CFRG (Crypto Forum Research Group)

- Date: Thursday, November 11, 2021
- Time: 12:00 - 14:00 UTC, Virtual
- Meetecho: https://meetings.conf.meetecho.com/ietf112/?group=cfrg&short=&item=1
- Jabber: cfrg@jabber.ietf.org
- Notes: https://codimd.ietf.org/notes-ietf-112-cfrg

Minutes for CFRG at Virtual IETF 112

RG Chairs:

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

Agenda

No changes.

CFRG Update

- Draft status, updates.
- Crypto review panel rotating December, will announce call for nominations.

Verifiable Distributed Aggregation Functions

Chris Patton

Not asking for adoption, introduce and solicit feedback

Ties into PRIV BoF, BoF on aggregating functions via MPC

Underlying crypto in this draft: lots of solutions in literature, but each slightly different. Draft puts them all in common framework. Abstraction boundary, target for cryptographers. Need to validate inputs, ZKP required, interactive verification. Working on implementations. Few microseconds work per sample.

Watson: Not sure why not asking for adoption

Chris: Waiting until BoF->WG

Stanislav: When you want adoption, ask on the list.

CPace (draft-irtf-cfrg-cpace)

Bjoern Haase

Two major updates to security analysis. SID can be removed and the protocol remains secure. Describing functions important for CPACE: generator, scalar multiplication, explicit point verification.

Appendix with security functions. SID: now optional, recommended. Can be piggybacked on messages.

Resolved SID and game-based proof.

Updating draft to focus on implementor. Parallel and initiator/responder setting. Four functions, then describe for ecosystems. Associated Data fields added to protocol messages for game based proof. Hashing now preappends lengths to hashed data. Questions on markdown and automated creation.

Need to decide: one environment with initator and responder or parallel? Github integration issues.

Stanislav: When do you want Crypto Review Panel to review, when RGLC?

Bjoern: Draft by the end of year should be in in shape for crypto review.

VOPRF (draft-irtf-cfrg-voprf)

Chris Wood

Major change: 2DHVOPRF to 3DHPOPRF to align with protocol needs. Some changes with ciphersuites. Test vectors, editorial clarity. POPRF: additional public input. Security differences: not yet a UC proof, just a game based one in algebraic group model. Confidence in security but UC proof makes OPAQUE analysis harder

Thresholding harder: is anyone actually using it? So plenty of other things: distributed key gen, separate objects with distinct APIs, etc. Pedersen? Apparently some questions.

Chris Patton: Agree on chopping out things.

Jonathan Hoyland: How do you know public data isn't too revealing?

Chris Wood: It is application dependent

Sofia Celi: Same issue in 2DH with keys, application dependent.

‘Short’ hash and KMAC as a KDF

Bob Moskowitz

Small hashes: constrained environment. Keyed or over cleartext. Hashing hardware makes evaluating lots of hashes cheap->collision finding faster. MAVlink 2. 48 bit authenticator. No good guidelines: should there be a doc. KMAC: sadly overlooked: cheaper than HMAC for short messages. Standardized length: no truncation. FIPS 202 distinguishes between XOF and hash. KMAC as KDF? NIST guidance lagging. Need analysis beyond Team Keccak. Keccak team says this is fine. Multiple secret generation etc. Cannot take CPU from the camera payloads.

Watson: Mac or Hash? Very different.

Scott Fluhrer: How you explain I don’t know.

John Mattsson: I support idea of guidance.

PHB: Worth looking at some of these things. Should be easier to get things right. Should be as safe as possible.

Chris Patton: describing usecase is a good start

Bob: A lot of times very constrained.

Stanislav: Take it to the list. People can collaborate and come back with specific request(s) to CFRG chairs

Private Access Tokens

Chris Wood

PATS is a big thing, this is a core crypto bit. Clients have secret values, mediators have public values X issuers k. Want to compute F(x, k). Issuer learns nothing. Client learns output if x corresponds with X. Sketch of protocol in the slides.

Questions: security model make sense? Sketch meet these goals? Does it compute a PRF?

Martin Thompson: Do we need to solve this?

Chris Wood: No consensus on that.

Jonathan Hoyland, Chris Patton, Britta Hale: Worth solving.

AOB

PHB: Announcement: threshold for SSH.