VOPRF  POPRF

draft-irtf-cfrg-voprf

Davidson, Faz-Hernandez, Sullivan, Wood — IETF 112 Online— CFRG
Updates
Draft -08

Major
• 2HashDH OPRF to 3HashSDHI POPRF

Minor
• Update P-384 suite to use SHA-384 instead of SHA-512
• Update test vectors and improve editorial clarity
Functionality Differences

POPRF Update

\[ y = F(k, x, t) \]
Functionality Differences

POPRF Update

\[ y = F(k, x, t) \]

- Server private key
- Shared public input
- PRF output
- Client private input
Functionality Differences

POPRF Update

\[ y = F(k, x, t) \]

- Server private key
- Shared public input
- PRF output
- Client private input
Functionality Differences

POPRF Update

\[ y = F(k, x, t) \]

- Server private key
- Shared public input
- PRF output
- Client private input
Functionality Differences

POPRF Update

\[ y = F(k, x, \perp ) \approx F(k, x) \]

POPRF with fixed public input is functionally an OPRF
Security Differences

POPRF Update

Formal security differences:

• 3HashSDHI has game-based security definition with reductions to q-DL in the AGM, not (yet) a proof that it satisfies the UC formalization from Jarecki et al.

• Identical security parameters for Cheon static-DH attack (best known complexity)
Security Differences

POPRF Update

Formal security differences:

- 3HashSDHI has game-based security definition with reductions to q-DL in the AGM, not (yet) a proof that it satisfies the UC formalization from Jarecki et al.

- Identical security parameters for Cheon static-DH attack (best known complexity)

**High-level point:** Confidence in both 2HashDH and 3HashSDHI, but formal differences may have implications for dependent applications (OPAQUE)

**Open issue:** UC analysis for 3HashSDHI POPRF (compatible with 2018/733)
Deployment Differences
POPRF Update

2HashDH is threshold-friendly: servers can secret share the private key and non-interactively run the protocol transparently to the client.

3HashSDHI is not threshold friendly: threshold implementation may require interactive, multi-round protocol between clients and servers.
Open Questions

Threshold-friendly OPRFs

What current use cases require threshold-friendly OPRFs, and should this be specified functionality?
Open Questions
Threshold-friendly OPRFs

What current use cases require threshold-friendly OPRFs, and should this be specified functionality?

If no, then only specify 3HashSDHI since it’s a generalization of 2HashDH
Open Questions

Threshold-friendly OPRFs

What current use cases require threshold-friendly OPRFs, and should this be specified functionality?

If yes, then more questions:

Should we specify both 2HashDH and 3HashSDHI protocols?

Should these be separate cryptographic objects with distinct APIs?

What do we do about distributed key generation? (See FROST)