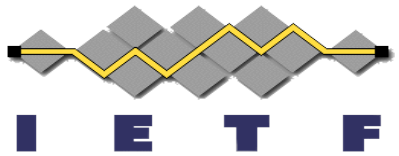
Barreto-Lynn-Scott Elliptic Curve Key Representations for JOSE and COSE

draft-ietf-cose-bls-key-representations

Tobias Looker and Mike Jones

IETF 119, Brisbane

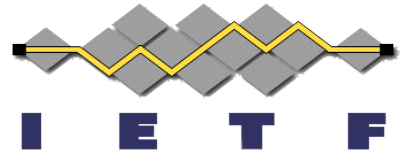
March 19, 2024



Developments Since IETF 118

- Changed to use key type “EC” for JOSE and equivalent “EC2” for COSE for uncompressed key representations
- Changed identifier spellings from “Bls” to “BLS”, since these letters are people’s initials

Compressed Key Representations



- We currently define only uncompressed key representations for JOSE and COSE
- draft-irtf-cfrg-pairing-friendly-curves (which is expired) defines a compressed representation, but it is bespoke to these curves
  - As opposed to being parallel to other “OKP” representations
  - Bespoke serialization based on ZCash implementation
- Do we want to also define a compressed key representation?
  - And if so, do we want to use the bespoke one or a more normal one?

Discussion

- Your input on the draft?