NTRU

draft-fluhrer-cfrg-ntru-03

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

NTRU Overview

NTRU (=NTRU-HPS+NTRU-HRSS) is:

- Post-quantum KEM (Key Encapsulation Mechanism)
- Finalist in Round 3 of NIST PQC competition.
- Based on lattices over polynomial rings.

Key features of NTRU

- Patent-free
- Mature specification based on NIST PQC (5 years passed)
- Ready to use (back to liboqs soon)

Recap of IETF 122

We presented that NTRU has:

- Advantages over ML-KEM
  - Patent free
  - Long history
  - Flexible parameter sets
  - Masking friendly
- Good performance/size

⇒ Practical alternative of ML-KEM.

Feedback and our responses:

- How about other NTRU variants?

⇒ We will compare in this talk.

- Too many parameters.

⇒ Since parameter flexibility is an advantage, this draft includes all. But further discussion is welcome.

Scope and Objectives of This Talk

- Questions have been raised about other NTRU variants.
- Classic McEliece and FrodoKEM are also in discussion.

⇒ It is important to clarify the position of NTRU among the KEMs.

By security/performance comparison with KEMs, NTRU has:

- Tighter IND-CCA2 security proof assuming OW-CPA
- Mot comparable performance and size to ML-KEM

Security Comparisons of KEMs

KEMs	Security (QROM)	Transform	Tightness	Assumption	Structure?
NTRU	IND-CCA2	$U_m^{\perp}$	$O(\sqrt{\epsilon_{OW}})$	NTRU	Yes
NTRU Prime	IND-CCA2	$U^{\perp}$	$O(\sqrt{\epsilon_{OW}})$	NTRU	Yes
NTRU+	IND-CCA2? [BCG+24]	Variant of $FO^{\not\perp}$	$O(q\sqrt{\epsilon_{OW}})$?	NTRU	Yes
ML-KEM	IND-CCA2	$FO_m^{\not\perp}$	$O(q\sqrt{\epsilon_{OW}})$ $O(\sqrt{q\epsilon_{CPA}})$	(D)MLWE	Yes
HQC	IND-CCA2	$FO^{\not\perp}$	$O(q\sqrt{\epsilon_{OW}})$ $O(\sqrt{q\epsilon_{CPA}})$	(D)QCSDP	Yes
Classic McEliece	IND-CCA2	$U_m^{\perp}$	$O(\sqrt{\epsilon_{OW}})$	SDP	No
FrodoKEM	IND-CCA2	$FO^{\not\perp}$	$O(q\sqrt{\epsilon_{OW}})$ $O(\sqrt{q\epsilon_{CPA}})$	(D)LWE	No

Referenced the latest specifications.

Tighter: Classic McEliece, NTRU, NTRU Prime
No Structure: Classic McEliece, FrodoKEM
⇒ We assume that any of the above KEMs can improve crypto agility.

[BCG+24] Report on evaluation of KpqC Round-2 candidates.

Performance/Size Comparisons of KEMs

Based on SUPERCOP (amd64; Golden Cove (906a4-40); 2022 Intel Core i3-1215U, P cores; 2 x 1600MHz)

KEMs	Parameter (128-bit)	Performance (CPU cycles)				Size (bytes)		
		KeyGen	Encaps	Decaps	Total	|pk|	|c|	Total
NTRU	hps2048667	202 578	22 458	26 246	251 282	930	930	1 860
	hrss701	19 6581	17 287	39 684	253 552	1 138	1 138	2 276
NTRU Prime	sntrup761	561 644	33 732	42 222	637 598	1 158	1 039	2 197
NTRU+	768	61 030	20 294	20 318	101 642	1 152	1 152	2 304
ML-KEM (Kyber)	512	17 916	25 962	20 972	64 850	800	768	1 568
HQC	128	69 460	175 773	308 836	554 069	2 249	4 497	6 746
Classic McEliece	348864	58 695 440	28 039	99 785	58 823 264	261 120	96	261 216
FrodoKEM	640AES	918 610	1 247 004	1 187 728	3 353 342	9 616	9 720	19 336

NTRU is the most competitive with ML-KEM.
(NTRU+ is faster but needs further analysis.)

Conclusion

- Tighter IND-CCA2 security proof assuming OW-CPA
- Mot comparable performance and size to ML-KEM

⇒ Without ML-KEM: NTRU is a practical alternative.

With ML-KEM: NTRU improves crypto agility with small overhead.

- A draft for hybrid KEMs in IKEv2 (RFC9370) using NTRU was published. (draft-skyline-ipsecme-ntru-ikev2-00)
- Public side meeting on post-quantum IKEv2 + NTRU: Friday 10:30 – 11:00. Please join us!

(Bonus) Comparison of Lattice-based KEMs

KEMs	Parameter (128-bit)	Block size β	Classical time complexity (log_2)	
			Conservative (0.292β)	Realistic (0.368β)
NTRU	hps2048667	496	145	182
	hrss701	470	151	172
NTRU Prime	sntrup761	523	153	203
ML-KEM	512	406	118	149
FrodoKEM	640	496	145	182

Referenced the latest specifications and based on evaluation of [BDGL16]

NTRU, NTRU Prime, and FrodoKEM achieve 128-bit classical security even in the conservative evaluation.

[BDGL16] Becker, Ducas, Gama, and Laarhoven, ACM-SIAM 2016.