

# On the Adding NTRU back in liboqs

March 5, 2025

**NTT Akira NAGAI** 

Copyright NIPPON TELEGRAPH AND TELEPHONE CORPORATION





- Let us propose the **re-addition of NTRU**.
- NTRU is planned for use in the **IETF** and **GlobalPlatform**.
- There are also already applications (software router, optical transport network) using the liboqs library (NTRU).
- We will contribute by providing faster implementations, etc.
- Maintenance is also available from us.



- Some companies are worried about the patent issues of ML-KEM, and we think it is important to have an alternative.
- After version 0.72, NTRU support has been discontinued.
- At the IETF hackathon, when I talked about re-adding NTRU to liboqs, I was advised to contact Douglas.
- We contacted Douglas, and he contacted John Schanck, but there was no response, so we requested that we would like to update and maintain NTRU ourselves. He suggested that we attend this meeting.
- Today, we would like to explain to you all, and we would be very happy if you could approve the re-addition of NTRU.

# **IETF Activities**



We are collaborating with other companies to promote the standardization of NTRU in the IETF. We have published the specifications, including NTRU test vectors. We plan to give a presentation at this month's IETF meeting and request an "adoption call."

| Workgroup:       | CFRG                       |            |         |         |           |           |
|------------------|----------------------------|------------|---------|---------|-----------|-----------|
| Internet-Draft:  | draft-fluhrer-cfrg-ntru-02 |            |         |         |           |           |
| Published:       | 3 March 2025               |            |         |         |           |           |
| Intended Status: | Informational              |            |         |         |           |           |
| Expires:         | 4 September 2025           |            |         |         |           |           |
| Authors:         | S. Fluhrer                 | S. Prorock | M. Celi | J. Gray | K. Xagawa | H. Kosuge |
|                  | Cisco Systems              | mesur.io   | Brave   | Entrust | TII       | NTT       |
|                  |                            |            |         |         |           |           |

## NTRU Key Encapsulation

#### Abstract

This draft document provides recommendations for the implementation of a post-quantum Key Encapsulation Mechanism (KEM) scheme based on the NTRU encryption scheme. The KEM is an existing cryptographic system; no new cryptography is defined herein. The well-defined and reviewed parameter sets for the scheme are defined and recommended. The test vectors are also provided.

### 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/.

#### agenda-122-cfrg-02

CFRG - Crypto Forum Research Group IETF 122 in Bangkok

Monday March 17, 2025, 13:00-15:00 (UTC+7)

https://meetings.conf.meetecho.com/ietf122/?session=33810
Jabber: cfrg@jabber.ietf.org
Notes: https://notes.ietf.org/notes-ietf-122-cfrg

- Chairs: Alexey Melnikov, Stanislav Smyshlyaev and Nick Sullivan
- 13:00 Stanislav Smyshlyaev, "Chairs' update" (5 mins)
- 13:05 Nick Sullivan, "KEM Combiners Design Team: current status" (5+5)
- 13:15 Vasilis Kalos, Greg Bernstein, "Blind BBS and BBS Pseudonyms" (10+5 mins)
- 13:30 Patrick Longa, "FrodoKEM" (5+5 mins)
- 13:40 Chris Wood, "Anonymous Rate-Limited Credentials" (10+5 mins)
- 13:55 Deirdre Connolly, "Hybrid PQ/T Key Encapsulation Mechanisms" (10+5 mins)
- 14:10 Yuchen Wang, "ECDH-PSI" (10+5 mins)
- 14:25 Rohan Mahy, "MIMI franking mechanism" (10+5 mins)
- 14:40 Haruhisa Kosuge, "Advantages of NTRU compared to ML-KEM" (5+5 mins)

14:50 - Michele Orru, "Sigma protocols and Fiat-Shamir" (5+5 mins)

# **GlobalPlatform Activities**



- GlobalPlatform (GP) is a standards organization for the management and security of secure components/devices. It does not standardize the cryptographic mechanisms themselves; it specifies the mechanisms to be used.
- NTRU will be supported in the Tee Internal Core API. We believe that NTRU is suitable for resource-constrained environments, such as IC cards or microcontrollers. For this reason, we want to standardize it in GP.

