CFRG:

Bringing Cryptography to the Internet Community

Alexey Melnikov

Stanislav Smyshlyaev, Ph.D.

Nick Sullivan

Crypto Forum Research Group

CFRG Goals

From the Charter:

- «The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.»
- «The CFRG **serves as a bridge between theory and practice, bringing new cryptographic techniques to the Internet community** and promoting an understanding of the use and applicability of these mechanisms via Informational RFCs.»
- «IETF working groups developing protocols that include cryptographic elements are welcome to bring questions concerning the protocols to the CFRG for advice.»

Broadly, the goals are:

- Define/standardize crypto primitives for use by IETF and other SDOs (e.g. W3C).
- Meeting place for both academics (cryptographers) and practitioners (security protocol designers and implementors).
- Educate IETF participants.
- Cryptographic expertise for IETF WGs and ISE.

Most CFRG meetings are co-located with IETF.

History

- David McGrew and Kevin Igoe – original chairs from July 2002
- Community lost faith in NIST and NSA, “Requesting removal of CFRG co-chair” thread in December 2013 started by Trevor Perrin
- Alexey Melnikov and Kenny Paterson – chairs from June 2014
- Elliptic curves selection: 2014-2015. Resulted in RFC 7748, selected Curve25519 and Curve448, now widely used in practice.
- Crypto Review Panel – “to ensure that CFRG chairs have at their disposal sufficient resources and lightweight processes to provide critical, objective, timely and consistent review of cryptographic algorithms in IRTF and IETF documents”, from 2016
- Alexey Melnikov, Kenny Paterson and Nick Sullivan – chairs from May 2019
- Alexey Melnikov, Nick Sullivan and Stanislav Smyshlyaev – chairs from January 2020
- PAKE protocols selection: 2019-2020. Selected 2 PAKEs: CPace (balanced), OPAQUE (augmented).
- Chris Wood – secretary from January 2022

[Some of the] Documents Published

- RFC 7664, *"Dragonfly Key Exchange"*, 2015-11
- RFC 7748, *"Elliptic Curves for Security"*, 2016-01
- RFC 8032, *"Edwards-Curve Digital Signature Algorithm (EdDSA)"*, 2017-01
- RFC 8125, *"Requirements for Password-Authenticated Key Agreement (PAKE) Schemes"*, 2017-04
- RFC 8391, *"XMSS: eXtended Merkle Signature Scheme"*, 2018-05
- RFC 8439, *"ChaCha20 and Poly1305 for IETF Protocols"*, 2018-06
- RFC 8452, *"AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption"*, 2019-04
- RFC 8554, *"Leighton-Micali Hash-Based Signatures"*, 2019-04
- RFC 8645, *"Re-keying Mechanisms for Symmetric Keys"*, 2019-08
- RFC 8937, *"Randomness Improvements for Security Protocols“*, 2020-10
- RFC 9106, *"Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications“*, 2021-09
- RFC 9180, *"Hybrid Public Key Encryption“*, 2022-02

CFRG and IETF

- Most of CFRG output directly feeds into IETF work:
  - Security Area WGs: TLS, MLS, IPSECME, LAMPS, DCRUP (ART), etc.
  - New mechanisms (VOPRF, HPKE, PAKEs) are developed taking into account needs of IETF WGs
- IETF sometimes comes with specific requests
  - E.g. what is the key lifetime boundary for a particular cryptographic mode of operation?
  - E.g. which elliptic curves/PAKEs should we use in TLS/IPsec/etc.?
- Crypto Review Panel
  - A panel of crypto experts (academics and applied security experts), that review literature on new crypto algorithms/constructs or their use in protocols
  - They review documents not only for readability and implementability, but also give outline of whether there can be security issues with the documents, based on the current state of research (not conducting new research during review!)
  - They do reviews of CFRG documents, documents from Security Area/IETF or Independent Stream, proposals during contests
- Currently 11 members, appointed for 2 years term ending in December 2023

CFRG and Research

- CFRG documents come together with new research papers in a majority of cases.
  - https://eprint.iacr.org/search?q=cfrg: PAKEs, elliptic curves, HPKE, AEAD usage limits, AEAD modes, re-keying mechanisms.
- When a new work item is proposed (before call for adoption) to CFRG, the authors present mechanisms together with security proofs.
- After drafts are adopted in CFRG, many authors present additional results of security assessment.
- Crypto Review Panel experts assess current state of research of the mechanisms in the drafts under review: recognized research results (e.g., presented at IACR conferences) are necessary.

