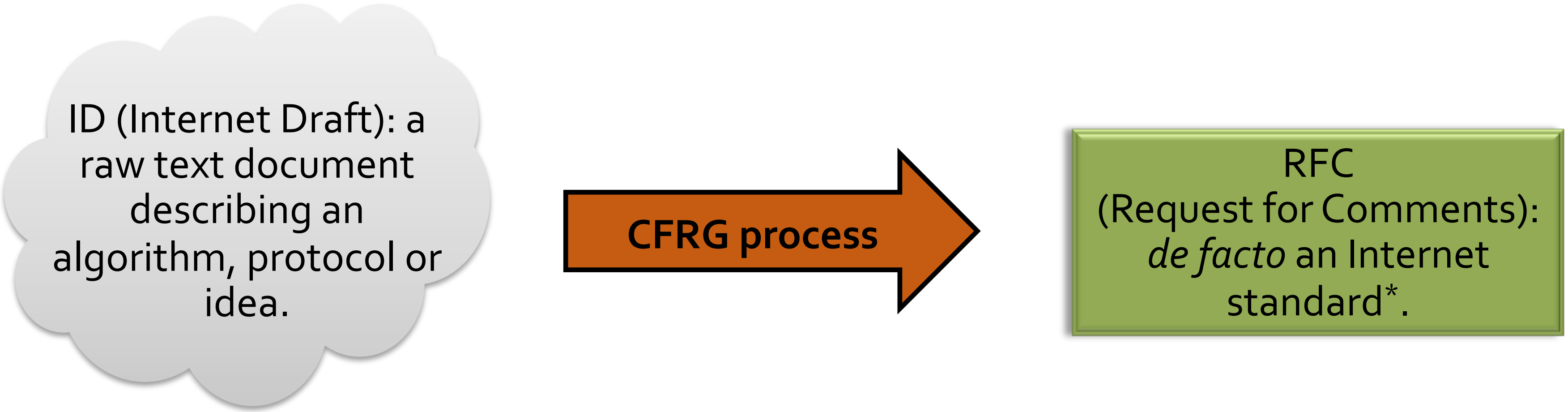
This makes CFRG a bit different from other RGs.

Recent example:

TLS Working Group request for new elliptic curves and associated algorithms for Diffie-Hellman and digital signatures.

In other cases, people doing crypto or needing crypto review/advice are steered towards CFRG by IETF leadership.

CFRG Processes



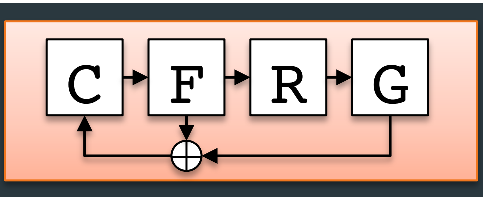
ID (Internet Draft): a raw text document describing an algorithm, protocol or idea.

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 Processes



- ID may be adopted by CFRG to become a CFRG draft after call for adoption issued by chairs.
- CFRG chairs manage the process and, with help of ID's editors/ authors, build consensus for contents of drafts.
- IDs evolve through different versions in response to feedback on CFRG mailing list and at CFRG meetings.
- Eventually, ID may become an Informational RFC.
- Typical time-line: 6 months to 1 year.
- NB: RFC does not mean wide-spread adoption on the Internet!

CFRG Chairs and Their Roles

Current chairs of CFRG:

- **Alexey Melnikov**: IETF lifer, huge experience in IETF processes, writing RFCs, running IETF WGs.

- **Kenny Paterson**: cryptographer, still learning the process ropes.

Role of chairs:

- Ideally processes are consensus- based, and 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.

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

Why Get Involved?

Benefits:

- Help make the Internet more secure, by helping move interesting and useful crypto from theory to practice.
- Demonstrate the impact of your research.
- Learn something about how and why crypto is hard in the real-world.
- Make a difference in the world.