| Global  | TEE Internal Core API Specification v1.3.1.35   | •        | Global<br>Platform®                 | TEE Internal<br>Public Review v1.3   | Core API Specification<br>.1.35 Page 16/449 |
|---|---|----------|-------------------------------------|--|---|
| Platform®   | Public Review Ends: 08 Sep 2023   | <b>U</b> | Standard / Specification            | Description  | Ref   |
| secure digital territore<br>and divides   | A minor version release with the following additions and hun fives applied  |          | GPD_SPE_024                         | GlobalPlatform Technology<br>TEE Secure Element API  | [TEE SE API]                                |
|   | A didad calling client (CA or TA) path identity chain enabling a TEE to describe all entities in the calling path to a TA   |          | GPD_SPE_025                         | GlobalPlatform Technology<br>TEE TA Debug Specification  | [TEE TA Debug]                              |
|   | <ul> <li>Added calling CECH (or or FA) pair identity chain, enabling a TEE to describe all entities in the calling pair to a FA.</li> <li>Added calling TEE instigation path identity chain, enabling a TEE to describe all entities layered below the TA.</li> </ul> |          | GPD_SPE_042                         | GlobalPlatform Technology<br>TEE TUI Extension: Biometrics API   | [TEE TUI Bio]                               |
| GlobalPlatform Technology   | Added ability to open TA-TA session in remote EE.   |          | GPD_SPE_055                         | GlobalPlatform Technology<br>TEE Trusted User Interface Low-level API  | [TEE TUI Low]                               |
| TEE Internal Core API<br>Specification<br>Version 13.35 (http://www.<br>Markow<br>Japana<br>Zeneter Workers (PR), 95, 95  | Added PQC optional algorithm support.   |          | GPD_SPE_100                         | GlobalPlatform Technology<br>TEE Sockets API Specification   | [TEE Sockets]                               |
|   | • TEE_TYPE_DILITHIUM  |          | GPD_SPE_120                         | GlobalPlatform Technology<br>TEE Management Framework (including ASN.1 Profile)<br>[Initially published as TEE Management Framework]   | [TMF ASN.1]                                 |
|   | TEE_TYPE_SPHINCSPLUS     TEE_TYPE_SPHINCSPLUS   |          | GPD_SPE_123                         | GlobalPlatform Technology<br>TEE Management Framework:<br>Open Trust Protocol (OTrP) Profile   | [TMF OTrP]                                  |
| Theorem 1 (1) 11 Mill Standwidsen van 21 April Neurona<br>Miller of Standard Standard<br>Standard Standard Standard<br>Standard Standard | TEE_TYPE_LMOIS     TEE_TYPE_LMS     TEE_TYPE_XMSS   |          | IANA LMS                            | Leighton-Micali Signatures (LMS)<br>https://www.iana.org/assignments/leighton-micali-<br>signatures/leighton-micali-signatures.xhtml dated<br>2021/06/01                       | [IANA 1]                                    |
|   | • TEE_TYPE_WOTS<br>• TEE_TYPE_FRODOKEM  |          | IANA XMSS                           | XMSS: Extended Hash-Based Signatures<br>https://www.iana.org/assignments/xmss-extended-hash-<br>based-signatures/xmss-extended-hash-based-<br>signatures.html dated 2020/05/15 | [IANA 2]                                    |
|   | TEE_TYPE_NTRU      Added entional CHACHA and POLV1205 elegrithm support (partly added to better enable TLS 1.2)   |          | IEEE P1363a-2004                    | IEEE Standard Specifications for Public-Key<br>Cryptography - Amendment 1: Additional Techniques   | [P1363]                                     |
|   | <ul> <li>Added optional CHACHA and POLTISOS algorithm support (party added to better enable TLS 1.5).</li> </ul>  |          | ISO/IEC 9899:1999                   | Programming languages – C  | [C99]                                       |
|   | <ul> <li>Expanded RSA asymmetric key sizes up to 8192.</li> <li>Added Panic masking mode for certain hard to programmatically avoid panic types.</li> </ul>   |          | NIST Recommended<br>Elliptic Curves | Recommended Elliptic Curves for Federal Government<br>Use  | [NIST Re Cur]                               |
|   | Added _PS functions to enable return of error code instead of Panic (generally for previous void return functions).   |          | NIST SP800-185                      | SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash,<br>and ParallelHash  | [NIST SP800-185]                            |
|   |   |          | NIST SP800-208                      | Recommendation for Stateful Hash-Based Signature<br>Schemes  | [NIST SP800-208]                            |
|   | Download Comment Form Patent Call Participant/Non-Participant Response forms  |          | NIST SP800-56B                      | Recommendation for Pair-Wise Key Establishment<br>Schemes Using Integer Factorization Cryptography   | [NIST SP800-56B]                            |
|   |   |          | NTRU                                | Algorithm Specifications And Supporting Documentation<br>March 30 2019 https://www.ntru.org/fintru-20190330.pdf  | [NTRU]                                      |
| https://globalplatform.or   | rg/wp-  |          |                                     |  |   |
| content/upi0aus/2023/0  |   | Algorith | m Specifications A                  | nd Supporting Documentatio   | n [NTRU]                                    |
|   |   | March 3  | 0 2019 https://www                  | w.ntru.org/f/ntru-20190330.pd  | ff  |

