CRYPTO FORUM RESEARCH GROUP
RESEARCH GROUP STATUS

IETF 123

Madrid

Chairs

Nick Sullivan (nicholas.sullivan+ietf@gmail.com)
Alexey Melnikov (alexey.melnikov@isode.com)
Stanislav Smyshlyaev (smyshsv@gmail.com)

ADMINISTRATIVE

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

PARTICIPANT'S 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-123-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
- Also see RFC 9775 (IRTF Code of Conduct)

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

- **NEW**: See “An IRTF Primer for IETF Participants” – RFC 7418

AGENDA

https://datatracker.ietf.org/meeting/123/session/cfrg

Chairs: Alexey Melnikov, Stanislav Smyshlyaev and Nick Sullivan

17:00 - Nick Sullivan, "Chairs' update" (5 mins)
17:05 - Richard Barnes, "Hybrid KEMs" (15+5 mins)
17:25 - Haruhisa Kosuge, "NTRU" (5 mins)
17:30 - Simon Josefsson, "Classic McEliece" (5 mins)
17:35 - PQ KEMs discussion (15 mins)
17:50 - Vasilis Kalos, Greg Bernstein, "Blind BBS and BBS Pseudonyms" (5+5 mins)
18:00 - Abhi Shelat, "libZK: a zero-knowledge proof library" (5+5 mins)
18:10 - Cathie Yun, "Sigma protocols and Fiat-Shamir" (10+5 mins)
18:25 - Yuto Nakano, "Rocca-S" (5+5 mins)
18:35 - Jean Paul Degabriele, "Improved ChaCha-based AEAD Scheme" (5+5 mins)
18:45 - Chris Wood, "Hybrid PQ PAKE" (10+5 mins)

CFRG RESEARCH GROUP

Online Agenda and Slides at:
https://datatracker.ietf.org/meeting/123/session/cfrg

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

CFRG AND PQ KEMS

- **FAQ at https://wiki.ietf.org/group/cfrg:**
  - 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.

- **CFRG@IETF 122 slides:**
  - "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."

- **"Post-quantum KEM requirements and adoption" thread on the CFRG mailing list** – we've got more pain due to these pain points!

On the agenda today:
17:35 - PQ KEMs discussion (15 mins)

ON THE AGENDA: PQ KEMS DISCUSSION

- Problem Definition: Are we convinced that the problem being solved by adopting a PQ KEM for CFRG is well-defined and well-motivated? (Having a clear problem statement and motivation is a known prerequisite for adoption consideration [2].)

- Need for Requirements Draft: Do we need a KEM requirements document before proceeding with any specific KEM adoption? In other words, should we first agree on a framework of criteria/priorities for KEMs in CFRG?

- Selection Criteria without Requirements: If we decide not to write a separate requirements draft, how will the group evaluate and select among multiple KEM proposals for adoption? (For example, if both Classic McEliece and FrodoKEM are on the table, by what process or criteria would we choose one or more to adopt?)

RG DOCUMENT STATUS

DOCUMENT STATUS (1/2)

- New RFC (since November)
  - RFC 9771: Properties of Authenticated Encryption with Associated Data (AEAD) Algorithms
  - **RFC 9807: The OPAQUE Augmented Password-Authenticated Key Exchange (aPAKE) Protocol**
- In RFC Editor's queue (since March)
  - draft-irtf-cfrg-kangarootwelve-17 (EDIT): KangarooTwelve and TurboSHAKE
  - draft-fluhrer-lms-more-parm-sets-19 (EDIT): Additional Parameter sets for LMS Hash-Based Signatures
  - draft-irtf-cfrg-opaque-18 (AUTH48): The OPAQUE Asymmetric PAKE Protocol
- In IESG review
  - None
- In IRSG review
  - draft-irtf-cfrg-aegis-aead-16 (unchanged): The AEGIS Family of Authenticated Encryption Algorithms
- Waiting for IRTF Chair
  - None
- In RG Last Call
  - draft-irtf-cfrg-aead-limits-10 (**updated**): Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-dnhpke-06 (unchanged): Deterministic Nonce-less Hybrid Public Key Encryption

DOCUMENT STATUS (2/2)

- In Crypto Panel review
  - draft-irtf-cfrg-vdaf-15 **(updated)**: Verifiable Distributed Aggregation Functions
  - draft-irtf-cfrg-rsa-guidance-04 (**updated, Crypto Panel review done**): Implementation Guidance for the PKCS #1 RSA Cryptography Specification
- Active CFRG drafts:
  - draft-irtf-cfrg-cpace-14 (**updated**): CPace, a balanced composable PAKE
  - draft-irtf-cfrg-kemeleon-00 (**adopted**): Kemeleon Encodings
  - draft-irtf-cfrg-signature-key-blinding-08 (**updated**): Key Blinding for Signature Schemes
  - draft-irtf-cfrg-det-sigs-with-noise-05 (unchanged): Deterministic ECDSA and EdDSA Signatures with Additional Randomness
  - draft-irtf-cfrg-partially-blind-rsa-01 (unchanged): Partially Blind RSA Signatures
  - draft-irtf-cfrg-bbs-signatures-09 (**updated**): The BBS Signature Scheme
  - draft-irtf-cfrg-bbs-blind-signatures-01 (unchanged): Blind BBS Signatures
  - draft-irtf-cfrg-bbs-per-verifier-linkability-01 (unchanged): BBS per Verifier Linkability
  - draft-irtf-cfrg-hybrid-kems-05 (**updated**): Hybrid PQ/T Key Encapsulation Mechanisms
  - draft-irtf-cfrg-concrete-hybrid-kems-00 (**adopted**): Concrete Hybrid PQ/T Key Encapsulation Mechanisms
  - draft-irtf-cfrg-cryptography-specification-02 (**updated**): Guidelines for Writing Cryptography Specifications
- Expired:
  - draft-irtf-cfrg-pairing-friendly-curves-11: Pairing-Friendly Curves
  - draft-irtf-cfrg-bls-signature-05: BLS Signature Scheme

ERRATA UPDATE

- 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
  - 5 errata reports
- RFC 8439: ChaCha20 and Poly1305 for IETF Protocols
  - 2 errata reports
- 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
  - 3 errata reports

CFRG MEETING FORMAT

- Two hour format
- Mostly introduction of potential new work and informational presentations relevant to the group
- Updates on ongoing work

- Issues
  - Oversubscribed: too many proposed presentations
  - Educational but not productive

- Proposal for IETF 124
  - Two-hour slot for informational presentations and new work
  - Additional one-hour slot focused on *consensus* and advancing drafts

AOB

CRYPTO FORUM RESEARCH GROUP
RESEARCH GROUP STATUS

IETF 123

Madrid

Chairs

Nick Sullivan (nicholas.sullivan+ietf@gmail.com)
Alexey Melnikov (alexey.melnikov@isode.com)
Stanislav Smyshlyaev (smyshsv@gmail.com)