KpqC 알고리즘 성능측정2

정보컴퓨터공학과 권혁동

기존 진행 사항

- 알고리즘의 성능을 Ryzen 프로세서 상에서 –O2로 측정
- 이는 **개발자들의 의도를 반영하지 못한다는 맹점**이 존재
  - 대부분의 KpqC 알고리즘은 **Intel 상에서 –O3**로 측정
- 일부 알고리즘은 성능 측정을 진행하지 못함
  - FIBS, **Layered-ROLLO**
- 따라서 추가적인 실험을 진행하고 이를 기록

추가 실험

- 알고리즘 벤치마킹은 다양한 환경에서 실험할 수록 좋음
  - 기존 측정 환경: 1개
  - 추가 측정 환경: **1+3개**
- Ryzen 프로세서 장비: TFG5746HS, Ryzen 7 4800H, 16GB RAM
- Intel 프로세서 장비: Intel NUC, Intel i5-8259U, 16GB RAM

	-O2	-O3
Intel	Intel –O2	Intel –O3
Ryzen	Ryzen –O2	Ryzen –O3

추가 실험

- 추가 실험을 위해 **Makefile을 –O2로 설정**하고 다시 컴파일
- 벤치마킹을 하지 못한 코드를 추가로 벤치마크
  - **Layered-ROLLO**
  - FIBS는 무한루프로 실행 불가, REDOG은 파이썬 코드로 측정 제외
- AVX 의존성이 있는 코드는 제거하기가 어려우므로 그대로 둠
  - **NTRU+, Layered-ROLLO, SOLMAE**
- 일부 소스코드는 **OpenSSL 의존성 제거가 필요**
  - **Layered-ROLLO**

~~취소선~~: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨)

녹색 이름 알고리즘: AVX 적용

Ryzen –O2

Unit: clock cycles

Algorithm	Keygen (Med.)	Encapsulation (Med.)	Decapsulation (Med.)	Keygen (Avr.)	Encapsulation (Avr.)	Decapsulation (Avr.)
IPCC_f1	14,362,627	~~164,892,550~~	2,484,981	14,376,006	~~239,300,607~~	2,501,514
IPCC_f3	14,170,647	898,710	2,619,570	14,178,752	941,012	2,633,907
IPCC_f4	14,209,594	1,075,059	2,904,524	14,245,778	1,135,740	2,935,161
NTRUplus-576	208,742	111,998	128,093	286,443	112,614	128,670
NTRUplus-768	279,386	148,480	181,250	298,193	154,346	185,298
NTRUplus-864	304,819	179,858	224,953	306,436	180,793	225,978
NTRUplus-1152	444,744	223,619	278,690	801,975	224,602	279,606
PALOMA-128	125,800,419	510,922	35,496	125,630,139	513,098	36,061
PALOMA-192	125,360,779	514,228	34,220	125,242,970	516,579	34,419
PALOMA-256	125,294,065	510,284	34,713	125,174,502	512,685	34,978
SMAUG-128 (revised)	171,477	154,483	178,205	181,007	156,512	181,950
SMAUG-192 (revised)	250,096	229,999	277,298	260,837	230,994	279,080
SMAUG-256 (revised)	479,138	385,178	438,364	490,702	387,420	439,345
TiGER-128	273,470	466,755	628,778	286,082	471,567	632,066
TiGER-192	288,550	518,491	674,192	293,000	524,467	691,838
TiGER-256	536,152	~~1,088,747~~	~~1,477,318~~	541,935	~~1,092,191~~	~~1,276,848~~

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨)

