Workgroup: COSE
Internet-Draft:
draft-ietf-cose-bls-key-representations-00
Published: 8 July 2022
Intended Status: Standards Track
Expires: 9 January 2023
Authors: T. Looker M. Jones
Mattr Microsoft

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

Abstract

This specification defines how to represent cryptographic keys for the pairing-friendly elliptic curves known as Barreto-Lynn-Scott (BLS), for use with the key representation formats of JSON Web Key (JWK) and COSE (COSE_Key).

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/tplooker/draft-ietf-cose-bls-key-representations.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 9 January 2023.

Copyright Notice

Table of Contents

1. Introduction

This specification defines how to represent cryptographic keys for the pairing-friendly elliptic curves known as Barreto-Lynn-Scott [BLS], for use with the key representation formats of JSON Web Key (JWK) and COSE_Key. This specification registers the elliptic curves in appropriate IANA JOSE and COSE registries.

There are a variety of applications for pairing based cryptography including schemes already published as RFCs, such as Identity-Based Cryptography [RFC5091] Sakai-Kasahara Key Encryption (SAKKE) [RFC6508], and Identity-Based Authenticated Key Exchange (IBAKE) [RFC6539]. SAKKE is applied to Multimedia Internet KEYing (MIKEY) [RFC6509].

This branch of cryptography has also been used to develop privacy-preserving cryptographic hardware attestations schemes, including the Elliptic Curve Direct Anonymous Attestation (ECDAA) in the Trusted Platform Modules [TPM] specified by the Trusted Computing Group. Further work on similar schemes has also occurred at the FIDO Alliance [ECDAA]. Similarly, Intel released [EPID] which provides a solution to remote hardware attestation for Intel Software Guard Extension (SGX) enabled environments.

More recently, applications of pairing based cryptography using the Barreto-Lynn-Scott curves include the standardization effort for BLS Signatures [id.draft.bls-signature-04], which are used extensively in multiple blockchain projects due to their unique signature aggregation properties, including [Ethereum] [DFINITY] [Algorand]. Additionally, efforts are under way to standardize the general purpose short group signature scheme of BBS Signatures [BBS], which features novel properties such as multi-message signing and selective disclosure alongside zero knowledge proving. It is intended that this draft will help with these efforts by standardizing the associated cryptographic key representation in the popular formats of JWK and COSE_Key.

Other relevant work to this draft includes [JWP] which is extending the JOSE family of specifications to provide support for representing a variety of new proof based cryptographic schemes such as [BBS] which as referred to above uses the Barreto-Lynn-Scott curves.

There are multiple different pairing-friendly curves in active use; however, this draft focuses on a definition for the Barreto-Lynn-Scott curves due to them being the most "widely used" and "efficient" whilst achieving 128-bit and 256-bit security (BLS12-381 and BLS48-581 respectively).

More extensive discussion on the broader application of pairing based cryptography and the assessment of various elliptic curves (including the BLS family) can be found in [id.draft.pairing-friendly-curves-10].

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Representation Definition

The following definitions apply to the pairing-friendly elliptic curves known as the Barreto-Lynn-Scott (BLS) curves.

2.1.1. JSON Web Key Representation

When expressing a cryptographic key for these curves in JSON Web Key (JWK) form, the following rules apply:

*The parameter "kty" MUST be present and set to "OKP".

*The parameter "crv" MUST be present and value MUST be one defined in Section 2.1.3.

*The parameter "x" MUST be present whose value represents the curve point for the public key. This value MUST be encoded using the serialization defined in [id.draft.pairing-friendly-curves-10] Appendix C and MUST be base64url encoded without padding as defined in [RFC7515] Appendix C.

*The parameter "d" MUST be present for private key representations whose value MUST contain the little-endian representation of the private key base64url encoded without padding as defined in [RFC7515] Appendix C. This parameter MUST NOT be present for public keys.

2.1.2. COSE_Key Representation

When expressing a cryptographic key for these curves in COSE_Key form, the following rules apply:

*The parameter "kty" (1) MUST be present and set to "OKP" (1).

*The parameter "crv" (-1) MUST be present and value MUST be one defined in Section 2.1.3.

*The parameter "x" (-2) MUST be present whose value represents the curve point for the public key. This value MUST be encoded using the serialization defined in [id.draft.pairing-friendly-curves-10] Appendix C.

*The parameter "d" (-4) MUST be present for private key representations whose value MUST contain the little-endian representation of the private key. This parameter MUST NOT be present for public keys.

2.1.3. Curve Parameter Registration

JWK "crv" value	COSE_Key "crv" value	Description
Bls12381G1	TBD (13 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 12 with 381-bit p in the subgroup of G1 defined as E(GF(p)) of order r
Bls12381G2	TBD (14 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 12 with 381-bit p in the subgroup of G1 defined as E(GF(p^2)) of order r
Bls48581G1	TBD (15 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding

JWK "crv" value	COSE_Key "crv" value	Description
		degree 48 with 581-bit p in the subgroup of G1 defined as E(GF(p)) of order r
Bls48581G2	TBD (16 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 48 with 581-bit p in the subgroup of G1 defined as E(GF(p^8)) of order r

Table 1

3. Security Considerations

See [id.draft.pairing-friendly-curves-10] for additional details on security considerations for the curves used. Implementers should also consider the general guidance provided in Section 9 of [RFC7517] and Section 17 of [RFC8152] when using this specification.

