PQC KEM Performance

David Cooper

April 7, 2020

For internal use only

Second Round KEM Candidates

Encryption/KEMs

Crystals-Kyber	Lattice	MLWE
Saber	Lattice	MLWR
FrodoKEM	Lattice	LWE
~~Round 5~~	~~Lattice~~	~~LWR/RLWR~~
~~LAC~~	~~Lattice~~	~~RLWE~~
NewHope	Lattice	RLWE
Three Bears	Lattice	IMLWE
NTRU	Lattice	NTRU
NTRUprime	Lattice	NTRU

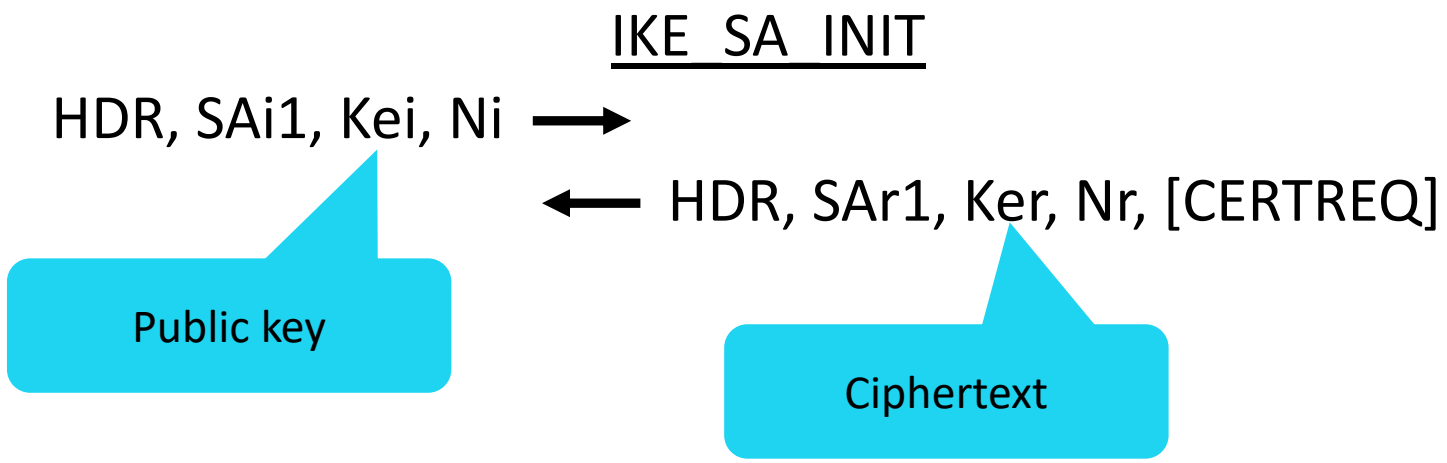
SIKE	Isogeny	Isogeny
Classic McEliece	Codes	Goppa
~~NTS-KEM~~	~~Codes~~	~~Goppa~~
BIKE	Codes	short Hamming
HQC	Codes	short Hamming
~~LEDAcrypt~~	~~Codes~~	~~short Hamming~~
~~ROLLO~~	~~Codes~~	~~low rank~~
~~RQC~~	~~Codes~~	~~low rank~~

KEM Summary

- Compared algorithms using bandwidth cost of 2000 cycles/byte
- Saber provides best overall performance
  - Small public keys and ciphertext
  - Fast operations
- Kyber best for constrained devices
  - Public keys a bit larger than Saber (about same ciphertext length)
  - Faster operations than Saber
  - Needs little memory (even Kyber-1024 uses < 4 KB RAM)
- BIKE-2 probably least bad non-lattice submission

Size Constraints

- RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*
  - All IKEv2 implementations MUST be able to send, receive, and process IKE messages that are up to 1280 octets long, and they SHOULD be able to send, receive, and process messages that are up to 3000 octets long.



