

CFRG Research Group Status

IETF 115 London

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 HedgeDoc
- Jabber comment relay

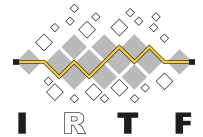
Participant guide: <https://www.ietf.org/how/meetings/technology/meetecho-guide-participant/>

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

Bluesheets are automatically generated based on IETF Datatracker information

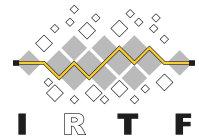
Minutes: <https://notes.ietf.org/notes-ietf-115-cfrg>

Note Well – Intellectual Property



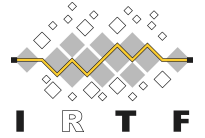
- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
 - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your 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/115/session/cfrg>

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

Agenda

<https://datatracker.ietf.org/meeting/115/session/cfrg>

Chairs: Stanislav Smyshlyaev, Nick Sullivan and Alexey Melnikov

09:30 - Chairs' update.

09:40 - Tobias Looker, "The BBS Signature Scheme" (10+5 mins)

09:55 - Andrey Bozhko, "Classification of properties of AEAD modes" (5+5 mins)

10:05 - Yuto Nakano, "Encryption algorithm Rocca-S" (10+5 mins)

10:20 - Scott Fluhrer, "The use of NTRU" (10+5 mins)

10:35 - AOB

RG Document Status

Document Status (1 of 2)

- New RFC (since July)
 - None
- In RFC Editor's queue
 - draft-irtf-cfrg-spake2-26 (**MISSREF**, Hash-to-curve): SPAKE2, a PAKE
 - draft-irtf-cfrg-hash-to-curve-16: Hashing to Elliptic Curves
- In IESG review
 - draft-irtf-cfrg-vrf-15 (updated): Verifiable Random Functions (VRFs)
- In IRSG review
 - None
- Waiting for IRTF Chair
 - None
- Active CFRG drafts
 - draft-irtf-cfrg-kangarootwelve-08 (**waiting for chairs to review second RGLC outcome**): KangarooTwelve eXtendable Output Function
 - draft-irtf-cfrg-voprf-14 (**updated, in RGLC**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
 - draft-irtf-cfrg-ristretto255-decaf448-04 (**in 2nd RGLC**): The ristretto255 and decaf448 Groups
 - draft-irtf-cfrg-aead-limits-05: Usage Limits on AEAD Algorithms
 - draft-irtf-cfrg-opaque-09: The OPAQUE Asymmetric PAKE Protocol
 - draft-irtf-cfrg-cpace-06: CPace, a balanced composable PAKE
 - draft-irtf-cfrg-frost-11 (**updated**): FROST: Flexible Round-Optimized Schnorr Threshold Signatures
 - draft-irtf-cfrg-rsa-blind-signatures-05 (**in RGLC**): RSA Blind Signatures
 - draft-fluhrer-lms-more-param-sets-08 (**updated**): Additional Parameter sets for LMS Hash-Based Signatures
 - draft-irtf-cfrg-bls-signature-05: BLS Signatures
 - draft-irtf-cfrg-pairing-friendly-curves-11 (**updated**): Pairing-Friendly Curves
 - draft-irtf-cfrg-vdaf-03 (**updated**): Verifiable Distributed Aggregation Functions

Document Status (2 of 2)

- Recently adopted documents
 - draft-irtf-cfrg-det-sigs-with-noise-00: Deterministic ECDSA and EdDSA Signatures with Additional Randomness
 - draft-irtf-aegis-aead-00: The AEGIS family of authenticated encryption algorithms
 - draft-irtf-cfrg-bbs-signatures-01: The BBS Signature Scheme
- Documents in adoption call
 - None
- 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-hoffman-c2pq-07: The Transition from Classical to Post-Quantum Cryptography

AOB