CFRG
Research Group Status

IETF 122 Bangkok

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-122-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 – Audio and Video Recordings

- The IRTF routinely makes recordings of online and in-person meetings, including audio, video and photographs, and publishes those recordings online
- If you participate in-person and choose not to wear a red “do-not-photograph” lanyard, then you consent to appear in such recordings, and if you speak at a microphone, appear on a panel, or carry out an official duty as a member of IRTF leadership then you consent to appearing in recordings of you at that time
- If you participate online, and turn on your camera and/or microphone, then you consent to appear in such recordings
- **This meeting is being recorded and live streamed**

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 – whether in-person or remote, and on the mailing lists as well as during the meetings – 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, the primary output of research groups is expected to be understanding and research results that may be disseminated by publication in scholarly journals and conferences
- See “An IRTF Primer for IETF Participants” – RFC 7418

CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/122/session/cfrg

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

Agenda

https://datatracker.ietf.org/meeting/122/session/cfrg

Chairs: Alexey Melnikov, Stanislav Smyshlyaev and Nick Sullivan

13:00 - Stanislav Smyshlyaev, "Chairs' update" (5 mins)

13:05 - Nick Sullivan, "KEM Combiners Design Team: current status" (5+5)

13:15 - Vasilis Kalos, Greg Bernstein, "Blind BBS and BBS Pseudonyms" (10+5 mins)

13:30 - Chris Wood, "Anonymous Rate-Limited Credentials" (10+5 mins)

13:45 - Michele Orru, "Sigma protocols and Fiat-Shamir" (5+5 mins)

13:55 - Patrick Longa, "FrodoKEM" (5+5 mins)

14:05 - Deirdre Connolly, "Hybrid PQ/T Key Encapsulation Mechanisms" (10+5 mins)

14:20 - Yuchen Wang, "ECDH-PSI" (10+5 mins)

14:35 - Rohan Mahy, "MIMI franking mechanism" (10+5 mins)

14:50 - Haruhisa Kosuge, "Advantages of NTRU compared to ML-KEM" (5+5 mins)

RG Document Status

Document Status (1/2)

- New RFC (since November)
  - None
- In RFC Editor's queue (since November)
  - draft-irtf-cfrg-aead-properties-09 (unchanged): Properties of AEAD algorithms
  - draft-irtf-cfrg-opaque-18 (**updated**): The OPAQUE Asymmetric PAKE Protocol
  - draft-irtf-cfrg-kangarootwelve-17 (**updated**): KangarooTwelve and TurboSHAKE
- Sent to the RFC Editor
  - draft-fluhrer-lms-more-parm-sets-19 (**updated**): Additional Parameter sets for LMS Hash-Based Signatures
- In IESG review
  - None
- In IRSG review
  - None
- Waiting for IRTF Chair
  - None
- In RG Last Call
  - draft-irtf-cfrg-aegis-aead-16 (**updated**): The AEGIS Family of Authenticated Encryption Algorithms
  - draft-irtf-cfrg-aead-limits-09 (unchanged): Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-dnhpke-05 (unchanged): Deterministic Nonce-less Hybrid Public Key Encryption

Document Status (2/2)

- In Crypto Panel review
  - draft-irtf-cfrg-rsa-guidance-03 (**updated**): Implementation Guidance for the PKCS #1 RSA Cryptography Specification
  - draft-irtf-cfrg-vdaf-14 (unchanged): Verifiable Distributed Aggregation Functions
- Active CFRG drafts:
  - draft-irtf-cfrg-cpace-13 (unchanged): CPace, a balanced composable PAKE
  - draft-irtf-cfrg-dnhpke-06 (**updated**): Deterministic Nonce-less Hybrid Public Key Encryption
  - draft-irtf-cfrg-det-sigs-with-noise-05 (**updated**): Deterministic ECDSA and EdDSA Signatures with Additional Randomness
  - draft-irtf-cfrg-signature-key-blinding-07 (unchanged): Key Blinding for Signature Schemes
  - draft-irtf-cfrg-partially-blind-rsa-00 (unchanged): Partially Blind RSA Signatures
  - draft-irtf-cfrg-bbs-signatures-08 (**updated**): The BBS Signature Scheme
  - draft-irtf-cfrg-bbs-blind-signatures-01 (**adopted, updated**): Blind BBS Signatures
  - draft-irtf-cfrg-bbs-per-verifier-linkability-01 (**adopted, updated**): BBS per Verifier Linkability
  - draft-irtf-cfrg-hybrid-kems-03 (**updated**): Hybrid PQ/T Key Encapsulation Mechanisms
- Expired:
  - draft-irtf-cfrg-cryptography-specification-01: Guidelines for Writing Cryptography Specifications
  - draft-irtf-cfrg-pairing-friendly-curves-11: Pairing-Friendly Curves
  - draft-irtf-cfrg-bls-signature-05: BLS Signature Scheme

Errata Summary

- RFC 7539: ChaCha20 and Poly1305 for IETF Protocols
  - 1 errata report
- RFC 7748: Elliptic Curves for Security
  - 1 errata report
- RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)
  - 4 errata reports
- RFC 8391: XMSS: eXtended Merkle Signature Scheme
  - 1 errata report
- RFC 8554: Leighton-Micali Hash-Based Signatures
  - 1 errata report
- RFC 9180: Hybrid Public Key Encryption
  - 1 errata report
- RFC 9497: Oblivious Pseudorandom Functions (OPRFs) Using Prime-Order Groups
  - 1 errata report
- RFC 7539: ChaCha20 and Poly1305 for IETF Protocols
  - 2 errata reports

Recharter?

- Lessons learnt based on
  - ECC selection;
  - Nine years of work of Crypto Review Panel;
  - PAKE selection;
  - work on KEM Combiners.

- CFRG documents come together with new research papers in a majority of cases.
  - https://eprint.iacr.org/search?q=cfrg: PAKEs, elliptic curves, HPKE, AEAD usage limits, AEAD modes, re-keying mechanisms…
- When a new work item is proposed (before call for adoption) to CFRG, the authors present mechanisms together with security proofs.
- After drafts are adopted in CFRG, many authors present additional results of security assessment.
- Crypto Review Panel experts assess current state of research of the mechanisms in the drafts under review: recognized research results (e.g., presented at IACR conferences) are necessary.
- CFRG gives an analysis of the academic consensus, provides guidance and seeks for solutions of the problems – starting with the problem, not a specific mechanism.

- A pain point: sometimes people want directions from CFRG to be given faster – but it seems necessary to be sure in mechanisms/approaches, have enough reviews and opinions, wait for academia to do enough research etc.
- A pain point: requests for documents whose primary goal is immediate implementation guidance and/or to unblock implementers.

Recharter?

- Possible re-charter? Add some focus on what CFRG is meant to do as an IRTF group?
  - Open, expert analysis and peer review of cryptographic techniques and algorithms relevant to Internet protocols.
  - Informational RFCs that document and explore the solution space for specific cryptographic topics, including detailed analyses, pseudocode, and test vectors as appropriate.
  - Guidance to inform cryptographic choices made by protocol designers and standardization efforts within the IETF.
  - CFRG does not directly standardize protocols or algorithms; it offers foundational research and cryptographic insights to inform standardization activities. CFRG is not intended as a venue for documents whose primary goal is immediate implementation guidance or solely to unblock implementers without substantial accompanying research context.

- More in Nick's slides on the KEM Combiners Design Team.

AOB