eBACS – 2013 Intel Xeon E3-1220 v3 (hiphop)

https://bench.cr.yp.to/results-kem.html#amd64-hiphop

Submission	Parameter Set	Claimed Security Level	Key gen	encrypt	decrypt	Public Key	ciphertext	Total Cycle Cost
Round5	R5ND_1KEM_5d	1	70,792	122,012	63,184	445	549	2,243,988
Round5	R5ND_1KEM_4longkey	1	73,728	124,908	65,200	453	563	2,295,836
Round5	R5ND_1KEM_0d	1	51,856	90,296	42,684	634	682	2,816,836
Saber	LightSaber2	1	48,668	67,328	69,464	672	736	3,001,460
CRYSTALS-Kyber	512-90s	1	15,860	26,684	22,220	800	736	3,136,764
CRYSTALS-Kyber	512	1	29,176	46,228	39,436	800	736	3,186,840
Three Bears	BabyBear(624r2cca)	2	43,792	64,480	117,968	804	917	3,668,240
NTRU Prime	ntrulpr653	2	43,768	71,800	87,996	897	1,025	4,047,564
NTRU	ntruhps2048677	1	291,540	53,740	73,196	930	930	4,138,476
New Hope	512cca	1	63,064	107,296	109,956	928	1,120	4,376,316
NTRU Prime	sntrup653	2	721,384	48,588	66,376	994	897	4,618,348
NTRU	ntruhrss701	1	284,884	51,904	75,532	1,138	1,138	4,964,320
Round5	R5N1_1KEM_0d	1	546108	651328	263556	5,214	5,236	22,360,992
Frodo	frodokem640aes	1	4,579,176	1,989,660	1,951,428	9,616	9,720	47,192,264
Frodo	frodokem640shake	1	7,171,140	4,524,864	4,514,080	9,616	9,720	54,882,084
SIKE	sikep503	2	15,011,760	24,642,176	26,273,080	378	402	67,487,016

Jacob's Numbers (Code-based Only)

- BIKE-2-CCA has 1,472 byte public keys and ciphertexts
  - Shortest code-based option, but wouldn't fit in a single packet.

Submission	Parameter Set	Keypair	Enc	Dec	pk	ct	time
BIKE (CPA)	BIKE2, LEVEL 1	3,317,667	115,423	1,539,072	1,271	1,271	10,056,162
BIKE (CPA)	BIKE3, LEVEL 1, BANDWIDTH_OPT	181,249	193,081	2,218,959	1,411	2,758	10,931,289
BIKE (CPA)	BIKE1, LEVEL 1	202,797	137,907	1,497,893	2,542	2,542	12,006,597
BIKE (CPA)	BIKE3, LEVEL 1	182,540	181,979	2,184,889	2,758	2,758	13,581,408
HQC	hqc-128-1	177,546	361,768	599,428	3,125	6,234	19,856,742

Performance Numbers from Submissions

Submission	Parameter Set	Claimed Security Level	architecture	Key gen	encrypt	decrypt	Public Key	ciphertext	total cycle cost
Round5	R5ND_1KEM_5d	1		54,000	94,400	55,800	445	549	2,192,200
Round5	R5ND_1KEM_4longkey	1		57,200	97,700	55500	453	563	2,242,400
Round5	R5ND_1KEM_0d	1		57,600	94,900	45,000	634	682	2,829,500
Saber	LightSaber2	1	Skylake	61,849	72,692	70,605	672	736	3,021,146
CRYSTALS-Kyber	512-90s	1	Haswell	20,004	30,384	24,604	800	736	3,146,992
LAC	lac128	1	Haswell	122,691	209,201	323,221	544	712	3,167,113
CRYSTALS-Kyber	512	1	Haswell	33,428	49,184	40,564	800	736	3,195,176
Three Bears	BabyBear	2	Skylake	41,000	60,000	101,000	804	917	3,644,000
New Hope	512cca	1	Haswell	68,080	109,836	114,176	928	1,120	4,388,092
NTRU	ntruhrss701	1	Haswell	381,476	71,238	77,848	1,138	1,138	5,082,562
BIKE-2	Level 1	1	Kaby Lake	4,460,000	120,000	5,550,000	1,270	1,270	15,211,500
BIKE-1	Level 1	1	Kaby Lake	200,000	150,000	5,300,000	2,541	2,541	15,813,000
HQC	hqc-128-1	1	Skylake	250,000	520,000	940,000	3,125	6,234	20,428,000
Round5	R5N1_1KEM_0d	1		2,766,000	4,049,000	188,800	5,214	5,236	27,903,800
SIKE	sikep434	1	Skylake	6,487,000	10,536,000	11,297,000	330	346	29,672,000
SIKE	sikep503	2	Skylake	8,956,000	14,783,000	15,759,000	378	402	41,058,000
Frodo	frodokem640aes	1	Skylake	1,384,000	1,858,000	1,749,000	9,616	9,720	43,663,000
Frodo	frodokem640shake	1	Skylake	4,015,000	4,442,000	4,331,000	9,616	9,720	51,460,000
SIKE	sikep434_compressed	1	Skylake	16,542,000	20,045,000	18,930,000	196	209	56,327,000
SIKE	sikep503_compressed	2	Skylake	23,395,000	27,543,000	25,534,000	224	248	77,416,000
Classic McEliece	kem/mceliece348864	1	Haswell	14,870,324	45,888	136,840	261,120	128	537,549,052

