CFRG (Crypto Forum Research Group)

IETF 114 in Philadelphia

- Date: Monday, July 25, 2022 (2 hours)
- Time: 10:00-12:00 (UTC - 4)
- Meetecho: https://meetings.conf.meetecho.com/ietf114/?group=cfrg&short=&item=1
- Onsite tool: https://meetings.conf.meetecho.com/onsite114/?group=cfrg&short=&item=1
- Jabber: cfrg@jabber.ietf.org
- Notes: https://notes.ietf.org/notes-ietf-114-cfrg

RG Chairs:

- Nick Sullivan nick@cloudflare.com
- Stanislav Smyshlyaev smyshsv@gmail.com
- Alexey Melnikov alexey.melnikov@isode.com

Note taker

Rich Salz

Minutes for CFRG at IETF 114

Chairs' update.

No time for agenda bashing; assume everyone has seen the NOTE WELL. Hardware problems ate 25% of the time.
Many documents in flight; two pages of doc status shown.

draft-mattsson-cfrg-det-sigs-with-noise has chairs working with IRTF Chair to determine about IP rights issues.

Please limit questions, to save time, and discuss on the list.

Tobias Looker, “The BBS Signature Scheme” (15+5 mins)

`https://identity.foundation/bbs-signature/draft-bbs-signatures.html`

- BBS signatures have selective disclosure, proof of position, ZKP protocol for unlinkable proofs.
- 2004 first appearance in research. Based on pairings, two subgroups, currently use BLS12-381 curves, but is agnostic.
- App data has headers, always disclosed, and message, which are selectively disclosed.
- Signature size constant: EC point plus two scalars regardless of which parts are signed.
- Several operations are constant time if no selective disclosure is used.
- One of the three use-cases presented: Privacy preserving anonymous credentials: Prove name/age to restaurant; student to library; address to post office.
- Seeking CFRG adoption. BOF on JSON web proofs could use this. Also PrivacyPass.

Deirdre Connolly, “Two-Round Threshold Schnorr Signatures with FROST” (10+5 mins)

- 2 round, multi-signers, looks like standard signature.
- Focus of this draft is post-keygen; focus on signing and then coordinator aggregates sig shares to final signature.
- See “Frost Overview” slide.
- Four ciphersuites defined, including 25519 and 448; resultant signatures are compatible with RFC 8032
- Seeking CFRG Crypto review, more implementations; thinking of adding secp256k1

Chris Wood, “Key Blinding for Signature Schemes” (10+5 mins)

- Update on recently adopted draft.
- New operations:
    - BlindKeyGen produce a blinding key; has a context (rate-limit, Tor info, etc.);

    - BlindPublicKey given public key and blinding key, produce blinded public key;
    - BlindKeySign sign with secret key and secret blind;
    - Optional UnblindPublicKey given blinded public key and blinding key, produce original.
- Have implementations, security analysis being done, think feature complete, want Crypto Panel review.

Chris Wood, “RSA Blind Signatures” (10+5 mins)

- Security proof showed issue in low-entropy uses (e.g., small size of pool).
- Plan: remove deterministic variants; add nonce for low-entropy uses. Want to know if the removal would be problematic.

Bjoern Haase, “CPace” (5+5 mins)

- Based on feedback and discussions, focusing on three personas: Application architecture designer, Implementer, Tester.
- New draft has been uploaded.
- Next steps: review from the Crypto Panel.

Sofia Celi and Thom Wiggers, “Post-Quantum NIST Process” (10+5 mins)

- This is a summary, not a complete overview. Biased toward familiar objects. Not pitching a draft or suggesting a particular path.
- Kyber is first NIST KeyEx. Based on Lattice; interactive, not a drop-in for DH style.
- Dilithium for signatures. Quite large but fast.
- Falcon for signatures. Smaller than Dilithium, hard to implement correctly, need constant time 64bit FPU.
- SPHINCS+ for signatures. Stateless hash-based, hundreds of hashing so slow, 36 parameter sets right now.
- Other KEMs could be added: Classic McEliece, SIKE, BIKE, HQC (see slides).
- NIST issuing a second call for proposals with goals of short signatures, fast verification; take years, probably 2030.
- Running code available.
- Questions to think: does your protocol handle non-DH-like KEM?

- Scott Fluhrer: IP concerns about patents on Kyber, not cleared-up. NIST report says they have plans, hope to resolve to their satisfaction; Scott: might not be to everyone's satisfaction. Scott intends to submit an NTRU draft "just in case."

Bas Westerbaan, "Kyber" (5+5 mins)

```
https://github.com/bwesterb/draft-schwabe-cfrg-kyber
```

- Think standard published 2024; expect incompatible but small changes.
- Want an RFC, with interim drafts for use by early adopters, include Python reference code, provide feedback to NIST.
- Any interest in that?
- PHB: I am very interested even if it does not match what NIST ends up with.

AOB