CFRG Research Group

Online Agenda and Slides at:

Data tracker:
http://datatracker.ietf.org/rg/cfrg/documents/
Agenda

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

❖ By participating with the IETF, you agree to follow IETF processes.

❖ If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.

❖ You understand that meetings might be recorded, broadcast, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)
BCP 25 (on the Working Group processes)
BCP 78 (on the IETF Trust)
BCP 79 (on Intellectual Property Rights in the IETF)

Also see: [http://www.ietf.org/about/note-well.html](http://www.ietf.org/about/note-well.html)
Administrative

• Audio Streaming/Recording
  – Please speak only using the microphones
  – Please state your name before speaking

• Minute takers & Etherpad
• Jabber
CFRG Research Group
Status

Chairs:
Kenny Paterson <kenny.paterson@rhul.ac.uk>
Alexey Melnikov <alexey.melnikov@isode.com>
RG Document Status
Document Status

• New RFC (since Prague)
  • None
• In RFC Editor's queue (since Singapore)
  • draft-irtf-cfrg-xmss-hash-based-signatures-10: XMSS: Extended Hash-Based Signatures
• In IRSG review
  • draft-nir-cfrg-rfc7539bis-02 (IESG conflict review): ChaCha20 and Poly1305 for IETF Protocols
• Completed, waiting for chairs
  • draft-mcgrew-hash-sigs-10 (updated, ready for IRSG): Hash-Based Signatures
  • draft-irtf-cfrg-argon2-03 (ready for IRSG): memory-hard Argon2 password hash and proof-of-work function
  • draft-irtf-gcmsiv-08 (updated, ready for IRSG): AES-GCM-SIV: nonce misuse-resistant authenticated encryption
  • draft-irtf-cfrg-re-keying-12 (updated, ready for IRSG): Re-keying Mechanisms for Symmetric Keys
• Active CFRG drafts
  • draft-irtf-cfrg-vrf-01 (new): Verifiable Random Functions (VRFs)
  • draft-irtf-cfrg-spake2-05 (updated): SPAKE2, a PAKE
  • draft-irtf-cfrg-augpake-09 (updated): Augmented Password-Authenticated Key Exchange (AugPAKE)
  • draft-hoffman-c2pq-02: The Transition from Classical to Post-Quantum Cryptography
• Related work/possible work item
  • draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
• Expired
  – draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
Crypto Review Panel

• Formed in September 2017
  • Wiki page for the team: <https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>
  • Mailing list for internal communications was requested
  • May be used to review documents coming to CFRG, Security Area or Independent Stream.
  • Lots of good reviews done!
Detailed Agenda for IETF 101 (1/2)

15:50 CFRG status update from CFRG chair
    (5 mins; chairs)
15:55 Hacspec
    (10 + 5; Franziskus Kiefer)
    https://github.com/HACS-workshop/hacspec/tree/master/specs

16:10 Randomness Improvements for Security Protocols
    (10 + 5; Christopher Wood)
16:25 Hashing to Elliptic Curves
(10 + 5; Christopher Wood)
https://datatracker.ietf.org/doc/draft-sullivan-cfrg-hash-to-curve/

16:40 Verifiable Oblivious Pseudorandom Functions (VOPRFs)
(10 + 5; Nick Sullivan)
https://datatracker.ietf.org/doc/draft-sullivan-cfrg-voprf/

16:55 VTBPEKE: Verifier-based Two-Basis Password Exponential Key Exchange
(10 + 5; Guilin Wang)
http://www.di.ens.fr/users/pointche/Documents/Papers/2017_asiaccsB.pdf

17:10 KangarooTwelve
(10 + 5; Benoît Viguier)
AOB