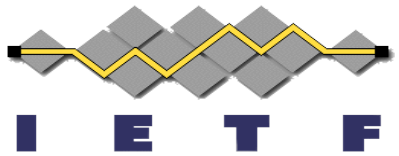
Barreto-Lynn-Scott Elliptic Curve Key Representations for JOSE and COSE



draft-ietf-cose-bls-key-representations

Tobias Looker & Mike Jones

IETF 116, Yokohama

March 27, 2023

What Does It Do?

- Defines and registers required parameters with IANA for cryptographic key representation of the Barreto-Lynn-Scott Elliptic curve family in both COSE_Key and JWK

Why Do It?

- Multiple new algorithms emerging that make use of this curve
  - BLS signatures, CFRG draft
  - The BBS signature scheme, CFRG draft (draft 02 recently published)

Status

- Simple draft primarily registering parameters
- Adopted by working group in July 2022
- Published –02 recently which:
  - Updated JWK based examples
  - Added COSE_Key based examples
  - Shifted to uncompressed public key representations

Question

Compressed or Uncompressed public key representation

Currently the predominant point encoding (used for public keys) is a compressed format defined by ZCash, which is referenced in Appendix C of draft-irtf-frg-pairing-friendly-curves[1] However this encoding is curve specific to BLS12381 rather than generalized. There is no other known compressed point encoding methods for the BLS curves that is currently used.

[1] https://www.ietf.org/archive/id/draft-irtf-cfrg-pairing-friendly-curves-11.html

Option 1

Uncompressed public key representation

- Change kty from OKP -> EC.
- Public key representation will require both the x and y co-ordinates in an ”uncompressed form”.
- Pro: Easy to define follows largely the guidance around elliptic curve public keys.
- Con: Less efficient public key representation.

Option 2

Compressed public key representation

- Keep kty from OKP -> EC.
- Define a suitable point encoding method that is generic to the curve, perhaps based upon [1] or [2].
- Public key representation in JOSE and COSE would have the compressed point expressed in the x parameter.
- Pro: Much more size efficient public key.
- Con: More complex to define, a new point encoding method.

[1] https://www.secg.org/sec1-v2.pdf
[2] https://datatracker.ietf.org/doc/html/draft-ietf-lwig-curve-representations-23