CRYPTO FORUM RESEARCH GROUP
RESEARCH GROUP STATUS

IETF 126

Vienna

Session 1: Wednesday, July 22, 900-1100 CEST
Session 2: Friday, July 24, 1130-1230 CEST

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

PARTICIPANT'S GUIDE

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

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

Bluesheets are automatically generated based on IETF Datatracker information

Minutes: https://notes.ietf.org/notes-ietf-126-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)

AGENDA

https://datatracker.ietf.org/doc/agenda-126-cfrg/

Chairs: Alexey Melnikov, Stanislav Smyshlyaev and Nick Sullivan

Wednesday, July 22, 2026, 9:00-11:00 (UTC+2)
09:00 - Alexey Melnikov, "Chairs' update" (10 mins)
09:10 - Open Discussion: PQ KEMs (30 mins)
09:40 - Julien Devevey, "Silithium" (10+5 mins)
09:55 - Uri Blumenthal, Valery Smyslov, "PQuAKE" (15+5 mins)
10:15 - Christopher Wood, "Hybrid Post-Quantum PAKE" (10+5 mins)
10:30 - Abhi Shelat, "Longfellow ZK" (5+5 mins)
10:40 - Emil Lundberg, "The ARKG algorithm" (10+5 mins)
10:55 - AOB

Friday, July 24, 2025, 11:30-12:30 (UTC+2)
11:30 - Felix Günther, "Kemeleon Encodings" (10+5 mins)
11:45 - Greg Bernstein, Anja Lehman, "BBS, Blind BBS, BBS pseudonyms" (15+5 mins)
12:05 - Shai Levin, Anja Lehman, "Schnorr-Type Proofs for ECDSA Device Binding" (10+5 mins)
12:20 - Yumi Sakemi, "Pairing-Friendly Curves" (5+5 mins)

CFRG RESEARCH GROUP

Online Agenda and Slides at:
https://datatracker.ietf.org/meeting/126/session/cfrg

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

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

CRYPTO REVIEW PANEL

- Formed in September 2016
- Provides critical, objective, timely, and consistent review of cryptographic work
- May review documents from CFRG, the Security Area, and the Independent Stream
- Reviews are public and advisory
- Current term: April 2026 - May 2028

Uri Blumenthal	**Wang Guilin**
Scott Fluhrer	**Kris Kwiatkowski**
Stephen Farrell	**Enrique Larraia**
Markku-Juhani O. Saarinen	**Sherman Chow**
Russ Housley	**Julia Hesse**

https://wiki.ietf.org/group/cfrg/CryptoPanel

RG DOCUMENT STATUS

DOCUMENT STATUS (1/2)

- New RFC (since July)
  - None
- In RFC Editor's queue
  - draft-irtf-cfrg-aegis-aead-18: The AEGIS Family of Authenticated Encryption Algorithms
- In IESG review
  - draft-irtf-cfrg-rsa-guidance-09 (updated): Implementation Guidance for the PKCS #1 RSA Cryptography Specification
- In IRSG review
  - draft-irtf-cfrg-cpace-21 (updated): CPace, a balanced composable PAKE
- Waiting for IRTF Chair
- In RG Last Call
  - draft-irtf-cfrg-dnhpke-08 (**updated**): Deterministic Nonce-less Hybrid Public Key Encryption
  - draft-irtf-cfrg-aead-limits-11 (expired): Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-vdaf-20 (**updated**): Verifiable Distributed Aggregation Functions
  - draft-irtf-cfrg-concrete-hybrid-kems-04 (**updated**): Concrete Hybrid PQ/T Key Encapsulation Mechanisms
  - draft-irtf-cfrg-hybrid-kems-12 (**updated**): Hybrid PQ/T Key Encapsulation Mechanisms

DOCUMENT STATUS (2/2)

- In Crypto Panel review
  - None
- Newly Adopted CFRG drafts:
  - None
- Active CFRG drafts:
  - draft-irtf-cfrg-fiat-shamir-02 (unchanged): Fiat-Shamir Transformation
  - draft-irtf-cfrg-sigma-protocols-02 (unchanged): Interactive Sigma Proofs
  - draft-irtf-cfrg-signature-key-blinding-09 (**updated**): Key Blinding for Signature Schemes
  - draft-irtf-cfrg-bbs-blind-signatures-03 (**updated**): Blind BBS Signatures
  - draft-irtf-cfrg-bbs-per-verifier-linkability-03 (**updated**): BBS per Verifier Linkability
  - draft-irtf-cfrg-bbs-signatures-10 (unchanged): The BBS Signature Scheme
  - draft-irtf-cfrg-bls-signature-07 (**updated**): BLS Signatures
  - draft-irtf-cfrg-cryptography-specification-03 (**updated**): Guidelines for Writing Cryptography Specifications
  - draft-irtf-cfrg-kemeleon-02 (**updated**): Kemeleon Encodings
- Expired adopted drafts:
  - draft-irtf-cfrg-partially-blind-rsa-02: Partially Blind RSA Signatures
  - draft-irtf-cfrg-det-sigs-with-noise-05: Hedged ECDSA and EdDSA Signatures

ERRATA UPDATE

for the last 3 months

Held for tooling update in errata system.

- RFC 8554, EID 8907
  - LMS public key XDR structure
  - Proposed: HOLD
- RFC 9858, EID 8896
  - Appendix A ASCII rendering of test messages
  - Proposed: HOLD
- RFC 9861, EID 8997
  - missing "M=" labels in KangarooTwelve/TurboSHAKE test-vector headings
  - Proposed: REJECT

AOB

CRYPTO FORUM RESEARCH GROUP
RESEARCH GROUP STATUS

IETF 126

Vienna

Session 1: Wednesday, July 22, 900-1100 CEST
Session 2: Friday, July 24, 1130-1230 CEST

Chairs

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

PQ KEM SECURITY CONSIDERATIONS
SHAPE OF THE WORK

Inputs received

ML-KEM, FrodoKEM, Classic McEliece, Streamlined NTRU Prime, NTRU, NTRU+, NTRU-family review checklist

Process

The chairs a discussion on list to help shape call for adoption of the topic

Questions for the RG

- One common KEM-use guidance document?
- Common integration guidance plus separate per-KEM analyses?
- Fit-for-purpose criteria and recommendations?

Goal today

Identify the scope and initial document structure for an adoption call.