PQM4 KEM Decryption Benchmarks

https://github.com/mupq/pqm4/blob/master/benchmarks.md

- Which fit in 4 KB RAM (max. RAM in payment cards)?
  - Kyber: 512, 512-90s, 768, 1024
  - NewHope-512cca
  - BabyBear is close (maybe M4-optimized version would fit?)
- Only showing KEMs w/ total cost < 10,000,000 cycles (decrypt only)
  - Optimized version of NTRU Prime not available

Submission	Parameter Set	impl.	Claimed Security Level	Key gen	encrypt	decrypt	Public Key	ciphertext	Code Size (bytes)	Key gen (bytes)	Encrypt (bytes)	Decrypt (bytes)	Total Cycle Cost
CRYSTALS-Kyber	512	m4	1	468,578	594,543	552,657	800	736	10,304	2,404	2,484	2,508	3,624,657
New Hope	512cca	m4	1	578,950	865,876	819,973	928	1,120	13,104	1,828	2,988	2,996	4,915,973
CRYSTALS-Kyber	512-90s	m4	1	335,085	393,319	402,365	800	736	10,468	2,912	2,992	3,016	3,474,365
Three Bears	BabyBear	opt	2	596,665	752,117	1,142,773	804	917	5,627	3,104	2,976	5,112	4,584,773
Round5	R5ND_1CCA_5d	m4	1	316,023	501,764	656,064	445	549	5,423	3,924	4,996	5,612	2,644,064
LAC	lac128	ref	1	2,266,368	3,979,851	6,303,717	544	712	30,076	2,916	5,116	5,952	8,815,717
Round5	R5ND_1CCA_0d	m4	1	419,911	637,673	807,621	634	682	2,581	4,492	5,596	6,332	3,439,621
Saber	LightSaber2	m4	1	459,965	651,273	678,810	672	736	44,916	9,656	11,392	12,136	3,494,810
NTRU	ntruhrss701	m4	1	154,676,705	402,784	890,231	1,138	1,138	132,224	27,580	19,372	20,580	5,442,231
NTRU	ntruhps2048677	m4	1	144,383,491	955,902	836,959	930	930	129,504	28,524	20,604	17,756	4,556,959

