NIST STPPA6 · JUL. 25, 2023

NIST STPPA6 · JUL. 25, 2023

NIST STPPA6 · JUL. 25, 2023

SPECIFYING CRYPTOGRAPHY FOR USE IN INTERNET PROTOCOLS

Current Efforts at the Crypto Forum Research Group

NIST STPPA6

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

CRYPTO FORUM RESEARCH GROUP

TIMELINE

2002 Original Chairs: Kevin Igoe, David McGrew

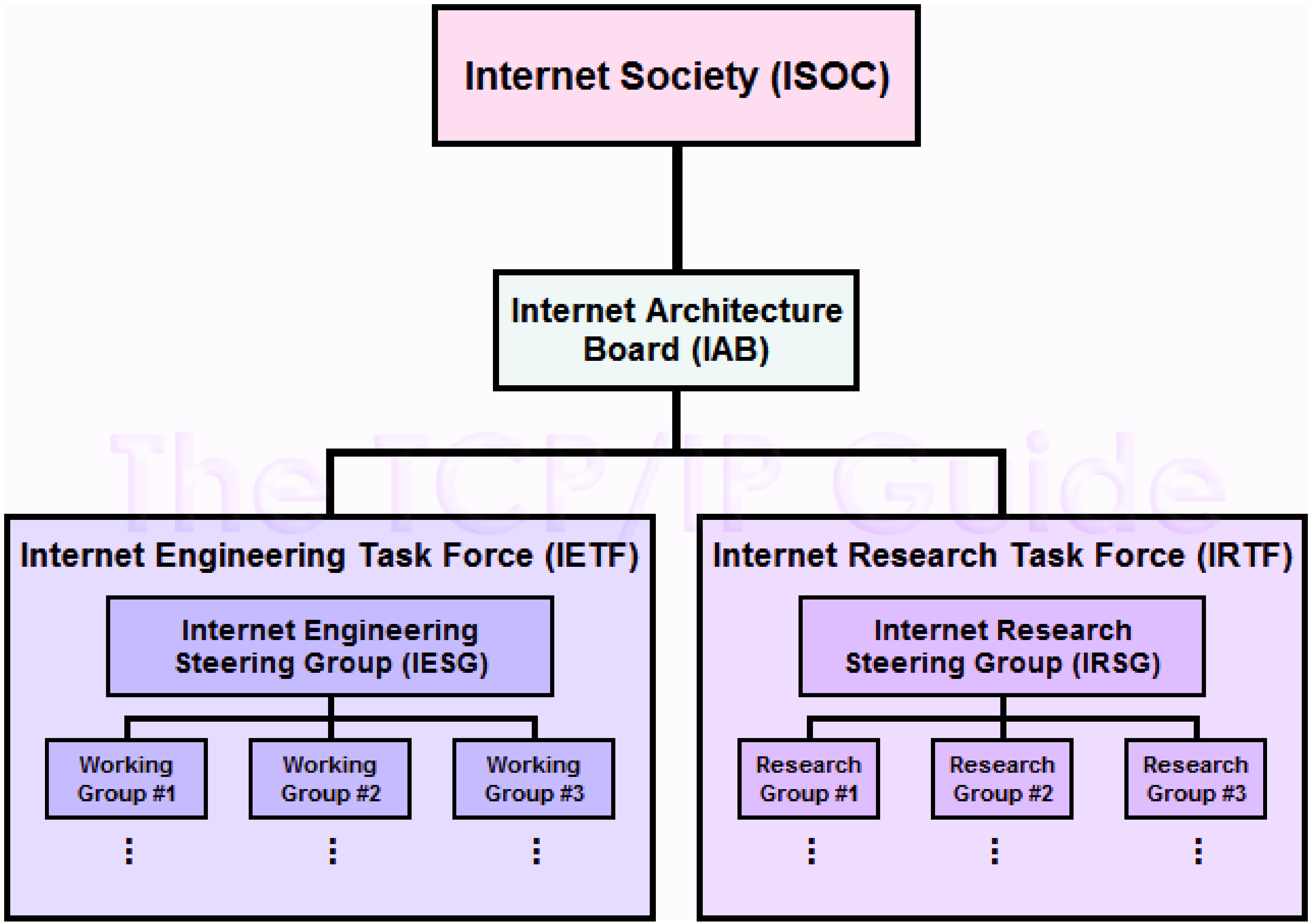
2013 Community backlash against NIST and NSA, “Requesting removal of CFRG co-chair” thread in December 2013 started by Trevor Perrin

2014-15 Kenny Paterson and Alexey Melnikov selected as chairs. Elliptic curves selection: 2014-2015. Resulted in RFC 7748, selected Curve25519 and Curve448, now widely used in practice.

