CFRG
Research Group Status

IETF 113 Vienna

Chairs:

Alexey Melnikov <alexey.melnikov@isode.com>

Nick Sullivan <nick@cloudflare.com>

Stanislav Smyshlyaev <smyshsv@gmail.com>

Administrative

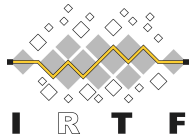
- This session is being recorded
- Minute taker in Codimd
- Jabber comment relay

Participant guide: https://www.ietf.org/how/meetings/technology/meetecho-guide-participant/
Request assistance and report issues via: http://www.ietf.org/how/meetings/issues/

Bluesheets are automatically generated based on IETF Datatracker information

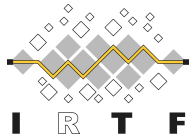
Minutes: **https://codimd.ietf.org/notes-ietf-113-cfrg**

Note Well – Intellectual Property



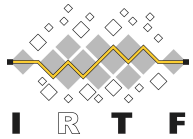
- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your 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/113/session/cfrg

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

Agenda

https://datatracker.ietf.org/meeting/113/session/cfrg

14:30 - Chairs' update (CFRG chairs)

14:35 - Chris Wood, "Discussion of pseudocode in CFRG drafts" (15 mins)

14:50 - Chris Wood, "Key Blinding for Signature Schemes" (15 mins)
https://github.com/chris-wood/draft-dew-cfrg-signature-key-blinding

15:05 - Stephen Farrell, "Signatures: deterministic vs randomized" (10+10 mins)

15:25 - Chris Patton, "Update on the VDAF (Verifiable Distributed Aggregation Functions) draft" (10+5 mins)
https://cjpatton.github.io/vdaf/draft-patton-cfrg-vdaf.html

15:40 - Joachim Fabini, "AES GCM exploit" (10+5 mins)

15:55 - Nimrod Aviram, "A dual-PRF construction" (10+5 mins)

16:10 - Bart Preneel, "The AEGIS family of authenticated encryption algorithms" (5+5 mins)
https://jedisct1.github.io/draft-aegis-aead/draft-denis-aegis-aead.html

16:20 - Dan Harkins, "Deterministic Nonce-less Hybrid Public Key Encryption" (5+5 mins)

16:30 - Meeting ends

RG Document Status

Document Status

- New RFC (since November)
  - RFC 9180: Hybrid Public Key Encryption
- In RFC Editor's queue (since November)
  - draft-irtf-cfrg-spake2-26 (**MISSREF**, Hash-to-curve): SPAKE2, a PAKE
- In IESG review
  - None
- In IRSG review
  - draft-irtf-cfrg-hash-to-curve-14 (**updated, Waiting for IRSG review**): Hashing to Elliptic Curves
- Waiting for IRTF Chair
  - None
- Active CFRG drafts
  - draft-irtf-cfrg-vrf-11 (updated**, waiting for shepherd**): Verifiable Random Functions (VRFs)
  - draft-irtf-cfrg-kangarootwelve-07 (**updated**, **waiting for chairs to review second RGLC outcome**): KangarooTwelve eXtendable Output Function
  - draft-irtf-cfrg-voprf-09 (**updated**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
  - draft-irtf-cfrg-ristretto255-decaf448-03 (**updated**): The ristretto255 and decaf448 Groups
  - draft-irtf-cfrg-aead-limits-04: (**updated**: Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-opaque-08 (**updated**): The OPAQUE Asymmetric PAKE Protocol
  - draft-irtf-cfrg-cpace-05 (**updated**): CPace, a balanced composable PAKE
  - draft-irtf-cfrg-frost-03 (**updated**): FROST: Flexible Round-Optimized Schnorr Threshold Signatures
  - draft-irtf-cfrg-rsa-blind-signatures-03 (**updated**): RSA Blind Signatures
  - draft-fluhrer-lms-more-parm-sets-06 (**adopted**): Additional Parameter sets for LMS Hash-Based Signatures
- Expired
  - draft-irtf-cfrg-bls-signature-04: BLS Signature Scheme
  - draft-irtf-cfrg-pairing-friendly-curves-10 (co-editor added, being worked on): Pairing-Friendly Curves
  - 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
  - draft-hoffman-c2pq-07: The Transition from Classical to Post-Quantum Cryptography

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.
- CFRG chairs ask for reviews from Crypto Review Panel before RGLC for CFRG documents.
- **Current members (**January 2022 – December 2023):
  - Scott Fluhrer, Russ Housley, Bjoern Tackmann, Chloe Martindale, Julia Hesse, Karthikeyan Bhargavan, Thomas Pornin, Jean-Philippe Aumasson, Jon Callas, **Virendra Kumar, Ludovic Perret**

AOB