CFRG RESEARCH GROUP STATUS
IETF 120 VANCOUVER

Chairs:

Stanislav Smyshlyaev <smyshsv@gmail.com>

Nick Sullivan <nicholas.sullivan@gmail.com>

Alexey Melnikov <alexey.melnikov@isode.com>

ADMINISTRATIVE

- **THIS SESSION IS BEING RECORDED**
- **MINUTE TAKER IN HEDGEDOC**
- **JABBER COMMENTS INTEGRATED IN MEETECHO**

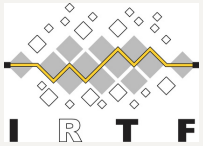
Participant guide:
https://www.ietf.org/how/meetings/technology/meetecho-guide-participant/

Request assistance and report issues via:
http://www.ietf.org/how/meetings/issues/

Bluesheets are automatically generated based on IETF Datatracker information

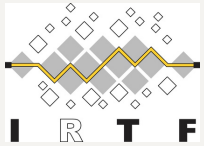
Minutes: https://notes.ietf.org/notes-ietf-120-cfrg

NOTE WELL - INTELLECTUAL PROPERTY



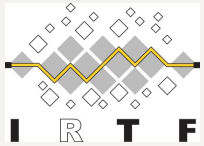
- The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, 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/120/session/cfrg

Datatracker:
https://datatracker.ietf.org/rg/cfrg/documents

AGENDA

https://datatracker.ietf.org/meeting/120/session/cfrg

13:00 - Chairs' update (5 mins).

13:05 - Ghous Amjad, "Partially Blind RSA Signatures" (10+5 mins)

13:20 - Burt Kaliski, "Merkle Tree Ladder (MTL) Mode Signatures" (10+5 mins)

13:35 - Ruediger Geib, "Crypto in IP Capacity Measurement Protocol" (5+10 mins)

13:50 - Shay Gueron, "Double Nonce Derive Key AES-GCM" (10+5 mins)

14:05 - Deirdre Connolly, Stephen Farrell, "KEM Combiners" (5+10 mins)

14:20 - Deirdre Connolly, "HPKE v2" (5+5 mins)

14:30 - End

RG DOCUMENT STATUS

DOCUMENT STATUS (1 OF 3)

- New RFC (since IETF 119)
  - **RFC 9591**: The Flexible Round-Optimized Schnorr Threshold (FROST) Protocol for Two-Round Schnorr Signatures
- In RFC Editor's queue
  - None
- In IESG review
  - **draft-irtf-cfrg-aead-properties-07**: Properties of AEAD Algorithms
  - **draft-irtf-cfrg-kangarootwelve-14**: KangarooTwelve eXtendable Output Function
- In IRSG review
  - None
- Waiting for IRTF Chair
  - **draft-fluhrer-lms-more-parm-sets-15**: Additional Parameter sets for HSS/LMS Hash-Based Signatures
  - **draft-irtf-cfrg-opaque-16**: The OPAQUE Augmented PAKE Protocol

DOCUMENT STATUS (2 OF 3)

- Active CFRG drafts
  - **draft-irtf-cfrg-dnhpke-04** (RGLC ended, needs shepherd followup): Deterministic Nonce-less Hybrid Public Key Encryption
  - **draft-irtf-cfrg-det-sigs-with-noise-03** (updated): Deterministic ECDSA and EdDSA Signatures with Additional Randomness
  - **draft-irtf-cfrg-signature-key-blinding-06** (updated): Key Blinding for Signature Schemes
  - **draft-irtf-aegis-aead-11** (updated): The AEGIS family of authenticated encryption algorithms
  - **draft-irtf-cfrg-bbs-signatures-06** (updated): The BBS Signature Scheme
  - **draft-irtf-cfrg-cpace-11** (updated): CPace, a balanced composable PAKE
  - **draft-irtf-cfrg-vdaf-10** (updated): Verifiable Distributed Aggregation Functions
  - **draft-irtf-cfrg-cryptography-specification-01** (updated): Guidelines for Writing Cryptography Specifications
  - **draft-irtf-cfrg-aead-limits-08** (updated): Usage Limits on AEAD Algorithms

DOCUMENT STATUS (3 OF 3)

- Recently adopted documents
  - None
- Documents in adoption call
  - None
- Expired (active)
  - **draft-irtf-cfrg-pairing-friendly-curves-11**: Pairing-Friendly Curves
  - **draft-irtf-cfrg-bls-signature-05**: BLS Signatures

- Expired (inactive and archived)
  - **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

ERRATA STATUS (1 OF 3)

- RFC7748: Elliptic Curves for Security (Langley, Hamburg, Turner)
  - https://www.rfc-editor.org/errata/eid7096 test vector error
  - https://www.rfc-editor.org/errata/eid7824 test vector error
  - https://www.rfc-editor.org/errata/eid7879 variable error
- RFC8032: Edwards-Curve Digital Signature Algorithm (EdDSA) (S. Josefsson, Liusvaara)
  - https://rfc-editor.org/errata/eid5968: equal sign
  - https://www.rfc-editor.org/errata/eid6306 capitalization
  - https://www.rfc-editor.org/errata/eid6348 punctuation
  - https://www.rfc-editor.org/errata/eid7031 test vectors
- RFC8391: XMSS: eXtended Merkle Signature Scheme (A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen)
  - https://www.rfc-editor.org/errata/eid6352: text
  - https://www.rfc-editor.org/errata/eid6821: numerical error
  - https://www.rfc-editor.org/errata/eid7420: function parameter

ERRATA STATUS (2 OF 3)

- RFC8439: ChaCha20 and Poly1305 for IETF Protocols (Nir, Langley)
  - https://www.rfc-editor.org/errata/eid6569: ambiguous endianness
  - https://www.rfc-editor.org/errata/eid6989: missing character in constant
  - https://www.rfc-editor.org/errata/eid7880: off-by-one
- RFC8554: Leighton-Micali Hash-Based Signatures (D. McGrew, M. Curcio, S. Fluhrer)
  - https://www.rfc-editor.org/errata/eid7409: size error
  - https://www.rfc-editor.org/errata/eid8035: terminology
- RFC 9180: Hybrid Public Key Encryption (Barnes, Bhargavan, Lipp, Wood)
  - https://www.rfc-editor.org/errata/eid7121: algorithm change:trim
  - https://www.rfc-editor.org/errata/eid7251: parenthetical
  - https://www.rfc-editor.org/errata/eid7790: added security text
  - https://www.rfc-editor.org/errata/eid7933: clarification
  - https://www.rfc-editor.org/errata/eid7937: missing details
  - https://www.rfc-editor.org/errata/eid7934: clarification

ERRATA STATUS (3 OF 3)

- RFC 9497: Oblivious Pseudorandom Functions (OPRFs) Using Prime-Order Groups (Davidson, Faz-Hernandez, Sullivan, Wood)
  - https://www.rfc-editor.org/errata/eid7999: algorithm error
  - https://www.rfc-editor.org/errata/eid6989: missing character in constant

CRYPTO REVIEW PANEL

- Formed in September 2016
  - Wiki page for the team: <https://wiki.ietf.org/group/cfrg/CryptoPanel>
- 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 (March 2024 – February 2026):
  - Stephen Farrell, Scott Fluhrer, Russ Housley, Chloe Martindale, Julia Hesse, Karthikeyan Bhargavan, Thomas Pornin, Jon Callas, Virendra Kumar

AOB