CFRG Research Group Status

Chairs:

Alexey Melnikov <alexey.melnikov@isode.com>

Nick Sullivan <nick@cloudflare.com>

Stanislav Smyshlyaev <smyshsv@gmail.com>

Administrative

- This WebEx Session is being recorded
- Minute taker in Etherpad
- Jabber comment relay

Jabber: xmpp:cfrg@jabber.ietf.org?join
  * For the virtual microphone queue, you may want to say "help q"
  * To add yourself to the queue send "q+" in Jabber
  * To remove yourself from the queue send "q-" in Jabber

Etherpad: https://etherpad.ietf.org/p/notes-ietf-107-cfrg?useMonospaceFont=true

Webex: https://ietf.webex.com/ietf/j.php?MTID=m8dded8f6e5c7f92e7262eaf88fa08e24

Note Well – Intellectual Property

- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion
  - The IRTF expects that you file such IPR disclosures in a timely manner – in a period measured in days or weeks, not months
  - The IRTF prefers that the most liberal licensing terms possible are made available for IRTF Stream documents – see RFC 5743
  - Definitive information is in RFC 5378 (Copyright) and RFC 8179 (Patents, Participation), substituting IRTF for IETF, and at https://irtf.org/policies/ipr

Note Well – Privacy & Code of

- As a participant in, or attendee to, any IRTF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public
- Personal information that you provide to IRTF will be handled in accordance with the Privacy Policy at https://www.ietf.org/privacy-policy/
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this
- See RFC 7154 (Code of Conduct) and RFC 7776 (Anti-Harassment Procedures), which also apply to IRTF

Goals of the IRTF

- The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organisation, the IETF, focuses on shorter term issues of engineering and standards making

- **The IRTF conducts research; it is not a standards development organisation**

- While the IRTF can publish informational or experimental documents in the RFC series, its primary goal is to promote development of research collaboration and teamwork in exploring research issues related to Internet protocols, applications, architecture, and technology
- See “An IRTF Primer for IETF Participants” – RFC 7418

CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/interim-2020-cfrg-01/session/cfrg

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

Agenda

https://datatracker.ietf.org/meeting/interim-2020-cfrg-01/session/cfrg

RG Document Status

Document Status

- New RFC (since Singapore)
  - None
- In RFC Editor's queue (since Singapore)
  - None
- In IRSG review
  - draft-irtf-cfrg-argon2-10 (**updated, revised ID needed as per IRSG review**): memory-hard Argon2 password hash and proof-of-work function
  - draft-irtf-cfrg-randomness-improvements-11 (**updated, waiting for IRSG review**): Randomness Improvements for Security Protocols
- Completed, waiting for chairs
  - draft-irtf-cfrg-spake2-10 (**waiting for shepherd's review** (Kenny)): SPAKE2, a PAKE
- Active CFRG drafts
  - draft-irtf-cfrg-hash-to-curve-06 (**updated**): Hashing to Elliptic Curves
  - draft-irtf-cfrg-vrf-06 (**updated**): Verifiable Random Functions (VRFs)
  - draft-irtf-cfrg-kangarootwelve-02 (**updated, RGLC**): KangarooTwelve eXtendable Output Function
  - draft-irtf-cfrg-xchacha-03 (**updated**): XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305
  - draft-irtf-cfrg-voprf-03 (unchanged): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
  - draft-irtf-cfrg-hpke-02 (**updated**): Hybrid Public Key Encryption
  - draft-irtf-cfrg-bls-signature-02: (**updated**): BLS Signature Scheme
  - draft-irtf-cfrg-pairing-friendly-curves-03 (**updated**): Pairing-Friendly Curves
  - draft-hdevalence-cfrg-ristretto-01 (**completed adoption call, expecting new version**): The ristretto255 Group
- Related work/possible work item
  - draft-hoffman-c2pq-06 (**updated**): The Transition from Classical to Post-Quantum Cryptography
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
- Expired
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
  - draft-irtf-cfrg-webcrypto-algorithms-00: Security Guidelines for Cryptographic Algorithms in the W3C Web Cryptography AP
  - draft-irtf-cfrg-augpake-09: Augmented Password-Authenticated Key Exchange (AugPAKE)

Crypto Review Panel

- Formed in September 2016
  - Wiki page for the team: <https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- **Lots of good reviews done!**
- CFRG chairs relied on help from the Crypto Review Panel to review PAKE candidates.
- **New Membership** as of January 2020 (2 years term):
  - Continuing: Scott Fluhrer, Russ Housley, Yaron Sheffer, Bjoern Tackmann
  - New: Chloe Martindale, Julia Hesse, Karthikeyan Bhargavan, Thomas Pornin, Jean-Philippe Aumasson, Jon Callas
  - Thank you to our past members: Stanislav Smyshlyaev, Tibor Jager and Pierre-Alain Fouque

PAKE selection process

- Crypto Review Panel completed Phase 2 reviews and provided its comments
  - We selected: (balanced) CPace and (augmented) OPAQUE.
- Stanislav is going to present summary of the process right after this presentation

AOB