Disbenefits:

- Various "colourful characters from the Internet" are also passionately involved (cf. Phil's talk).
- You might need to repeatedly explain things you take for granted to people who don't know as much crypto as you (but who know a lot about the Internet).
- You are not spending time writing your next research paper.

Current CFRG Work

Building a portfolio of useful primitives:

- New curves, along with ECDH and EC-based signature schemes for TLS 1.3.
- Hash-based signatures.
- AES-GCM-SIV.
- Password hashing: adoption of Argon 2 (PHC winner).
- Requirements for PAKE protocols, leading to call for PAKE proposals.

Figuring out what to do more generally in the post-quantum arena.

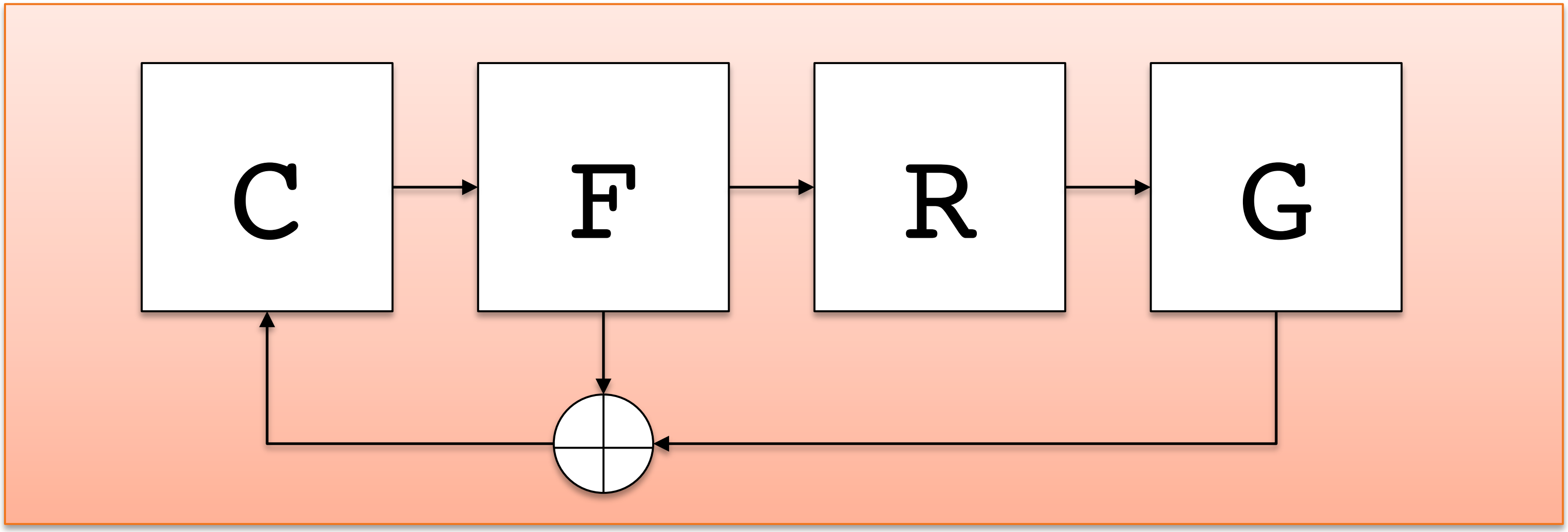
How to Get Involved

- CFRG is meeting this Thursday 13:30 – 15:30 in the main hall.
  - Presentations and discussions on memory-hard functions for password hashing, AES-GCM-SIV, hash-based signatures and more.
- Next CFRG meeting: IETF Berlin, July 2016

