Investigation on NIST post-quantum lattice-based encryption schemes

Giacomo mazzola (G.Mazzola-1@student.tudelft.nl), Kaitai Liang (Kaitai.Liang@tudelft.nl), Huanhuan Chen (H.Chen-2@tudelft.nl)

1. Research Question:

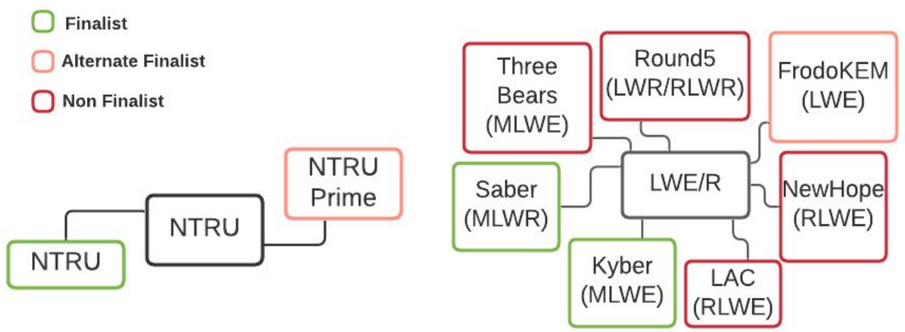
Present the state of the art lattice-based cryptography and perform a comparative analysis of the lattice-based encryption schemes submitted to NIST quantum competition over the following points:

- Theoretical and practical security
- Theoretical and practical level of cost, efficiency and complexity (bandwidth, memory, runtime)
- Computation/distinguishing features
- Potential vulnerabilities and shortages
- Overall complexity of the schemes

2. Method:

- Literature research
- For each scheme:
  - read the description paper
  - clone, understand and run the code
  - read public reviews
  - compare it with previous ones
- draw conclusions and write final paper

3. Analyzed Schemes:



4. Results

	NewHope	FrodoKem	Kyber	Saber	NTRU	LAC	Three Bears	NTRU Lprime	SNTRU	Round5
private key	3 680	43 088	3 168	1 664 (384)	1 592	2 080	(40)	1 999	1 462	-
bandwidth	5 888	43 152	3 136	2 784	2 460	2 480	3 281	2 506	2 496	2 272
key gen	245	30 301	331	131	31 835	377	118	45	940	101
encryption	377	32 611	397	159	1 856	643	145	81	45	152
decryption	437	32 387	451	165	4 920	917	211	113	94	207
failure rate	2^{-213}	2^{-252}	2^{-228}	2^{-165}	0	2^{-138}	2^{-256}	0	0	2^{-239}
primal attack	259/235	281/256	256/232	283/257	179/-	323/293	354/321	140/153	153/139	256/233
dual attack	257/233	279/254	256/232	338/308	N/A	320/290	-	N/A	N/A	257/234

Data for private key and bandwidth (public key + ciphertext) expressed in bytes.
Data for runtime performance expressed in thousands CPU cycles.
Data for primal and dual attack is gathered through theoretical analysis and is expressed in $\log_2$ of CPU operations.

	NewHope	FrodoKem	Kyber	Saber	NTRU	LAC	NTRU Lprime
key gen	138	2 813	226	150	3 432	101	6 374
encryption	195	3 587	257	174	341	171	12 708
decryption	227	3 414	280	190	169	286	19 060

Experimental data gathered by running schemes on an Intel Core i7-8750H 2.2 GHz with hyperthreading and turbo boost on.
Expressed in thousands CPU cycles.

5. Conclusions

Performance:

- (Module/Ring) LWE/R > LWE/R
- (Module/Ring) LWE/R ≃ NTRU

Security:

- theoretically LWE/R > (Module/Ring) LWE/R
- NTRU has no formal proof but has old cryptanalytic history

Complexity:

- (Module/Ring) LWE/R > LWE/R

General:

- Experimental results confirm theoretical claims (except for NTRU LPrime).
- Lattice-based schemes best alternative so far

Future Work:

- Further study of the schemes and performance optimizations
- deploy hybrid schemes for sudden quantum protection