draft-irtf-cfrg-cpace

Michel Abdalla, Björn Haase, Julia Hesse

Status IETF 111, July 2021

Previous status update

Paper available online:
https://eprint.iacr.org/2021/114

Results in a nutshell

- CPace protocol variants in current draft provide strong security guarantees:
    - Composability & adaptive security under sSDH (DDH-type assumption)
    - Map2Point security analyzed without random oracles
        - security-relevant properties are fulfilled by Hash2Curve maps
    - CPace using Ristretto 25519 secure as well
    - Cofactor does not impact security
- Establishment of unique session identifiers is required for composability guarantees

Recent updates

Paper currently under submission to ASIACRYPT 2021

Latest updates

- RFC mostly unchanged
- Refined security analysis of CPace protocol variants in the associated paper
    - Clarification of security definitions and proofs
    - Improved readability
- Clarified role of unique session identifiers (SIDs)
    - Unique SIDs are required for composability guarantees
    - SID needs to be added to all hash function inputs
    - SID needs to be established before running CPace

Session identifiers in practice

Users can agree on a joint session identifier

- Both users should contribute randomness to the SID
- Party identifiers should be incorporated in the SID
- Agreement does not require secrecy
- Can potentially be piggy-backed to messages sent by the application

Next steps

▶ Provide a game-based security analysis without SIDs

Objective: Provide security guarantees when unique SIDs are not available

Security guarantees would be similar to that of non-UC protocols

- Weak forward security
- Perfect forward security when adding key confirmation
- Underlying security assumptions would remain unchanged

▶ Incorporate changes into the RFC