SPECIFYING CRYPTOGRAPHY FOR USE IN INTERNET PROTOCOLS

Current Efforts at the Crypto Forum Research Group
PRESENTATION HIGHLIGHTS

FOCUS AREAS
- Brief history of the CFRG
- How the IRTF and the IETF work
- Summary of published RFCs
- Relevant active work
- Lessons learned
- Summary
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.
BROAD GOALS

SPECIFICATION
Define/standardize crypto primitives for use by IETF and other SDOs (e.g. W3C)

CONNECTION
Meeting place for both academics (cryptographers) and practitioners (protocol designers and implementors).

EDUCATION
Cryptographic expertise for IETF WGs and ISE
2002
Original Chairs: Kevin Igoe, David McGrew

2013
Community backlash against NIST and NSA, “Requesting removal of CFRG co-chair” thread in December 2013 started by Trevor Perrin

2014-15

2016
Crypto Review Panel Established

2019-20
Nick Sullivan, Stanislav Smyshlyaev join Alexey Melnikov. PAKE protocol selection (selected CPace and OPAQUE)
IETF vs IRTF

The IETF is an organization that develops and maintains Internet standards through the publication of Internet Engineering Task Force (IETF) RFCs. The IRTF, on the other hand, is a part of the Internet Society (ISOC) that focuses on research and experimentation in the domain of networking technologies.
CFRG FEEDS INTO IETF WORK

- Security Area WGs: TLS, MLS, IPSECME, LAMPS, etc.
- New mechanisms (VOPRF, HPKE, PAKEs) are developed taking into account needs of IETF WGs

SPECIFIC REQUESTS FROM IETF

- What is the key lifetime boundary for a particular cryptographic mode of operation?
- Which elliptic curves/PAKEs should we use in TLS/IPsec/etc.?

CRYPTO REVIEW PANEL

- Academics and applied security experts
- Reviews of CFRG documents, proposals during contests, other IETF documents
- Currently 11 members, appointed for 2 years term ending in December 2023
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.
PATH TO RFC

ADOPTION -> ACTIVE -> PANEL -> RGLC -> IRTF CHAIR -> IESG/RFC EDITOR

Versions:

- draft-barnes-cfg-hpke
  - 00 01
- draft-irtf-cfg-hpke
  - 00 02 04 05 06 07 08 09 10 11 12
- RFC 9180
- rfc9180

Date: Jul. 25, 2023
Selected Publications

- RFC 7664, “Dragonfly Key Exchange”, 2015-11
- 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 9180, “Hybrid Public Key Encryption“, 2022-02
Protocol designers choosing mechanisms for their higher-level protocols
Implementers of cryptography needing guidance

You can bring new mechanisms if they are well-studied and desired by practitioners

A mechanism has to be mature, standardized for 3 or more years on a national level

A CFRG RFC must not have any ambiguity regarding the secure usage of mechanisms
An international standard must be flawless as a document
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”
Relevant Active Work

Zero-knowledge Proofs
- Pairing-Friendly Curves
- The BBS Signature Scheme

Threshold Cryptography
- Two-Round Threshold Schnorr Signatures with FROST

Multi-party Computation
- Verifiable Distributed Aggregation Functions
## Zero-Knowledge Proofs

### Pairing-Friendly Curves

1. **Security Concerns:** Recent algorithmic advancements (exTNFS) pose threats to certain pairing-friendly curves.
2. **Curve Classification:** Curves classified and recommended based on security levels (128-bit, 192-bit, 256-bit).
3. **Comprehensive Guide:** Document serves as a detailed guide on applications, security, and recent attacks on pairing-friendly curves.

### BBS Signatures

1. A unique digital signature scheme that allows signing multiple messages with a single output signature.
2. **Selective Disclosure:** Disclose subsets of the originally signed set of messages, preserving their authenticity and integrity.
3. **Proof of Possession:** Allows the generation of proofs that demonstrate possession of a signature.
4. **Unlinkable Proofs:** The generated proofs are zero-knowledge.
5. **Application to the JWP effort in the JOSE working group**
FEATURES

1. Threshold Cooperation: Signatures can be issued after a threshold number of entities cooperate to compute a signature.

2. Compatibility with Existing Curves: Can produce signatures compatible with Edwards-Curve Digital Signature Algorithm (EdDSA) variants Ed25519 and Ed448, allowing verification with an RFC8032 compliant verifier.

3. Non-Deterministic Signatures: Unlike EdDSA, the signatures produced by FROST are not deterministic, providing protection against key-recovery attacks in multi-party settings.
MULTI-PARTY COMPUTATION FOR DATA AGGREGATION

1. A family of multi-party protocols for computing aggregate statistics over user measurements while ensuring privacy.

2. Privacy and Robustness: As long as one server executes the protocol honestly, individual measurements are never seen by any server in the clear. VDAFs also allow servers to detect and remove malformed inputs that would result in incorrect aggregate results.

3. Compatibility with Differential Privacy: VDAFs can be composed with various mechanisms for differential privacy, providing assurance that the aggregate result does not leak too much information about any one measurement.

4. Central piece of work at the the PPM working group
Lessons Learned and Adaptations to Challenges

Speed of specification is a pain point for some

Inconsistent review quality for different aspects of specifications

Cultural expectations regarding mailing list engagement
SPECIFYING CRYPTOGRAPHY FOR USE IN INTERNET PROTOCOLS

Current Efforts at the Crypto Forum Research Group