FYI: ML-DSA has already been implemented in IC cards

Lattice-based mechanism is expected to be used in constrained devices such as IC cards. The same can be expected for NTRU.



https://www.holdings.toppan.com/en/news/2024/10/newsrelease241007\_1.html

## Industry adoption: software router "Kamuee"



- NTRU will be implemented in Kamuee, a software router that provides fast and secure communications and is already in commercial use.
- The Kamuee team is also working to standardize router functions at the IETF, and they plan to use liboqs as their cryptographic library. They are currently using liboqs version 0.72 for testing, which supports NTRU.

## 100G Router version

- Hardware Price: Approx. \$40,000USD
- Supermicro 7048GR-TR: 4U Tower Server
- 100GbE (QSFP28: SR4/LR4) x 12 ports (6 slot) or
- 100GbE (QSFP28: SR4/LR4) x 10 ports + 10GbE (SFP+: SR/LR) x 4 ports





| - [ |                  |   |                    |  |
|-----|------------------|---|--------------------|--|
|     | Workgroup:       | SPRING  |                    |  |
|     | Internet-Draft:  | draft-watal-spring-srv6-sfc-sr-aware-functions-02 |                    |  |
|     | Published:       | 31 January 2025                                   |                    |  |
|     | Intended Status: | Informational                                     |                    |  |
|     | Expires:         | 4 August 2025                                     |                    |  |
|     | Authors:         | W. Mishima  | Y. Fukagawa        |  |
|     |                  | NTT Communications                                | NTT Communications |  |

## SRv6 SFC Architecture with SR-aware Functions

## Abstract

This document describes the architecture of Segment Routing over IPv6 (SRv6) Service Function Chaining (SFC) with SR-aware functions. This architecture provides the following benefits:

- Comprehensive Management: a centralized controller for SFC, handling SR Policy, link-state, and network metrics.
- Simplicity: no SFC proxies, so that reduces nodes and address resource consumption.

https://www.ietf.org/archive/id/draft-watal-spring-srv6-sfc-sr-aware-functions-02.html

## **Industry adoption: Optical Transport Network**



- Defined by the ITU-T, **Optical Transport Network** (**OTN**) is a digital wrapper that encapsulates frames of data, to allow multiple data sources to be sent on the same channel.
- Our company applied hybrid mode to OTN and testing currently using liboqs version 0.72



https://www.ciena.com/insights/what-is/What-is-Optical-Transport-Networking-OTN.html



https://www.rd.ntt/e/research/JN202302\_20961.html

# **Our Plans**



- Implementation will be based off of John Schanck's implementation
- Planning some implementation improvements
  - About 20% to 30% faster Toeplitz matrix-vector product (TMVP) based polynomial multiplication for encapsulation and decapsulation.

|            |                       | HPS40961229 | HRSS1373  |
|------------|-----------------------|-------------|-----------|
| TMVP       | <mark>keygen 💦</mark> | 4,378,071   | 5,649,592 |
| (proposed) | <mark>encaps</mark>   | 151,795     | 109,235   |
|            | <mark>decaps</mark>   | 206,129     | 300,504   |
| Toom       | <mark>keygen 💦</mark> | 4,866,283   | 6,129,491 |
| (current)  | <mark>encaps</mark>   | 187,182     | 156,283   |
|            | <mark>decaps</mark>   | 306,927     | 438,446   |

Comparison of CPU cycle count (mean)

• Masking implementation if necessary

# Maintenance



- We can provide maintenance for the NTRU part.
- We have also merged NTRU into the latest version of liboqs and are currently testing it to confirm that there are no problems. We are ready to merge it.