2016 Crypto Review Panel Established

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

IETF vs IRTF



Internet Society (ISOC)

Internet Architecture Board (IAB)

Internet Engineering Task Force (IETF)

Internet Engineering Steering Group (IESG)

Working Group #1 ⋮

Working Group #2 ⋮

Working Group #3 ⋮

Internet Research Task Force (IRTF)

Internet Research Steering Group (IRSG)

Research Group #1 ⋮

Research Group #2 ⋮

Research Group #3 ⋮

CFRG AND IETF

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

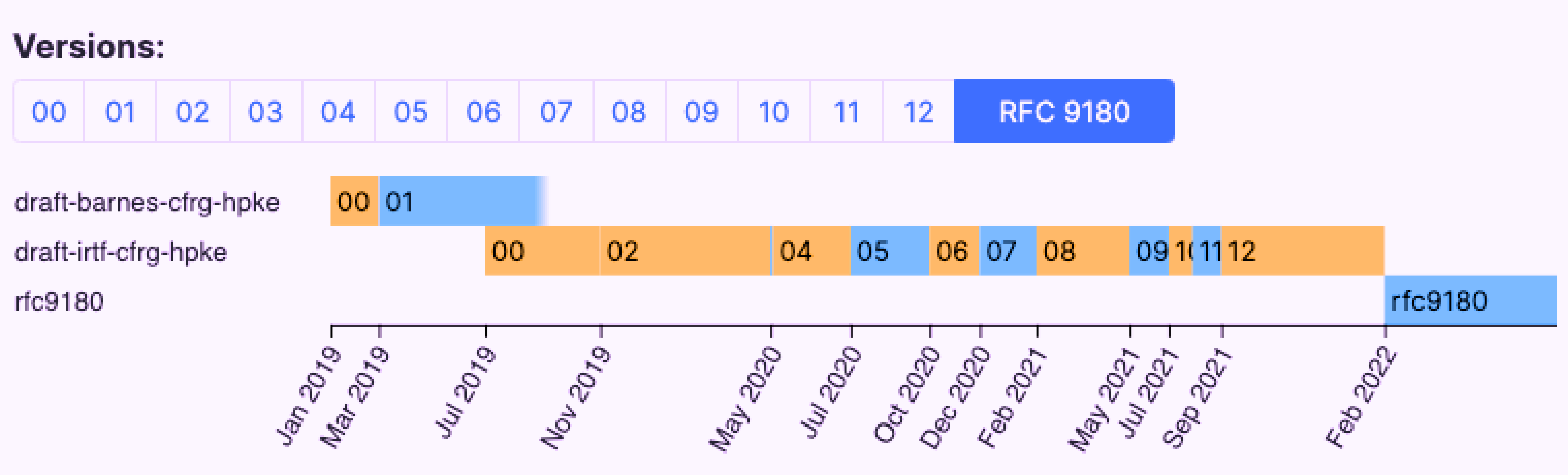
CFRG AND RESEARCH

CFRG WORK INSPIRED BY RESEARCH PAPERS

- 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



Selected Publications

- 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

AUDIENCES

- Protocol designers choosing mechanisms for their higher-level protocols
- Implementers of cryptography needing guidance

MATURITY

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

WRITING DOCUMENTS

- A CFRG RFC must not have any ambiguity regarding the secure usage of mechanisms

ISO

AUDIENCES

- Regulatory bodies
- Industry-specific bodies (including SDOs) choosing which mechanisms to require