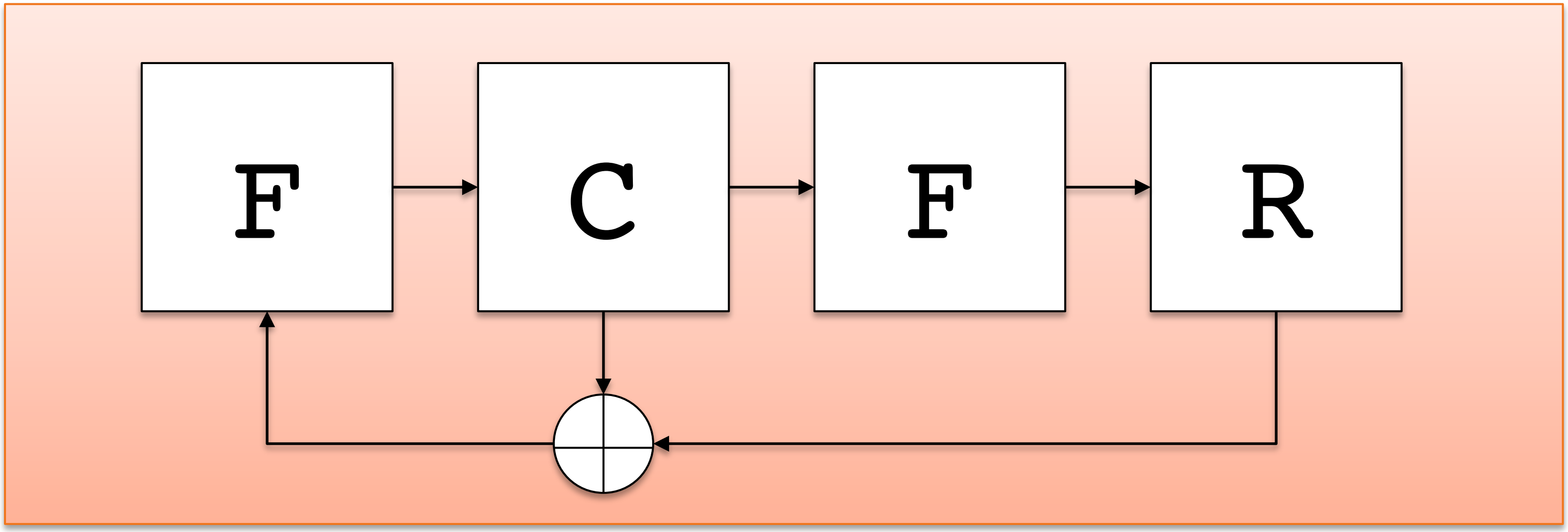
  http://www.ietf.org/
- Have a dig around in the mail archive:

  http://www.ietf.org/mail-archive/web/cfrg/
- Then subscribe to the CFRG mailing list.
- AMA.

