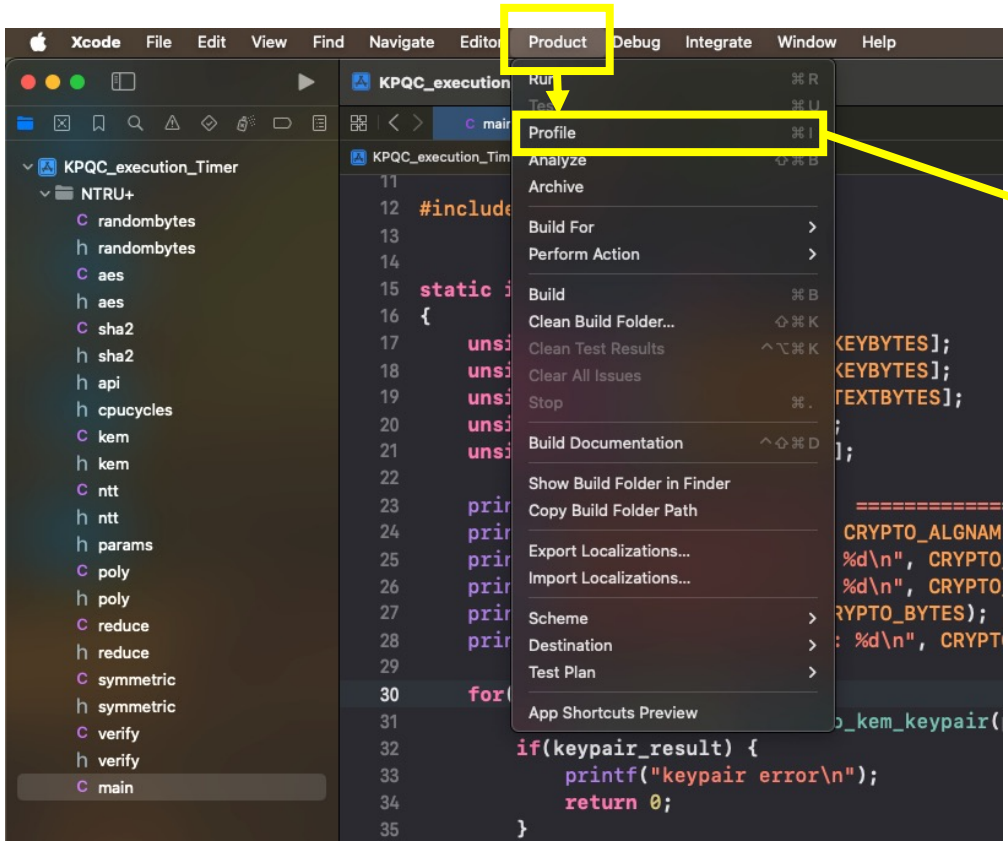
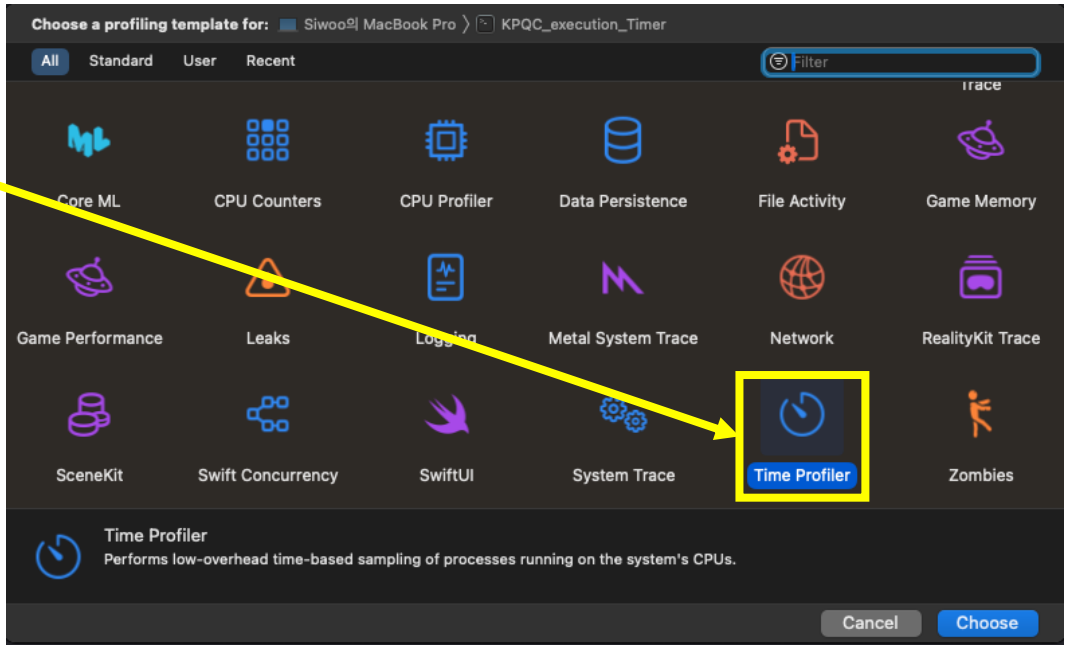
KPQC 알고리즘의 연산 시간 분석

