Advantages of NTRU compared to ML-KEM

draft-fluhrer-cfrg-ntru-02

Scott Fluhrer, Michael Prorock, Sofia Celi, John Gray, Keita Xagawa,
Haruhisa Kosuge

Quick Overview

NTRU is:

- Post-quantum KEM (Key Encapsulation Mechanism) used for secret key sharing.
- One of Round 3 candidates of NIST PQC competition.
- Based on lattices over polynomial rings.

NTRU must be standardized in IETF, because NTRU has:

- Some advantages over ML-KEM
- Mature Specification
- Industrial adoption
- Plans for further adoption

Are others interested in the CFRG working on this?

Let's discuss on the mailing list.

Some advantages over ML-KEM

Advantages over ML-KEM

- No patent issues (patent free).
- Long history without security issues (since 1996)
- Flexible parameter such as lattice dimensions.
- Masking implementation is easy since FO-transform is not used.

Disadvantages over ML-KEM

- KeyGen (key generation) is slower.

NTRU can be used in almost all scenarios where ML-KEM is applicable.

Performance Comparison on Cortex-M4

		Bit security in non-local model	KeyGen [K cycles]	Encaps [K cycles]	Decaps [K cycles]
NTRU [PC22]	hps2048677	145	142,378	816	729
	hrss701	151	153,508	369	787
	hps4096821	178	212,377	1,026	914
ML-KEM (Round 3 Kyber Specification)	512	118	434	530	476
	768	183	706	863	783
	1024	256	1,122	1,315	1,209

For the same security in non-local model, NTRU is as fast as ML-KEM (except KeyGen).

[PC22]:Paksoy, I. K., & Cenk, M. (2022). Faster NTRU on ARM Cortex-M4 with TMVP-based multiplication.

Size Comparison

		Bit security in non-local model	Public Key [bytes]	Private Key [bytes]	Ciphertext [bytes]	Public key + Ciphertext [bytes]
NTRU (Round 3 NTRU Specification)	hps2048677	145	699	935	699	1,398
	hrss701	151	930	1,234	930	1,860
	hps4096821	178	1,138	1,450	1,138	2,276
ML-KEM (Round 3 Kyber Specification)	512	118	800	1,632	768	1,568
	768	183	1,184	2,400	1,088	2,272
	1024	256	1,568	3,168	1,568	3,136

For the same security in non-local model, NTRU has the similar sizes as ML-KEM.

Size Comparison to HQC

		Public Key [bytes]	Private Key [bytes]	Ciphertext [bytes]	Public key + Ciphertext [bytes]
NTRU	hps2048677	699	935	699	1,398
	hrss701	930	1,234	930	1,860
	hps4096821	1,138	1,450	1,138	2,276
HQC	128	2,249	2,289	4,481	6730
	192	4,522	4,595	9,026	13548
	256	7,245	7.349	14,469	21714

There is no performance analysis of HQC on Cortex-M4.

Mature Specification

Workgroup: CFRG
Internet-Draft: draft-fluhrer-cfrg-ntru-latest
Published: 1 March 2025
Intended Status: Informational
Expires: 2 September 2025

Authors: S. Fluhrer (*Cisco Systems*), S. Prorock (*mesur.io*), M. Celi (*Brave*), J. Gray (*Entrust*), K. Xagawa (*TII*), H. Kosuge (*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/.

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

Table of Contents

GitHub - mesur-io/ntru-key-encapsulation: NTRU Key Encapsulation

Industrial Adoption (two examples)

Post-quantum Secure Transport System

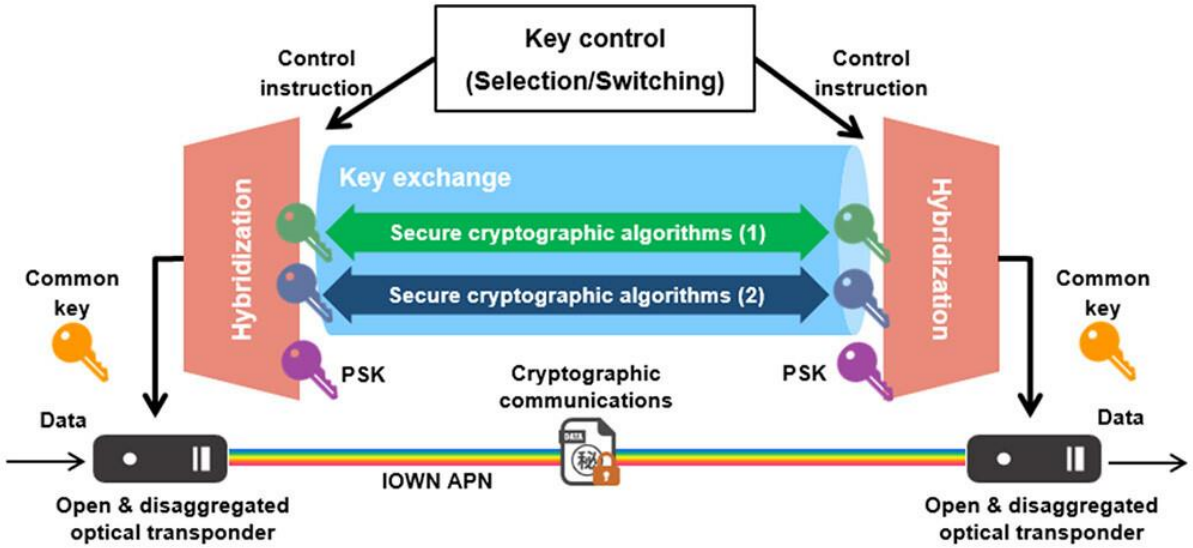
- Technology enabling flexible crypto switching, which will be utilized in all photonic network connecting Japan and Taiwan.
- The system implements NTRU for the key exchange function.