녹색 이름 알고리즘: AVX 적용

Ryzen –O3

Unit: clock cycles

Algorithm	Keygen (Med.)	Encapsulation (Med.)	Decapsulation (Med.)	Keygen (Avr.)	Encapsulation (Avr.)	Decapsulation (Avr.)
IPCC_f1	13,940,097	~~160,111,204~~	~~16,360,164~~	13,969,607	~~232,561,407~~	2,408,173
IPCC_f3	13,996,024	926,492	2,512,836	14,036,005	967,543	2,532,438
IPCC_f4	13,989,832	1,106,031	2,714,531	14,007,544	1,165,274	2,732,139
NTRUplus-576	202,652	110,026	121,742	287,810	110,910	123,929
NTRUplus-768	270,512	146,566	174,435	281,685	147,174	175,018
NTRUplus-864	297,192	168,113	204,537	302,876	168,857	206,046
NTRUplus-1152	435,305	222,459	266,626	772,442	223,429	268,110
PALOMA-128	122,325,408	498,365	34,307	122,253,994	500,446	34,484
PALOMA-192	122,290,738	503,266	34,278	122,173,457	506,366	34,468
PALOMA-256	122,321,957	497,959	34,249	122,254,172	500,026	34,420
SMAUG-128 (revised)	72,790	57,246	50,460	82,292	57,466	50,708
SMAUG-192 (revised)	105,966	82,940	80,475	108,491	83,648	81,029
SMAUG-256 (revised)	158,021	139,925	135,749	161,110	141,573	138,010
TiGER-128	65,482	48,749	51,214	68,866	49,105	51,589
TiGER-192	69,426	63,510	57,739	79,105	63,805	59,383
TiGER-256	81,316	87,551	93,090	90,989	88,218	93,436
Layered ROLLO I-128	285,940	83,346	788,104	296,880	84,198	805,790
Layered ROLLO I-192	320,958	136,503	1,014,203	345,689	149,843	1,110,378
Layered ROLLO I-256	687,721	201,913	1,945,871	700,284	207,030	1,948,662

~~취소선~~: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨)

녹색 이름 알고리즘: AVX 적용

Intel –O2

Unit: clock cycles

Algorithm	Keygen (Med.)	Encapsulation (Med.)	Decapsulation (Med.)	Keygen (Avr.)	Encapsulation (Avr.)	Decapsulation (Avr.)
IPCC_f1	13,792,887	~~159,126,951~~	1,196,157	13,896,694	~~231,010,613~~	1,259,215
IPCC_f3	13,754,219	870,059	1,235,991	13,864,988	922,755	1,307,538
IPCC_f4	13,754,687	1,050,451	1,318,173	13,851,205	1,151,306	1,380,740
NTRUplus-576	186,944	105,686	120,194	271,460	121,722	132,428
NTRUplus-768	246,616	139,310	166,938	265,516	154,868	174,788
NTRUplus-864	270,494	160,789	200,702	288,025	180,014	206,856
NTRUplus-1152	698,490	202,678	257,114	744,381	212,073	267,046
PALOMA-128	118,204,341	499,914	39,724	118,365,137	511,837	41,693
PALOMA-192	118,310,371	499,302	38,846	118,490,933	514,299	41,016
PALOMA-256	118,366,206	503,814	43,174	118,507,160	518,903	45,385
SMAUG-128 (revised)	158,149	164,598	196,470	165,414	169,648	203,288
SMAUG-192 (revised)	244,736	225,490	272,132	265,142	236,227	285,366
SMAUG-256 (revised)	435,790	411,917	465,572	448,654	422,602	486,263
TiGER-128	163,856	209,168	311,924	182,794	217,723	325,532
TiGER-192	171,578	214,126	312,702	181,774	221,613	324,412
TiGER-256	444,558	433,462	673,105	461,623	448,364	714,429

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨)

녹색 이름 알고리즘: AVX 적용

Intel –O3

Unit: clock cycles

Algorithm	Keygen (Med.)	Encapsulation (Med.)	Decapsulation (Med.)	Keygen (Avr.)	Encapsulation (Avr.)	Decapsulation (Avr.)
IPCC_f1	12,643,392	~~145,233,220~~	1,159,273	12,712,124	~~210,977,105~~	1,185,580
IPCC_f3	12,795,377	874,663	1,206,585	12,874,291	922,533	1,267,783
IPCC_f4	13,078,917	1,037,485	1,310,503	13,250,237	1,107,017	1,368,035
NTRUplus-576	177,748	102,296	111,820	258,761	117,949	124,783
NTRUplus-768	239,546	137,135	161,970	257,560	165,057	177,077
NTRUplus-864	260,672	153,481	186,386	272,001	163,794	197,686
NTRUplus-1152	568,556	201,226	246,050	698,764	209,569	256,800
PALOMA-128	108,402,198	459,846	40,838	108,597,537	473,532	42,840
PALOMA-192	108,206,652	460,374	40,688	108,344,570	472,432	42,798
PALOMA-256	108,216,713	459,880	40,886	108,461,853	465,766	41,780
SMAUG-128 (revised)	63,020	49,324	39,196	65,919	55,873	42,528
SMAUG-192 (revised)	92,658	69,739	67,691	95,436	74,836	70,950
SMAUG-256 (revised)	135,202	122,766	115,096	142,842	128,734	118,789
TiGER-128	62,490	45,398	53,248	66,987	48,285	56,591
TiGER-192	66,512	60,238	58,572	71,626	71,973	71,967
TiGER-256	78,772	82,776	89,902	83,770	90,129	98,287
Layered ROLLO I-128	203,181	66,529	558,503	231,523	77,774	602,966
Layered ROLLO I-192	227,813	102,758	671,605	255,243	125,567	761,739
Layered ROLLO I-256	375,056	136,052	1,245,346	455,911	146,919	1,337,504