https://youtu.be/NMYF8ZlSjuY

측정 도구 및 방법

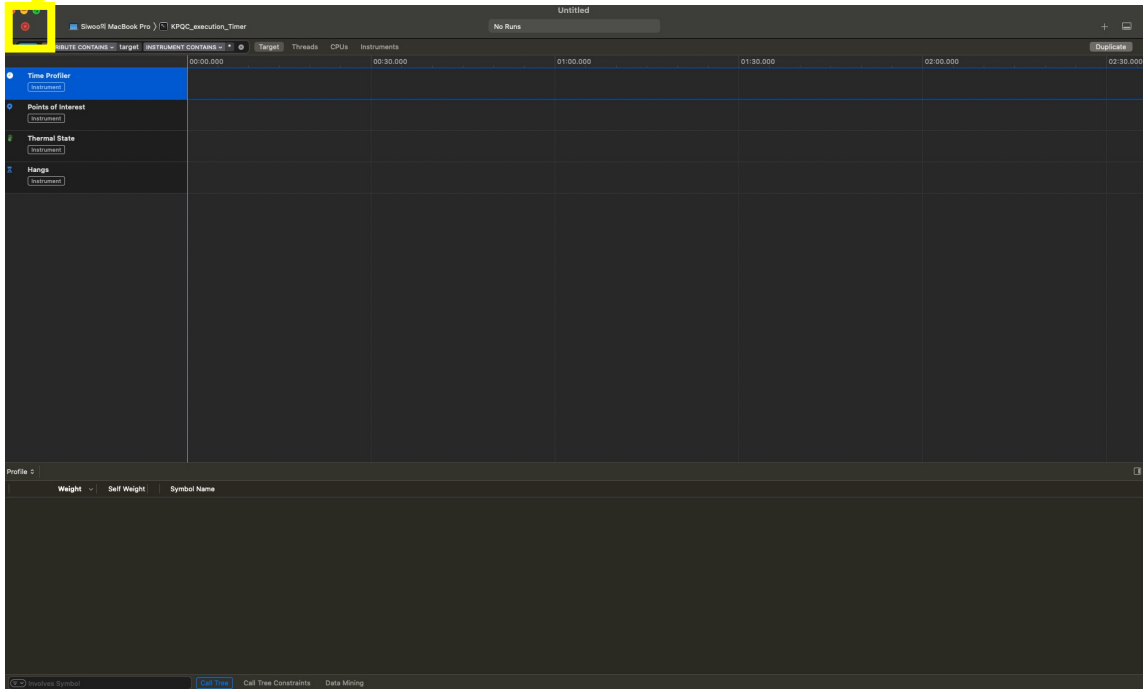
- Xcode에서 제공하고 있는 Profile 도구 활용
  - Product -> Profile -> Time Profiler



