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

draft-looker-cose-bls-key-representations

Tobias Looker & Mike Jones
IETF 113, Vienna
March 21, 2022
Barreto-Lynn-Scott (BLS) elliptic curves belong to the pairing-friendly curves branch of cryptography.


In reference to pairing friendly curves, the BLS family is regarded by many as the most secure and efficient curves available for pairing-based operations.

This draft registers identifiers for BLS-based cryptographic keys in both JWK and COSE_Key formats.
Why

- There are numerous applications for pairing-based cryptography, however the most relevant and recent work includes:

- Standardizing the key representations for the BLS curves will help to support these initiatives.

- Ongoing work with JSON Web Proof (JWP) will provide the basis for JOSE-based expression of signature schemes like BBS signatures, meaning a way to express the keys in a manner consistent with JOSE (e.g., via JWK) becomes valuable.
Next Steps

- The authors request working group review of the document.
- Following addressing working group review comments, we plan to request working group adoption.