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨) 녹색 이름 알고리즘: AVX 적용 Ryzen –O2 Unit: clock cycles

Algorithm	Keygen (Med.)	Sign (Med.)	Verify (Med.)	Keygen (Avr.)	Sign (Avr.)	Verify (Avr.)
AIMER-I	145,058	3,912,361	3,669,834	156,204	3,966,517	3,701,498
AIMER-III	296,496	8,001,274	7,550,063	315,810	8,033,590	7,548,322
AIMER-V	710,442	18,068,276	17,415,022	730,960	18,077,211	17,421,527
GCKSign-II	179,771	601,707	176,987	181,822	848,504	178,229
GCKSign-III	186,673	649,049	183,367	198,852	899,646	185,793
GCKSign-V	252,822	917,415	277,733	255,206	1,099,271	284,217
HAETAE-II (revised)	798,312	4,605,461	147,494	1,091,637	5,704,780	148,078
HAETAE-III (revised)	1,533,941	11,474,155	257,926	2,127,683	12,068,749	259,846
HAETAE-V (revised)	846,713	3,902,298	305,428	1,104,472	5,214,861	306,973
MQSign-72/46	94,788,559	516,954	1,461,281	94,829,257	518,651	1,465,923
MQSign-112/72	488,913,828	1,493,703	5,211,909	490,448,324	1,513,132	5,258,218
MQSign-148/96	1,488,480,956	3,162,943	12,036,827	1,488,377,972	3,164,654	12,041,118
NCCSign-II(con)	2,650,542	10,404,301	5,232,079	2,670,083	10,419,012	5,244,741
NCCSign-III(con)	4,477,513	17,657,839	8,867,243	4,497,436	17,666,605	8,869,094
NCCSign-V(con)	7,240,343	64,377,767	14,358,074	7,257,655	64,387,183	14,375,040
NCCSign-II(ori)	1,869,079	23,762,252	3,681,057	1,882,892	23,763,293	3,684,640
NCCSign-III(ori)	3,655,334	39,587,190	7,241,808	3,675,996	39,635,337	7,246,465
NCCSign-V(ori)	6,263,739	179,281,596	12,418,902	6,268,503	179,337,534	12,422,702
Peregrine-512	12,401,256	329,933	37,294	12,609,569	332,600	37,505
Peregrine-1024	39,405,505	709,848	80,243	42,160,344	722,426	81,200
pqsigRM-613	6,013,112,315	7,210,560	2,223,401	5,970,970,554	9,823,994	2,303,399
pqsigRM-612	58,238,108,879	1,864,512	1,053,034	58,669,322,672	2,650,133	1,064,763
SOLMAE-512	23,848,774	378,392	43,935	29,181,985	385,719	44,109
SOLMAE-1024	55,350,546	760,380	141,375	70,141,847	764,304	142,357

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨) **녹색 이름 알고리즘: AVX 적용** Ryzen –O3 Unit: clock cycles