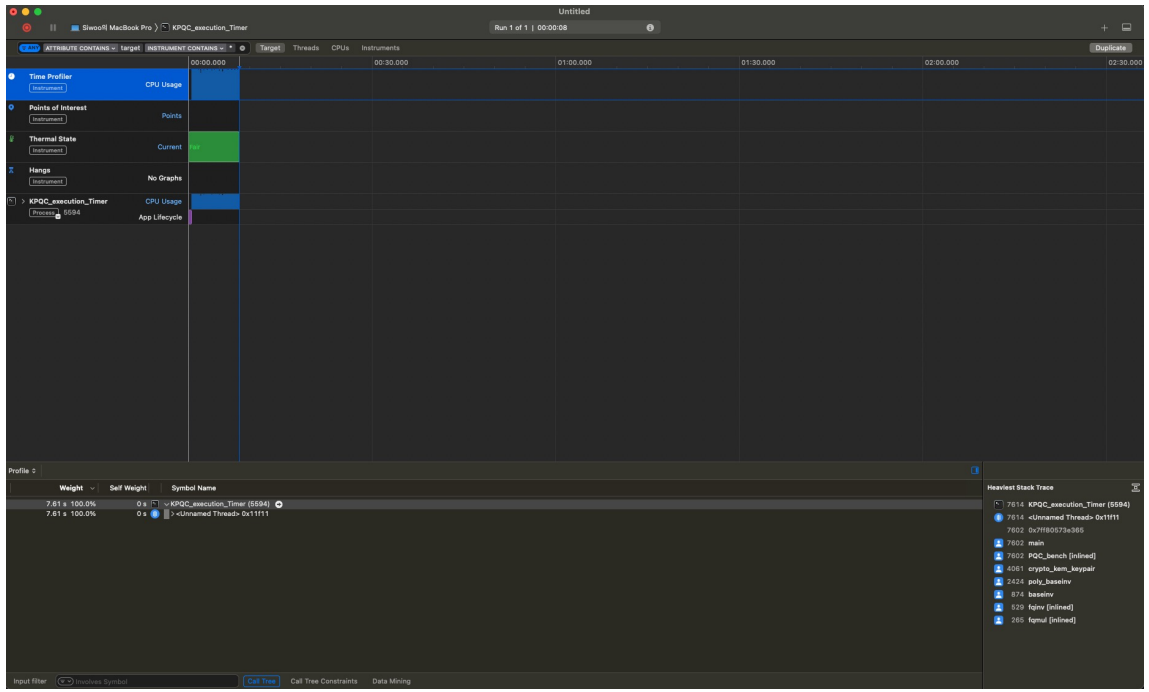


측정 도구 및 방법

- Time Profiler 실행 모습
  - 왼쪽 상단 녹화버튼으로 프로그램 실행
    - 키 생성, 암호화, 복호화를 **여러 번 반복해야** 함수 이름이 정확하게 분석됨