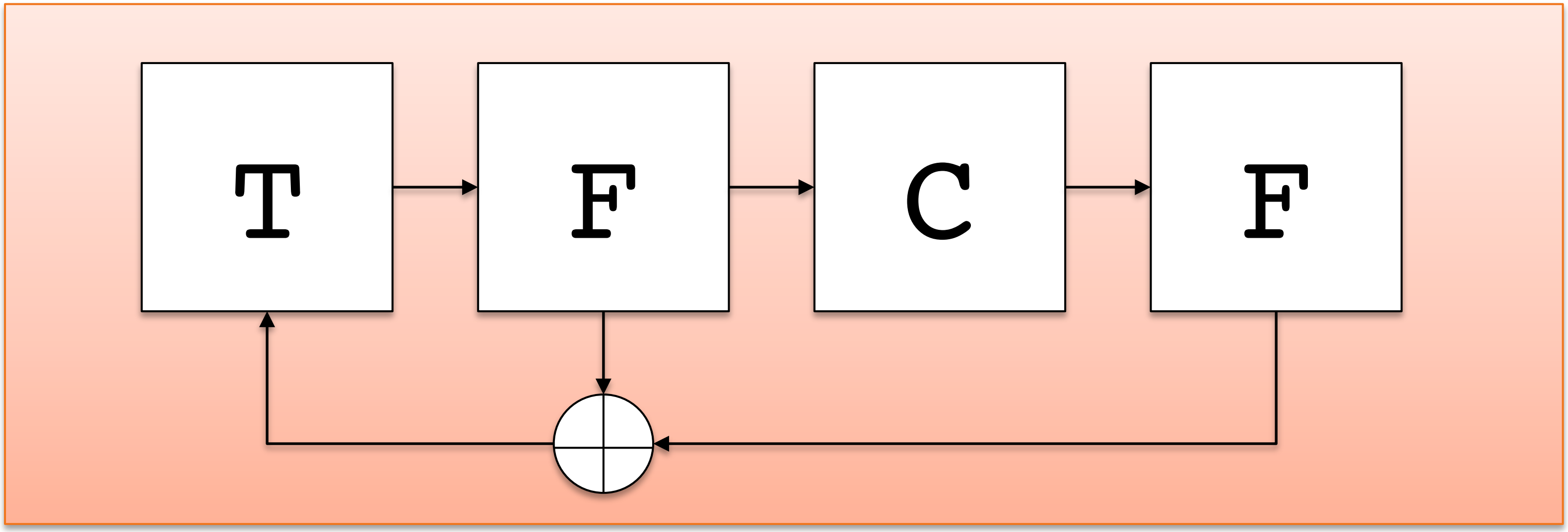
Thanks/Danke/Merci



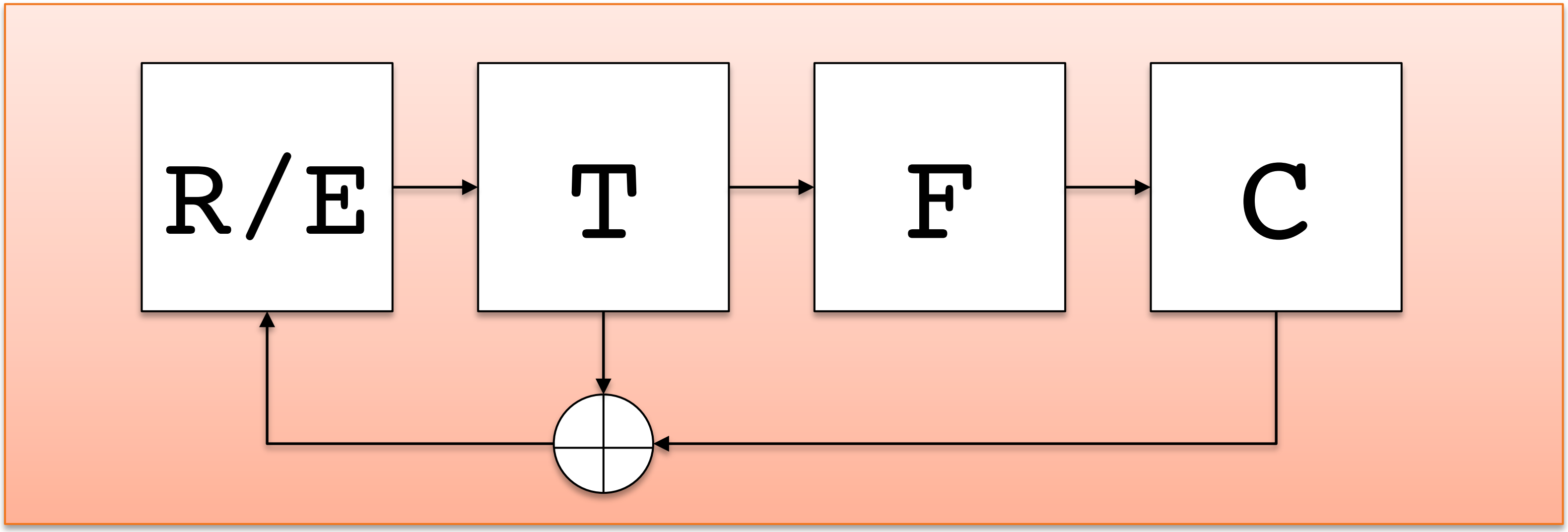
Thanks/Danke/Merci



Thanks/Danke/Merci



Thanks/Danke/Merci



Thanks/Danke/Merci