CBOR Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 15 April 2026

M. Prorock
mesur.io
O. Steele
Tradeverifyd
H. Tschofenig
H-BRS

12 October 2025

FN-DSA for JOSE and COSE
draft-ietf-cose-falcon-03

Abstract

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 206 (expected to be published in late 2026 early 2027).

It does not define new cryptographic primitives; rather, it specifies how existing FN-DSA mechanisms are serialized for use in JOSE and COSE. This document registers signature algorithms for JOSE and COSE, specifically FN-DSA-512 and FN-DSA-1024.

About This Document

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

The latest revision of this draft can be found at https://cose-wg.github.io/draft-ietf-cose-falcon/draft-ietf-cose-falcon.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-cose-falcon/.

Discussion of this document takes place on the CBOR Object Signing and Encryption Working Group mailing list (mailto:cose@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/cose/. Subscribe at https://www.ietf.org/mailman/listinfo/cose/.

Source for this draft and an issue tracker can be found at https://github.com/cose-wg/draft-ietf-cose-falcon.

Status of This Memo

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

Copyright Notice

Table of Contents

1. Introduction

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 206 (expected to be published in late 2026 early 2027).

FN-DSA (formerly known as Falcon) is a lattice-based digital signature scheme based on the GPV hash-and-sign framework [GPV08], instantiated over NTRU lattices with fast Fourier sampling techniques [DP16]. The core hard problem underlying FN-DSA is the SIS (Short Integer Solution) problem over NTRU lattices.

FN-DSA (formerly known as Falcon) is a digital signature algorithm based on lattice mathematics. It follows the hash-and-sign design introduced by Gentry, Peikert, and Vaikuntanathan [GPV08]. FN-DSA operates on NTRU lattices and uses fast Fourier techniques [DP16] to make signature generation compact and efficient. The security of the scheme relies on the hardness of solving certain lattice problems, in particular the Short Integer Solution (SIS) problem.

FN-DSA offers:

* Post-quantum security under the assumption that NTRU-SIS remains hard.

* Compactness in key and signature size.

* Efficient operations (roughly O(n log n)).

* A requirement for careful implementation to avoid side-channel leakage (notably Gaussian sampling must be constant-time where applicable).

The sizes of public key, private key, and signature for the parameter sets are the same as in the original Falcon specification:

Parameter Set	Signature size (bytes)	Public Key size (bytes)	Private Key size (bytes)
FN-DSA-512	666	897	1281
FN-DSA-1024	1280	1793	2305

Table 1

For a detailed comparison of FN-DSA with ML-DSA [USNIST.FIPS.204] and SLH-DSA [USNIST.FIPS.205] see Section 11.3 of [I-D.draft-ietf-pquip-pqc-engineers].

This document defines how FN-DSA is used with JSON Object Signing and Encryption (JOSE) [RFC7515] and CBOR Object Signing and Encryption (COSE) [RFC9052] [RFC9053].

2. Terminology

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.

3. The FN-DSA Algorithm Family

The FN-DSA Signature Scheme is parameterized to support different security levels.

This document introduces the registration of the following algorithms in [IANA.jose]:

Name	alg	Description
FN-DSA-512	FN-DSA-512	FN-DSA with parameter set 512
FN-DSA-1024	FN-DSA-1024	FN-DSA with parameter set 1024

Table 2: JOSE Algorithms for FN-DSA

This document introduces the registration of the following algorithms in [IANA.cose]:

Name	alg	Description
FN-DSA-512	TBD1 (-54)	CBOR Object Signing Algorithm for FALCON512
FN-DSA-1024	TBD2 (-55)	CBOR Object Signing Algorithm for FALCON1024

Table 3: COSE Algorithms for FN-DSA

4. FN-DSA Keys

The FN-DSA Algorithm Family uses the Algorithm Key Pair (AKP) key type, as defined in [I-D.draft-ietf-cose-dilithium].

The specific algorithms for FN-DSA, such as FALCON512 and FALCON1024, are defined in this document and are used in the alg value of an AKP key representation to specify the corresponding algorithm.

Thumbprints for FN-DSA keys are computed according to the process described in [I-D.draft-ietf-cose-dilithium].

5. Security Considerations

The security considerations of [RFC7515], [RFC7517] and [RFC9053] apply to this specification as well.

A detailed security analysis of FN-DSA is beyond the scope of this specification; see [USNIST.FIPS.206] for additional details.

All the usual caveats for PQC and side-channel resistance apply.

* Implementations MUST ensure that alg matches the intended algorithm variant.

* Private implementations of sampling (Gaussian, etc.) must be constant-time to prevent leakage.

* Public keys SHOULD be validated before use (e.g., against encoding constraints).

* Nonces, random values, blinding factors (if used) MUST originate from a secure source of randomness.

5.1. Validating Public Keys

TODO

5.2. Side-Channel Attacks

Implementers should follow best practices to mitigate timing, cache, and power side channels, such as:

* Using constant-time arithmetic
* Maintaining uniform memory access patterns
* Avoiding data-dependent branching or memory indexing

5.3. Randomness Considerations

All required randomness (e.g. for signature generation) MUST be derived from a cryptographically secure, high-entropy source.

6. IANA Considerations

6.1. New COSE Algorithms

IANA is requested to add the following entries to the COSE Algorithms Registry. The following completed registration templates are provided as described in [RFC9053] and [RFC9054].