October 30, 2024 NTT Corporation

World's first post-quantum secure transport system capable of switching cryptography methods without interrupting communications

News Highlights:

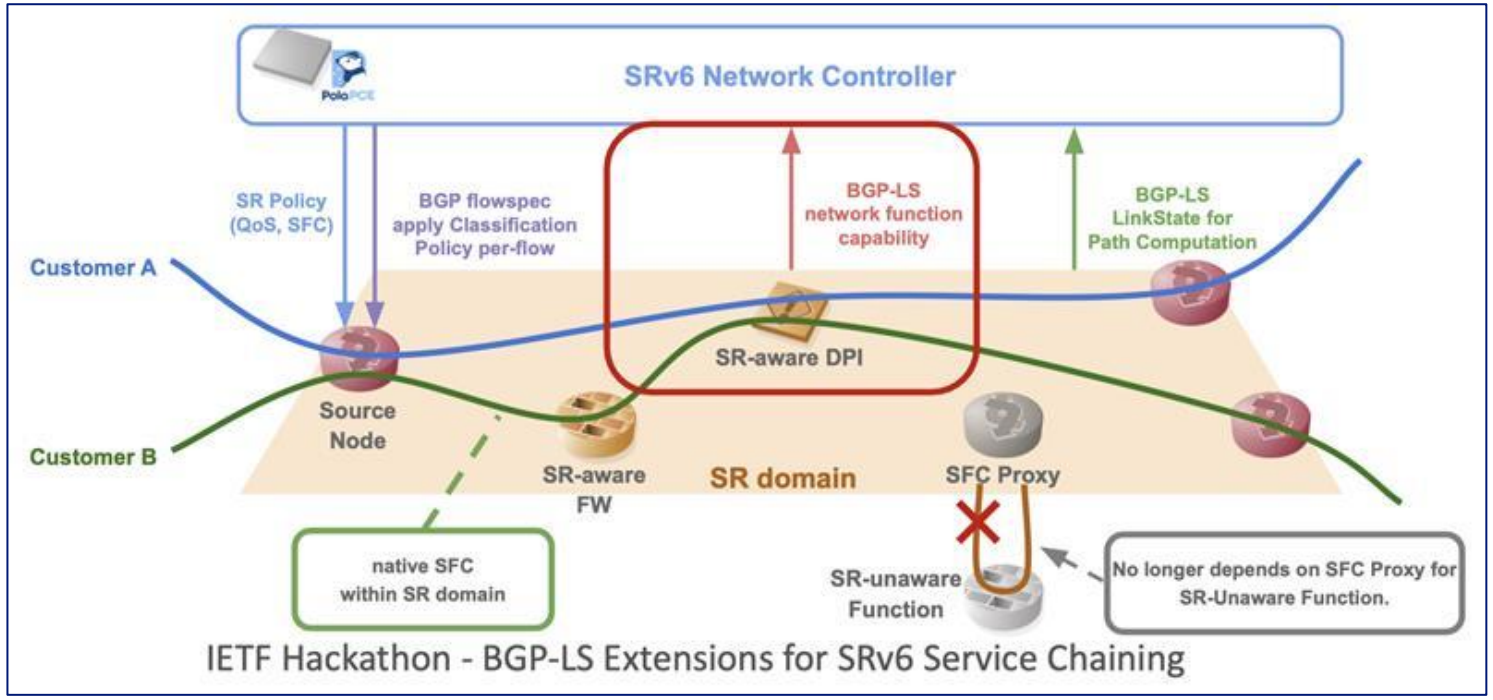
- **New technology enabling flexible encryption switching provides continuous and secure communications:** Allows cryptography algorithms to be updated without system disruption, preventing service interruptions while maintaining the latest security.
- **Pre-emptive security response to threats in the quantum computer era:** Enables rapid transition to post-quantum cryptography and forestalls future security risks.
- **Enhancing societal security through open optical transponder:** Applying open optical transponder to optical networks enhances the security of social infrastructure.



https://group.ntt/en/newsrelease/2024/10/30/241030a.html

VPN in Software Router Kamuee

- Kamuee is DPDK-based software router that is in commercial use.
- The Kamuee team is working on standardizing SRv6 SFC-Arch at IETF.
- An NTRU-based IPsec VPN will be implemented in Kamuee soon.



https://datatracker.ietf.org/meeting/121/materials/slides-121-hackathon-sessd-bgp-ls-extensions-for-srv6-service-chaining-00

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

Plans for Further Adoption

We are working on:

- Re-adding NTRU to liboqs (almost completed).
- Launching a project to standardize IKEv2 with NTRU.
- Updating NTRU.org, and using it to share the latest information.

We still have very challenging work ahead, so we are looking for teammates.
We will hold a public side meeting for NTRU. If you're interested, join us!

(March 18th, 16:00-17:00 @Meeting Room 3)

Summary

NTRU must be standardized in IETF, because NTRU has:

- Some advantages over ML-KEM
- Mature draft
- Industrial adoption
- Plans for further adoption

Are others interested in the CFRG working on this?
Let's discuss on the mailing list.