

# CFRG Research Group

Online Agenda and Slides at:

<https://datatracker.ietf.org/meeting/99/agenda/cfrg/>

Data tracker: [http://datatracker.ietf.org/rg/cfrg/  
documents/](http://datatracker.ietf.org/rg/cfrg/documents/)

# Agenda

<https://datatracker.ietf.org/meeting/99/agenda/cfrg/>

# IETF Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

## **The brief summary:**

- ❖ **By participating with the IETF, you agree to follow IETF processes.**
- ❖ **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- ❖ **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Also see: <http://www.ietf.org/about/note-well.html>:

# Administrative

- Audio Streaming/Recording
  - Please speak only using the microphones
  - Please state your name before speaking
- Minute takers & Etherpad
- Jabber

# CFRG Research Group Status

Chairs:

Kenny Paterson <[kenny.paterson@rhul.ac.uk](mailto:kenny.paterson@rhul.ac.uk)>

Alexey Melnikov <[alexey.melnikov@isode.com](mailto:alexey.melnikov@isode.com)>

# RG Document Status

# Document Status

- New RFC (since Seoul)
  - RFC 8032: Edwards-curve Digital Signature Algorithm (EdDSA)
  - RFC 8125: Requirements on PAKE schemes
- In RFC Editor's queue
  - None since Seoul
- In IRSG review
  - draft-irtf-cfrg-xmss-hash-based-signatures-09 (**updated**): XMSS: Extended Hash-Based Signatures
  - draft-nir-cfrg-rfc7539bis-01 (**updated**): ChaCha20 and Poly1305 for IETF Protocols
- Completed, waiting for chairs
  - None
- Active CFRG drafts
  - draft-irtf-cfrg-argon2-02 (**updated**): memory-hard Argon2 password hash and proof-of-work function
  - draft-irtf-gcmsiv-05 (**updated**): AES-GCM-SIV: nonce misuse-resistant authenticated encryption
  - draft-irtf-cfrg-re-keying-05 (**updated**): Re-keying Mechanisms for Symmetric Keys
  - draft-mcgrew-hash-sigs-07 (**updated**): Hash-Based Signatures
  - draft-irtf-cfrg-augpake-07 (**expires soon**): Augmented Password-Authenticated Key Exchange (AugPAKE)
- Related work/possible work item
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
- 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 API
  - draft-irtf-cfrg-spake2-03: SPAKE2, a PAKE

# Crypto Review Panel

- Formed in September
  - Wiki page for the team: <<https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>>
  - Mailing list for internal communications was requested
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- **Lots of good reviews done!**



# AOB