6.1.1. FN-DSA-512

* Name: FN-DSA-512
* Value: TBD1 (requested assignment -54)
* Description: CBOR Object Signing Algorithm for FALCON512
* Capabilities: [kty]
* Change Controller: IETF
* Reference: RFC XXXX
* Recommended: Yes

6.1.2. FN-DSA-1024

* Name: FN-DSA-1024

* Value: TBD2 (requested assignment -55)

* Description: CBOR Object Signing Algorithm for FALCON1024

* Capabilities: [kty]

* Change Controller: IETF

* Reference: RFC XXXX

* Recommended: Yes

6.2. New JOSE Algorithms

IANA is requested to add the following entries to the JSON Web Signature and Encryption Algorithms Registry. The following completed registration templates are provided as described in [RFC7518].

6.2.1. FN-DSA-512

* Algorithm Name: FN-DSA-512

* Algorithm Description: FN-DSA-512 as described in US NIST FIPS 206.

* Algorithm Usage Location(s): alg

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): RFC XXXX

* Algorithm Analysis Documents(s): [USNIST.FIPS.206]

6.2.2. FN-DSA-1024

* Algorithm Name: FN-DSA-1024

* Algorithm Description: FN-DSA-1024 as described in US NIST FIPS 206.

* Algorithm Usage Location(s): alg

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): RFC XXXX

* Algorithm Analysis Documents(s): [USNIST.FIPS.206]

7. References

7.1. Normative References

[I-D.draft-ietf-cose-dilithium]
Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-09, 12 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-09>.

[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/rfc/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/rfc/rfc7515>.

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

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/rfc/rfc7518>.

[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/rfc/rfc8174>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[RFC9054] Schaad, J., "CBOR Object Signing and Encryption (COSE): Hash Algorithms", RFC 9054, DOI 10.17487/RFC9054, August 2022, <https://www.rfc-editor.org/rfc/rfc9054>.

[USNIST.FIPS.206]
"Fast Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm", n.d., <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

7.2. Informative References

[DP16] Ducas, L. and T. Prest, "Fast Fourier Orthogonalization", Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC '16), pp. 191198 , 2016, <https://doi.org/10.1145/2930889.2930923>.

[GPV08] Gentry, C., Peikert, C., and V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions", Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08), pp. 197206 , 2008, <https://doi.org/10.1145/1374376.1374407>.

[I-D.draft-ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[IANA.cose]
IANA, "CBOR Object Signing and Encryption (COSE)", <https://www.iana.org/assignments/cose>.

[IANA.jose]
IANA, "JSON Object Signing and Encryption (JOSE)", <https://www.iana.org/assignments/jose>.

[USNIST.FIPS.204]
"Module-Lattice-Based Digital Signature Standard", n.d., <https://doi.org/10.6028/NIST.FIPS.204>.

[USNIST.FIPS.205]
"Stateless Hash-Based Digital Signature Standard", n.d., <https://doi.org/10.6028/NIST.FIPS.205>.

Appendix A. Examples

A.1. JOSE

A.1.1. Key Pair

```
{
  "kty": "AKP",
  "alg": "FN-DSA-512",
  "pub": "V53SIdVF...uvw2nuCQ",
  "priv": "V53SIdVF...cDKLbsBY"
}
```

Figure 1: Example FN-DSA-512 Private JSON Web Key

```
{
  "kty": "AKP",
  "alg": "FN-DSA-512",
  "pub": "V53SIdVF...uvw2nuCQ"
}
```

Figure 2: Example FN-DSA-512 Public JSON Web Key

A.1.2. JSON Web Signature

```
{
  "kid: "clpwZ...RWYU9CUF",
  "alg": "FN-DSA-512",
  "typ": "JWT"
}
```

Figure 3: Example FN-DSA-512 Decoded Protected Header for a JSON Web Signature

A.2. COSE

A.2.1. Key Pair

```
{
  / kty AKP        / 1: 7,
  / alg FN-DSA-512 / 3: -54,
  / public key     / -1: h'7803c0f9...3f6e2c70',
  / private key    / -2: h'7803c0f9...3bba7abd'
}
```

Figure 4: Example FN-DSA-512 Private COSE Key

```
{
  / kty AKP         / 1: 7,
  / alg FN-DSA-512  / 3: -54,
  / public key      / -1: h'7803c0f9...3f6e2c70',
}
```

Figure 5: Example FN-DSA-512 Public COSE Key

A.2.2. COSE Sign1

```
18([
  <<{
    / alg FN-DSA-512 / 1: -54,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature / h'53e855e8...0f263549'
])
```

Figure 6: Example FN-DSA-512 COSE Sign1

Appendix B. Document History

-02

* Converted to markdown
* Applied feedback from IESG Evaluation on ML-DSA
* Revised references
* Revised abstract

-01

* Added Acknowledgements
* Added Document History
* Updated test vectors

Acknowledgments

We would like to especially thank David Balenson for careful review of approaches taken in this document. We would also like to thank Michael B. Jones for guidance in authoring.

Contributors

Rafael Misoczki
Google
Email: rafaelmisoczki@google.com

Michael Osborne
IBM
Email: osb@zurich.ibm.com

Christine Cloostermans
NXP
Email: christine.cloostermans@nxp.com

Authors' Addresses

Michael Prorock
mesur.io
Email: mprorock@mesur.io

Orie Steele
Tradeverifyd
Email: orie@or13.io

Hannes Tschofenig
University of Applied Sciences Bonn-Rhein-Sieg
Germany
Email: hannes.tschofenig@gmx.net