- 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.

Processes in CFRG and [other] SDOs: audiences

CFRG and ISO (ISO/IEC JTC 1/SC 27/WG 2 "Cryptography and Security Mechanisms")

- Audiences:
  - ISO:
    - Regulatory bodies seeking for guidance regarding the mechanisms to allow in information systems
    - Industry-specific bodies (including SDOs) choosing which mechanisms to require for their areas (e.g., which block cipher/AEAD mode to require to protect communications in traffic management systems)
  - CFRG:
    - Protocol designers choosing mechanisms for their higher-level protocols (e.g., TLS) and parameters for those mechanisms
    - Implementers of cryptography needing guidance for secure implementations (e.g., how to avoid side-channel attacks, how to test their code for correctness using test vectors)

CFRG and ISO: differences and similarities

CFRG and ISO (ISO/IEC JTC 1/SC 27/WG 2 "Cryptography and Security Mechanisms")

- Maturity of mechanisms:
  - ISO: a mechanism has to be mature, standardized for 3 or more years on a national level
  - CFRG: you can (or even should) bring new mechanisms if they are well-studied and desired by practitioners
- Writing documents: MUSTs/MUST NOTs
  - ISO: an international standard must be an editorially flawless document.
  - CFRG: a CFRG RFC must not have any ambiguity regarding the secure usage of mechanisms

- Cryptography and security:
  - ISO, CFRG: the security of mechanisms must be thoroughly assessed
  - ISO, CFRG: the research papers dedicated to the standardized mechanisms must contain all necessary information for protocol designers to incorporate the mechanisms into their protocols (e.g., how to define the total number of re-keying operations to maximize the security of implementations of a certain application-specific protocol).

Future plans: 2023

Completed by CFRG, awaiting IRSG/IESG reviews and/or publication:

- Cryptographic primitives/modes/parameters:
  - *"The ristretto255 and decaf448 Groups"*
  - *"Hashing to Elliptic Curves"*
- PAKEs:
  - *"SPAKE2, a PAKE"* (no consensus boilerplate, not a result of the PAKE selection process)
- Signature schemes with specific properties:
  - *"RSA Blind Signatures"*
  - *"Two-Round Threshold Schnorr Signatures with FROST"*
- Protocols:
  - *"Verifiable Random Functions (VRFs)"*
  - *"Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups"*

Future plans: medium term work

- Cryptographic primitives/modes/parameters:
  - *“Pairing-Friendly Curves”*
  - *“KangarooTwelve and TurboSHAKE”*
  - *“The AEGIS family of authenticated encryption algorithms”*
  - *“Additional Parameter sets for LMS Hash-Based Signatures”*
- Short signature schemes based on pairings:
  - *“BLS Signature Scheme”*
  - *“The BBS Signature Scheme”*
- PAKEs:
  - *“CPace, a balanced composable PAKE”*
  - *“The OPAQUE Asymmetric PAKE Protocol”*

Future plans: medium term work

- Privacy-preserving protocols
  - *“Key Blinding for Signature Schemes”*
  - *“Verifiable Distributed Aggregation Functions”*
- Selection/usage of AEADs:
  - *“Usage Limits on AEAD Algorithms”*
  - *“Properties of AEAD algorithms”*
- Towards [even more] secure implementations:
  - *“Deterministic Nonce-less Hybrid Public Key Encryption”*
  - *“Deterministic ECDSA and EdDSA Signatures with Additional Randomness”*

Thank you!

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

cfrg-chairs@ietf.org