Algorithm	Keygen (Med.)	Sign (Med.)	Verify (Med.)	Keygen (Avr.)	Sign (Avr.)	Verify (Avr.)
AIMER-I	**145,986**	3,878,272	3,672,923	**156,213**	4,077,840	4,384,331
AIMER-III	296,032	8,087,462	7,678,098	307,498	8,364,809	7,740,701
AIMER-V	713,922	17,983,857	17,361,691	817,056	18,096,797	17,472,521
GCKSign-II	164,836	537,675	159,674	175,216	765,476	160,447
GCKSign-III	**166,199**	**581,189**	**161,646**	**180,908**	**806,260**	**162,452**
GCKSign-V	**231,797**	895,549	279,009	**242,850**	1,068,798	280,118
HAETAE-II (revised)	688,083	3,429,265	131,805	957,268	4,247,185	132,462
HAETAE-III (revised)	1,329,157	8,734,670	228,578	1,843,459	9,183,604	229,703
HAETAE-V (revised)	723,318	2,790,612	272,542	946,202	3,700,449	273,840
MQSign-72/46	**39,040,917**	311,112	512,227	**39,057,616**	312,293	514,042
MQSign-112/72	**115,942,827**	669,465	1,143,296	**116,040,569**	672,499	1,147,066
MQSign-148/96	**235,289,035**	1,186,622	1,943,667	**235,425,321**	1,190,984	1,952,355
NCCSign-II(con)	2,619,295	10,301,902	**5,171,686**	2,639,164	10,308,375	**5,175,958**
NCCSign-III(con)	4,379,261	86,475,941	**8,685,877**	4,405,049	86,515,726	**8,685,125**
NCCSign-V(con)	7,178,921	42,637,366	**14,245,148**	7,194,274	42,681,718	**14,247,358**
NCCSign-II(ori)	1,843,356	**50,520,712**	3,636,803	1,860,128	**50,540,655**	3,643,639
NCCSign-III(ori)	3,618,997	**21,416,384**	7,170,903	3,646,841	**21,437,009**	7,169,406
NCCSign-V(ori)	6,149,059	**151,973,282**	12,196,791	6,162,746	**152,011,122**	12,213,326
Peregrine-512	11,953,307	**253,402**	**25,462**	12,146,320	**254,228**	**25,634**
Peregrine-1024	38,366,232	**535,920**	**53,621**	41,014,591	**538,260**	**53,946**
pqsigRM-613	**6,139,551,981**	4,610,319	2,278,806	**6,144,274,759**	6,276,554	2,376,095
pqsigRM-612	**54,994,439,928**	714,647	225,577	**55,073,661,751**	967,439	234,553
SOLMAE-512	23,053,028	349,566	40,513	28,233,370	355,950	40,812
SOLMAE-1024	53,966,332	698,581	135,256	68,603,714	702,006	136,193

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨) **녹색 이름 알고리즘: AVX 적용** Intel –O2 Unit: clock cycles

Algorithm	Keygen (Med.)	Sign (Med.)	Verify (Med.)	Keygen (Avr.)	Sign (Avr.)	Verify (Avr.)
AIMER-I	**145,566**	3,691,256	3,713,173	**159,391**	3,845,843	4,018,047
AIMER-III	274,358	7,771,108	7,366,672	304,919	7,863,536	7,438,953
AIMER-V	790,456	18,394,069	**17,662,359**	899,383	18,802,192	**18,080,181**
GCKSign-II	171,176	640,093	167,116	190,739	845,502	173,676
GCKSign-III	**173,252**	**698,964**	**168,824**	**185,265**	**943,376**	**176,768**
GCKSign-V	**248,629**	945,815	273,631	**264,811**	1,151,316	282,979
HAETAE-II (revised)	700,875	4,173,002	142,584	979,130	5,274,158	150,759
HAETAE-III (revised)	1,352,577	10,615,663	250,534	1,940,364	11,445,286	262,470
HAETAE-V (revised)	752,413	3,418,728	311,986	983,382	4,622,966	328,866
MQSign-72/46	**87,038,447**	509,630	1,377,392	**87,156,508**	527,234	1,411,202
MQSign-112/72	**448,271,119**	1,472,032	4,808,216	**448,141,266**	1,500,297	4,875,532
MQSign-148/96	**1,326,638,494**	3,128,536	11,091,036	**1,328,649,536**	3,150,219	11,143,601
NCCSign-II(con)	2,296,351	15,914,954	**4,519,308**	2,412,156	16,002,740	**4,622,316**
NCCSign-III(con)	4,009,717	16,015,734	**7,996,462**	4,169,703	16,116,734	**8,085,000**
NCCSign-V(con)	6,561,582	26,019,063	13,005,536	6,639,348	26,080,187	13,084,234
NCCSign-II(ori)	1,704,190	**27,083,021**	3,344,228	1,799,742	**27,354,886**	3,460,388
NCCSign-III(ori)	3,271,119	**65,455,745**	6,533,931	3,402,118	**65,582,525**	6,586,857
NCCSign-V(ori)	5,723,169	**39,565,842**	11,290,884	6,088,747	**39,658,546**	11,384,040
Peregrine-512	12,073,005	**295,128**	**33,114**	12,299,755	**305,264**	**35,943**
Peregrine-1024	38,493,479	**640,132**	**71,246**	41,112,188	**652,620**	**74,891**
pqsigRM-613	**4,961,556,899**	7,505,040	2,125,125	**4,973,260,518**	10,823,438	2,645,728
pqsigRM-612	**74,021,054,015**	2,113,913	1,126,131	**73,941,690,821**	2,765,068	1,295,161
SOLMAE-512	22,494,902	351,311	64,526	27,556,843	366,508	68,880
SOLMAE-1024	52,388,360	706,028	152,984	65,688,581	729,400	158,540