MATURITY

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

WRITING DOCUMENTS

- An international standard must be flawless as a document

Pending Publications

- 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

FROST TWO-ROUND THRESHOLD SCHNORR SIGNATURES

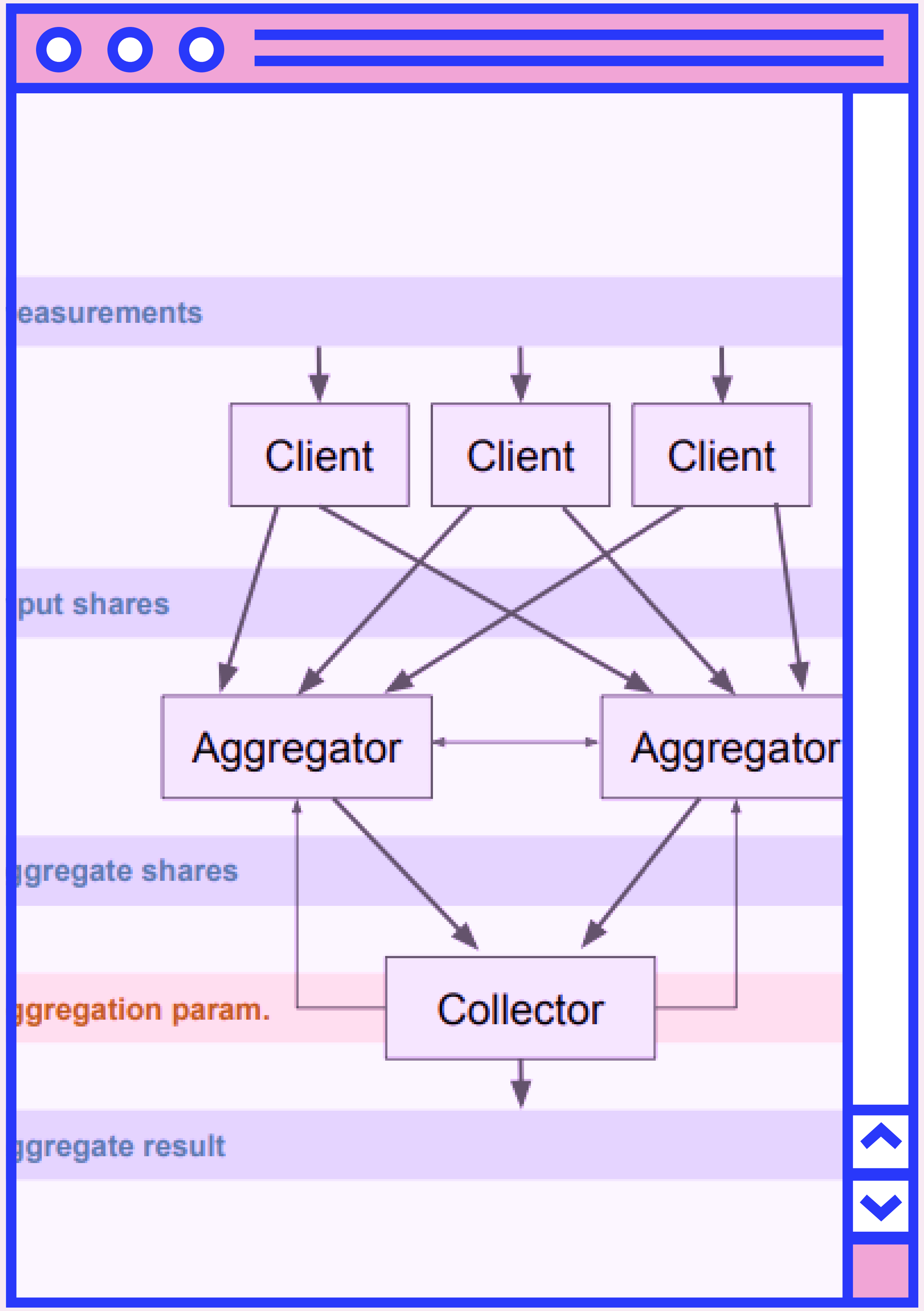
FEATURES

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.

VDAFs VERIFIABLE DISTRIBUTED AGGREGATION FUNCTIONS

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

NIST STPPA6 • JUL. 25, 2023

NIST STPPA6 • JUL. 25, 2023

NIST STPPA6 • JUL. 25, 2023

NIST STPPA6

SPECIFYING CRYPTOGRAPHY FOR USE IN INTERNET PROTOCOLS

Current Efforts at the Crypto Forum Research Group