PQM4 KEM Encryption Benchmarks

https://github.com/mupq/pqm4/blob/master/benchmarks.md

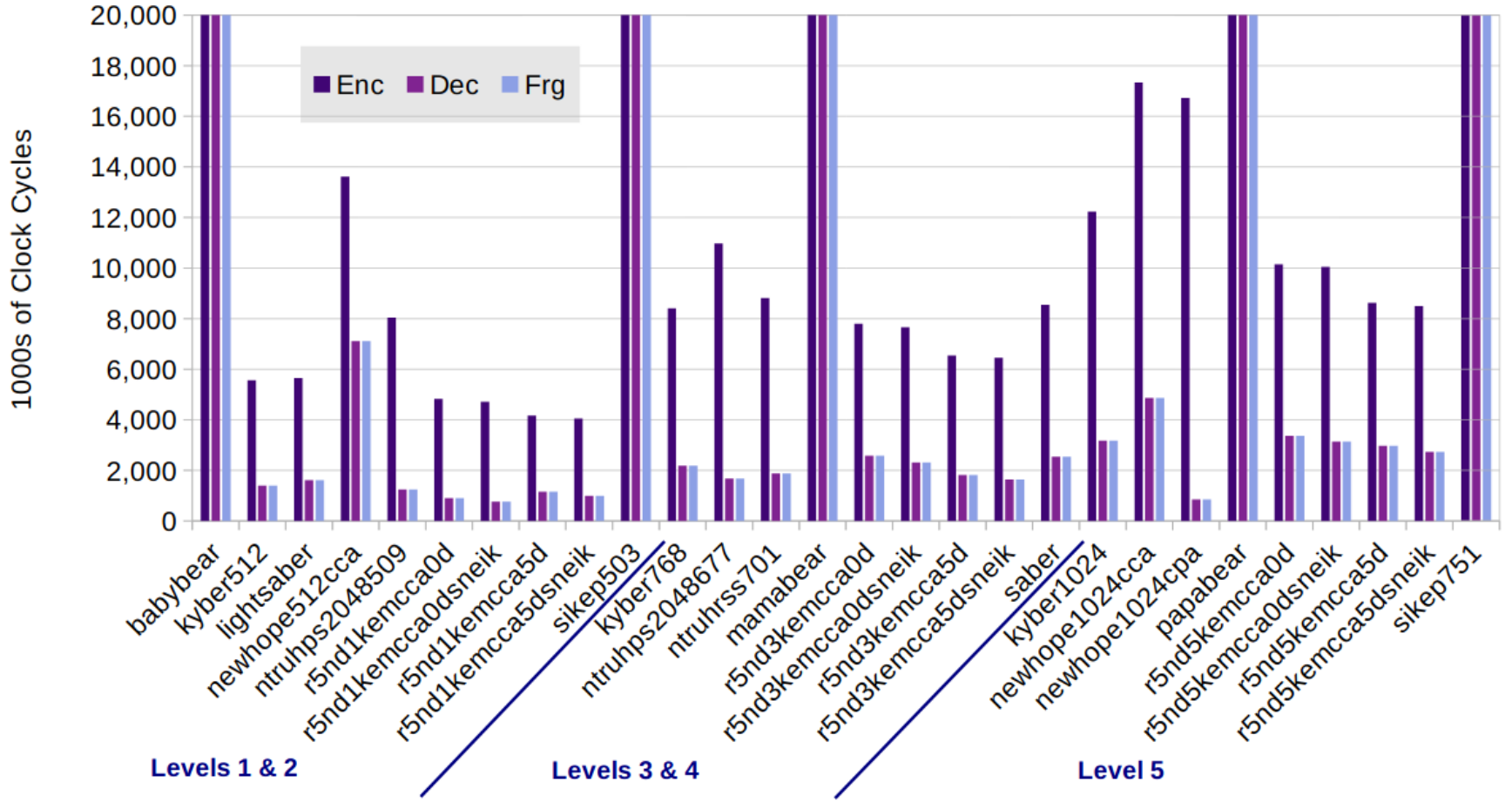
- Only showing KEMs w/ total cost < 10,000,000 cycles (encrypt only)
  - Optimized version of NTRU Prime not available

Submission	Parameter Set	impl.	Claimed Security Level	Key gen	encrypt	decrypt	Public Key	ciphertext	Code Size (bytes)	Key gen (bytes)	Encrypt (bytes)	Decrypt (bytes)	Total Cycle Cost
CRYSTALS-Kyber	512	m4	1	468,578	594,543	552,657	800	736	10,304	2,404	2,484	2,508	3,666,543
Three Bears	BabyBear	opt	2	596,665	752,117	1,142,773	804	917	5,627	3,104	2,976	5,112	4,194,117
New Hope	512cca	m4	1	578,950	865,876	819,973	928	1,120	13,104	1,828	2,988	2,996	4,961,876
CRYSTALS-Kyber	512-90s	m4	1	335,085	393,319	402,365	800	736	10,468	2,912	2,992	3,016	3,465,319
Round5	R5ND_1CCA_5d	m4	1	316,023	501,764	656,064	445	549	5,423	3,924	4,996	5,612	2,489,764
LAC	lac128	ref	1	2,266,368	3,979,851	6,303,717	544	712	30,076	2,916	5,116	5,952	6,491,851
Round5	R5ND_1CCA_0d	m4	1	419,911	637,673	807,621	634	682	2,581	4,492	5,596	6,332	3,269,673
Saber	LightSaber2	m4	1	459,965	651,273	678,810	672	736	44,916	9,656	11,392	12,136	3,467,273
NTRU	ntruhrss701	m4	1	154,676,705	402,784	890,231	1,138	1,138	132,224	27,580	19,372	20,580	4,954,784
NTRU	ntruhps2048677	m4	1	144,383,491	955,902	836,959	930	930	129,504	28,524	20,604	17,756	4,675,902