Furthermore, because this specification only defines the cryptographic key representations and not the usage of these keys with specific algorithms, implementers should be aware to follow any guidance that may be provided around appropriate usage of the keys and or additional steps that may be required to validate the keys within the context of particular algorithms.

4. IANA Considerations

4.1. JSON Web Key (JWK) Elliptic Curve Registrations

This section registers the following values in the IANA "JSON Web Key Elliptic Curve" registry [IANA.JOSE.Curves].

Bls12381G1

- *Curve Name: Bls12381G1
- *Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))
- *JOSE Implementation Requirements: Optional
- *Change Controller: IESG
- *Specification Document(s): Section 2.1.1

Bls12381G2

- *Curve Name: Bls12381G2

*Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^2))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.1

Bls48581G1

*Curve Name: Bls48581G1

*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.1

Bls48581G2

*Curve Name: Bls48581G2

*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^8))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.1

4.2. COSE Elliptic Curve Registrations

This section registers the following value in the IANA "COSE Elliptic Curves" registry [IANA.COSE.Curves].

Bls12381G1

*Curve Name: Bls12381G1

*Value: TBD (13 requested)

*Key Type: OKP

*Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.2

*Recommended: Yes

Bls12381G2

*Curve Name: Bls12381G2

*Value: TBD (14 requested)

*Key Type: OKP

*Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^2))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.2

*Recommended: Yes

Bls48581G1

*Curve Name: Bls48581G1

*Value: TBD (15 requested)

*Key Type: OKP

*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.2

*Recommended: Yes

Bls48581G2

*Curve Name: Bls48581G2

*Value: TBD (16 requested)

*Key Type: OKP

*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^8))

*JOSE Implementation Requirements: Optional

*Change Controller: IESG

*Specification Document(s): Section 2.1.2

*Recommended: Yes

5. Normative References

[BLS] Barreto, P., Lynn, B., and M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees", 2003.

[IANA.COSE.Curves] IANA, "COSE Elliptic Curves", <https://www.iana.org/assignments/cose/cose.xhtml#elliptic-curves>.

[IANA.JOSE.Curves] IANA, "JOSE Elliptic Curves", <https://www.iana.org/assignments/jose/jose.xhtml#web-key-elliptic-curve>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[id.draft.bls-signature-04] IETF CFRG, "BLS Signature", <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-bls-signature-04>.

[id.draft.pairing-friendly-curves-10] IETF CFRG, "Pairing-Friendly Curves", <https://www.ietf.org/archive/id/draft-irtf-cfrg-pairing-friendly-curves-10.html>.

6. Informative References

[BBS] Decentralized Identity Foundation, "The BBS Signature Scheme", <https://identity.foundation/bbs-signature/draft-bbs-signatures.html>.

[ECDAA] FIDO Alliance, "ECDAA Algorithm", 2018, <https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html>.

[EPID] Intel Corporation, "Intel (R) SGX: Intel (R) EPID Provisioning and Attestation Services", <https://software.intel.com/en-us/download/intel-sgx-intel-epid-provisioning-and-attestation-services>.

[JWP] Miller, J. and M. Jones, "JSON Web Proof", <https://json-web-proofs.github.io/json-web-proofs/draft-jmiller-json-proof-algorithms.html#name-bls-curve>.

[RFC5091] Boyen, X. and L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, DOI 10.17487/

RFC5091, December 2007, <https://www.rfc-editor.org/info/rfc5091>.

[RFC6508] Groves, M., "Sakai-Kasahara Key Encryption (SAKKE)", RFC 6508, DOI 10.17487/RFC6508, February 2012, <https://www.rfc-editor.org/info/rfc6508>.

[RFC6509] Groves, M., "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)", RFC 6509, DOI 10.17487/RFC6509, February 2012, <https://www.rfc-editor.org/info/rfc6509>.

[RFC6539] Cakulev, V., Sundaram, G., and I. Broustis, "IBAKE: Identity-Based Authenticated Key Exchange", RFC 6539, DOI 10.17487/RFC6539, March 2012, <https://www.rfc-editor.org/info/rfc6539>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TPM] Trusted Computing Group, "Trusted Platform Module", <https://trustedcomputinggroup.org/>.

Appendix A. Acknowledgments

The authors would like to acknowledge the work of Kyle Den Hartog, which was used as the foundation for this draft.

Appendix B. Document History

-00

*Created draft-ietf-cose-bls-key-representations-00 from draft-looker-cose-bls-key-representations-00 following working group adoption.

Authors' Addresses

Tobias Looker
Mattr

Email: tobias.looker@mattr.global

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: https://self-issued.info/