

# CFRG Research Group Status

## IETF 109 Online

Chairs:

Alexey Melnikov <[alexey.melnikov@isode.com](mailto:alexey.melnikov@isode.com)>

Nick Sullivan <[nick@cloudflare.com](mailto:nick@cloudflare.com)>

Stanislav Smyshlyaev <[smyshsv@gmail.com](mailto:smyshsv@gmail.com)>

# Administrative

- This session is being recorded
- Minute taker in Codimd
- Jabber comment relay

**Jabber:** xmpp:cfrg@jabber.ietf.org?join

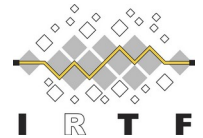
- \* For the virtual microphone queue, you may want to say "help q"
- \* To add yourself to the queue send "q+" in Jabber
- \* To remove yourself from the queue send "q-" in Jabber

Participant guide: <https://www.ietf.org/how/meetings/109/session-participant-guide>  
Request assistance and report issues via: <http://www.ietf.org/how/meetings/issues/>

**Bluesheets** are automatically generated based on IETF Datatracker information

**Minutes:** <https://codimd.ietf.org/notes-ietf-109-cfrg>

# 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 Conduct



- 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/109/session/cfrg>

Data tracker: <https://datatracker.ietf.org/rg/cfrg/documents>

# Agenda

<https://datatracker.ietf.org/meeting/109/session/cfrg>

**05:00 CFRG Update**

(10 mins, CFRG chairs)

**05:10 OPAQUE**

(15+5; Christopher Wood)

**05:30 CPace**

(10+5; Bjoern Haase)

**05:45 Ristretto+Decaf**

(15+5, Henry de Valence)

**06:05 AEAD limits**

(5+5, Martin Thomson)

**06:15 VOPRFs**

(10+5, Armando Faz Hernandez)

**06:30 Secure Crypto Config**

(10+5, Kai Mindermann)

**06:45 AOB**

# RG Document Status



# Document Status

- New RFC (since July)
  - RFC 8937, C. Cremers, L. Garratt, S. Smyshlyaev, N. Sullivan, C. Wood. «Randomness Improvements for Security Protocols»
- In RFC Editor's queue (since April)
  - None
- In IESG review
  - draft-irtf-cfrg-argon2-12 (**updated, IETF conflict review done**): memory-hard Argon2 password hash and proof-of-work function
- In IRSG review
  - None
- Active CFRG drafts
  - draft-irtf-cfrg-spake2-14 (**updated**): SPAKE2, a PAKE
  - draft-irtf-cfrg-hash-to-curve-10 (**updated**): Hashing to Elliptic Curves
  - draft-irtf-cfrg-vrfr-07 (unchanged): Verifiable Random Functions (VRFs)
  - draft-irtf-cfrg-kangarootwelve-04 (**updated, Second RGLC**): KangarooTwelve eXtendable Output Function
  - draft-irtf-cfrg-voprf-05 (**updated**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
  - draft-irtf-cfrg-hpke-06 (**updated, RGLC done, waiting for Shepherd's review**): Hybrid Public Key Encryption
  - draft-irtf-cfrg-bls-signature-04: (**updated**): BLS Signature Scheme
  - draft-irtf-cfrg-pairing-friendly-curves-08 (**updated, addressing concerns from RGLC**): Pairing-Friendly Curves
  - draft-irtf-cfrg-ristretto255-decaf448-00 (**updated, was: draft-irtf-cfrg-ristretto255-00**): The ristretto255 and decaf448 Groups
  - draft-irtf-cfrg-aead-limits-01: (adopted, **updated**): Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-opaque-01 (adopted, **updated**): The OPAQUE Asymmetric PAKE Protocol
  - draft-irtf-cfrg-cpace-00 (adopted, **updated**): CPace, a balanced composable PAKE
- Related work/possible work item
  - draft-hoffman-c2pq-07 (unchanged): The Transition from Classical to Post-Quantum Cryptography
- 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)
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
  - draft-irtf-cfrg-xchacha-03: XChaCha: eXtended-nonce ChaCha and AEAD\_XChaCha20\_Poly1305
  - draft-mattsson-cfrg-det-sigs-with-noise-02: Deterministic ECDSA and EdDSA Signatures with Additional Randomness

# 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.
- CFRG chairs ask for reviews from Crypto Review Panel before RGLC for CFRG documents.
- **Current members (January 2020 – December 2021):**
- Scott Fluhrer, Russ Housley, Yaron Sheffer, Bjoern Tackmann, Chloe Martindale, Julia Hesse, Karthikeyan Bhargavan, Thomas Pornin, Jean-Philippe Aumasson, Jon Callas

# AOB