취소선: 성능 측정 중 다소 이상한 부분이 있어서 재측정 필요 (성능의 일관성 확인이 안됨) **녹색 이름 알고리즘: AVX 적용** Intel –O3 Unit: clock cycles

Algorithm	Keygen (Med.)	Sign (Med.)	Verify (Med.)	Keygen (Avr.)	Sign (Avr.)	Verify (Avr.)
AIMER-I	**133,130**	3,960,345	3,747,101	143,746	4,070,924	3,834,717
AIMER-III	272,484	8,440,184	7,968,982	282,896	8,530,553	8,041,509
AIMER-V	643,253	17,998,305	**17,373,174**	662,744	18,202,241	**17,455,874**
GCKSign-II	175,993	597,712	172,893	188,999	869,677	182,127
GCKSign-III	**183,987**	**698,941**	**179,608**	**223,689**	**976,483**	**186,837**
GCKSign-V	**238,884**	928,251	262,868	259,401	1,228,167	293,133
HAETAE-II (revised)	672,901	3,334,242	126,972	944,910	4,200,552	132,300
HAETAE-III (revised)	1,291,292	8,261,232	227,780	1,828,235	8,769,910	238,478
HAETAE-V (revised)	719,708	2,627,334	270,600	973,865	3,546,813	280,493
MQSign-72/46	**38,474,591**	298,952	533,676	**38,612,360**	308,203	547,680
MQSign-112/72	**117,049,542**	650,928	1,120,124	**117,234,338**	667,681	1,147,333
MQSign-148/96	**236,124,011**	1,165,706	1,897,664	**236,332,422**	1,173,558	1,908,458
NCCSign-II(con)	2,317,555	13,776,448	**4,568,006**	2,393,641	13,868,809	**4,647,302**
NCCSign-III(con)	3,981,551	83,521,123	**7,935,382**	4,209,101	83,634,184	**8,001,129**
NCCSign-V(con)	6,333,006	25,183,392	12,555,623	6,470,472	25,269,299	12,680,799
NCCSign-II(ori)	1,666,543	**16,352,341**	3,248,162	1,846,947	**16,530,887**	3,321,373
NCCSign-III(ori)	3,141,974	**34,454,252**	6,234,249	3,227,617	**34,523,301**	6,288,505
NCCSign-V(ori)	5,613,303	**167,158,023**	11,155,020	5,851,360	**167,337,719**	11,307,818
Peregrine-512	11,783,005	**260,328**	**26,262**	12,032,320	**269,678**	**28,484**
Peregrine-1024	37,875,534	**551,168**	**55,654**	40,364,494	**569,794**	**58,474**
pqsigRM-613	**4,702,612,115**	4,732,706	2,064,731	**4,703,836,987**	6,667,564	2,458,625
pqsigRM-612	**71,111,088,778**	923,513	417,658	**71,168,430,985**	1,166,665	502,448
SOLMAE-512	22,627,042	332,848	64,838	27,866,035	348,841	67,662
SOLMAE-1024	53,245,753	668,103	149,168	67,369,725	686,523	154,073

실험 결과

- 공개키 암호화
  - **TiGER > SMAUG > NTRU+ > PALOMA > ROLLO > IPCC**
  - **TiGER > SMAUG > PALOMA > NTRU+ > IPCC > ROLLO (AVX 패널티 적용: 성능*3)**
- 전자서명
  - **Peregrine > SOLMAE> pqsig > GCKSign > MQSign > HAETAE > AIMer > NCC**
  - **Peregrine > pqsig > GCKSign > SOLMAE> HAETAE > MQSign > AIMer > NCC (AVX 패널티 적용: 성능*3)**
- 최적화 레벨에 따른 성능 차이는 크지 않음
  - 대부분의 알고리즘이 최적화가 잘 되었다고 할 수 있음

향후 과제

- **개발자들과 직접적인 소통**
  - 벤치마크는 좋으나, 개발자들의 의도를 반영하지 못하는 부분이 존재
  - 독단적인 실험보다는 연락을 통해 더 좋은 결과를 도출하는 것이 좋음
- **AVX 비활성화가 가능한 경우는 일반 성능도 측정**
  - SOLMAE가 이에 해당 됨
- **무결성 검증이 추가적으로 필요**
  - 현재 일부 알고리즘은 KAT 값이 일부만 맞는 현상이 확인됨
  - 메모리 문제일 가능성이 높음

Q & A