More Cortex M4 Numbers

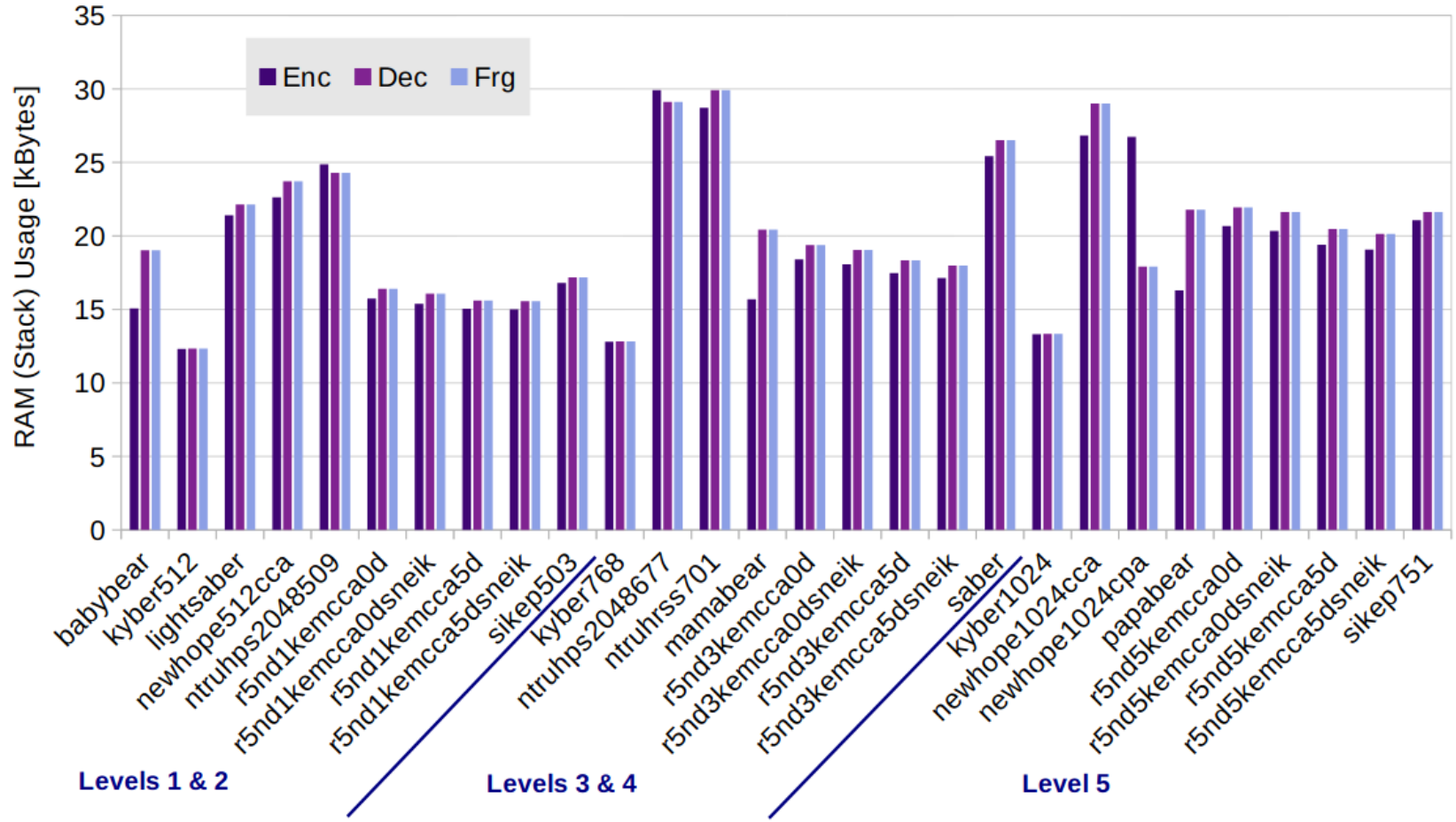
- *Feasibility and Performance of PQC Algorithms on Microcontrollers*, Brian Hession and Jen-Peter Kaps, Second PQC Standardization Conference:
  - If execution time or power consumption are of greatest concern, the Kyber, NewHope, Ntru, and Saber implementations are good candidates for KEM algorithms. However, if memory usage is of greatest concern, the Kyber and Three Bears algorithms are best suited.

Clock Cycles till 20,000,000



- Kyber, NewHope, NTRU, Round5, and Saber complete
- Encapsulation significantly slower than decapsulation

Stack Usage



- Our Platform only has 32 kByte of RAM
- This causes several algorithms to crash, e.g., firesaber

NewHope on ARM Cortex M0 and M3

- Post-quantum crypto on µC: Peter Schwabe, December, 12, 2017
  - https://cryptojedi.org/peter/data/continental-20171212.pdf
- Cortex M0:
  - Fits in 8 KB of RAM
  - Key generation: 1,170,892 cycles
  - Encryption: 1,760,837 cycles
  - Decryption: 298,877 cycles
- Cortex M4:
  - Key generation: 781,518 cycles
  - Encryption: 1,140,594 cycles
  - Decryption: 174,798 cycles