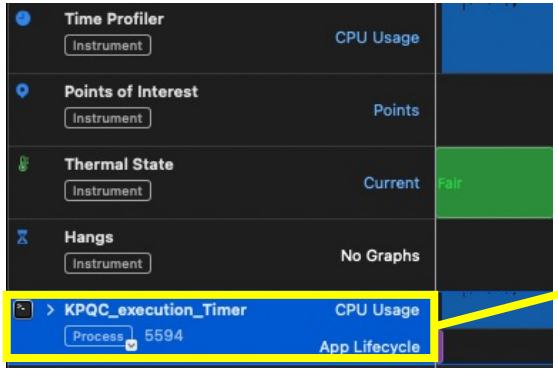
녹화전

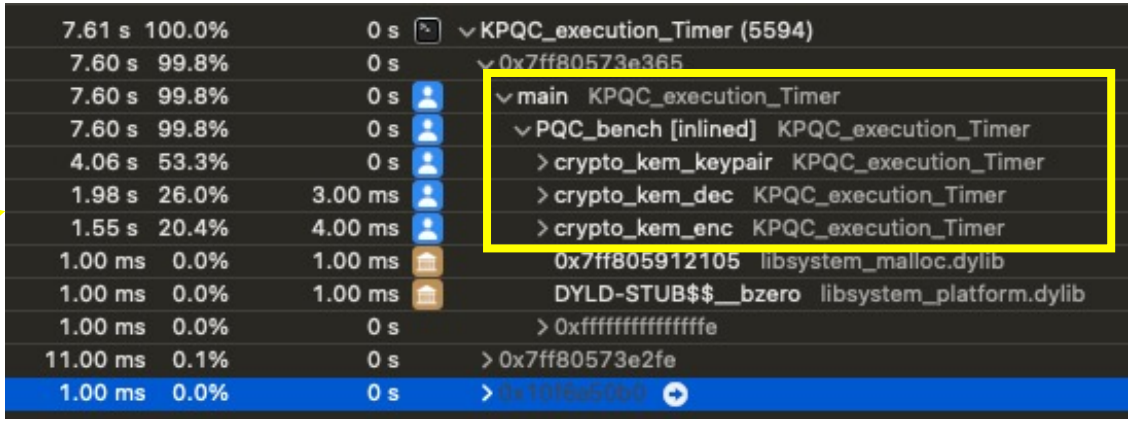


녹화후

측정 결과

선택



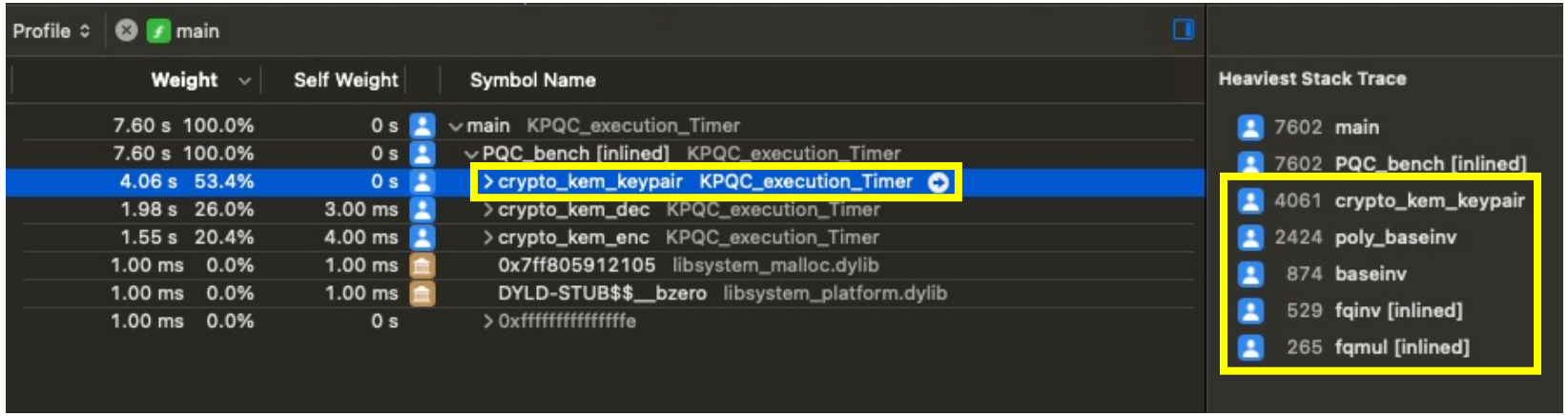



```c
for(int i=0; i<50000; i++){
    int keypair_result = crypto_kem_keypair(pk, sk);
    if(keypair_result) {
        printf("keypair error\n");
        return 0;
    }

    int enc_result = crypto_kem_enc(ct, ss, pk);
    if(enc_result) {
        printf("encap error\n");
        return 0;
    }

    int dec_result = crypto_kem_dec(dss, ct, sk);
    if(dec_result) {
        printf("decap error\n");
        return 0;
    }
}
```

main 함수의 코드



대략적인 사용 함수같음

측정 결과

실행 시간 | Self 실행시간

실행 시간		Self 실행시간	
4.06 s	53.3%	0 s	crypto_kem_keypair KPQC_execution_Timer
2.42 s	31.8%	16.00 ms	poly_baseinv KPQC_execution_Timer
353.00 ms	4.6%	250.00 ms	ntt KPQC_execution_Timer
278.00 ms	3.6%	5.00 ms	poly_basemul KPQC_execution_Timer
243.00 ms	3.1%	1.00 ms	hash_f KPQC_execution_Timer
169.00 ms	2.2%	7.00 ms	aes_ctr KPQC_execution_Timer
151.00 ms	1.9%	0 s	fqmul [inlined] KPQC_execution_Timer
113.00 ms	1.4%	36.00 ms	poly_reduce KPQC_execution_Timer
70.00 ms	0.9%	70.00 ms	poly_tobytes KPQC_execution_Timer
68.00 ms	0.8%	67.00 ms	poly_cbd1 KPQC_execution_Timer
62.00 ms	0.8%	0 s	aes256_ecb_keyexp KPQC_execution_Timer
34.00 ms	0.4%	0 s	randombytes_bsd_randombytes [inlined] KPQC_execution_Timer
30.00 ms	0.3%	0 s	fqmul [inlined] KPQC_execution_Timer
26.00 ms	0.3%	0 s	0xfffffffffffffffe
24.00 ms	0.3%	0 s	fqmul [inlined] KPQC_execution_Timer
9.00 ms	0.1%	9.00 ms	poly_triple KPQC_execution_Timer
3.00 ms	0.0%	0 s	0x7ff8058ebb8a libsystem_malloc.dylib
1.00 ms	0.0%	1.00 ms	0x7ff8058ebd23 libsystem_malloc.dylib
1.00 ms	0.0%	1.00 ms	0x7ff80597195c libsystem_c.dylib
1.00 ms	0.0%	1.00 ms	0x7ff8058fc8fa libsystem_malloc.dylib
1.00 ms	0.0%	1.00 ms	0x7ff8059086b6 libsystem_malloc.dylib

238.00 ms	3.1%	1.00 ms	sha256 KPQC_execution_Timer
228.00 ms	2.9%	1.00 ms	sha256_inc_finalize KPQC_execution_Timer
222.00 ms	2.9%	207.00 ms	crypto_hashblocks_sha256 KPQC_execution_Timer
4.00 ms	0.0%	4.00 ms	_platform_memmove$VARIANT$Haswell libsystem_platform.dylib
1.00 ms	0.0%	1.00 ms	_platform_bzero$VARIANT$Haswell libsystem_platform.dylib

- 실행 시간
  - 함수의 전체 실행 시간
- Self 실행시간
  - 함수에서 다른 함수를 제외한 자체의 실행시간

예) sha256
실행 시간은 238ms
self 실행시간은 1ms

237ms은 sha256함수 내부의 또 다른 함수에서 실행되고 있음

sha256 함수 자체는 1ms 걸림
sha256 내부 함수 중에서
crypto_hash_blocks_sha256 함수가 207ms 동안 동작

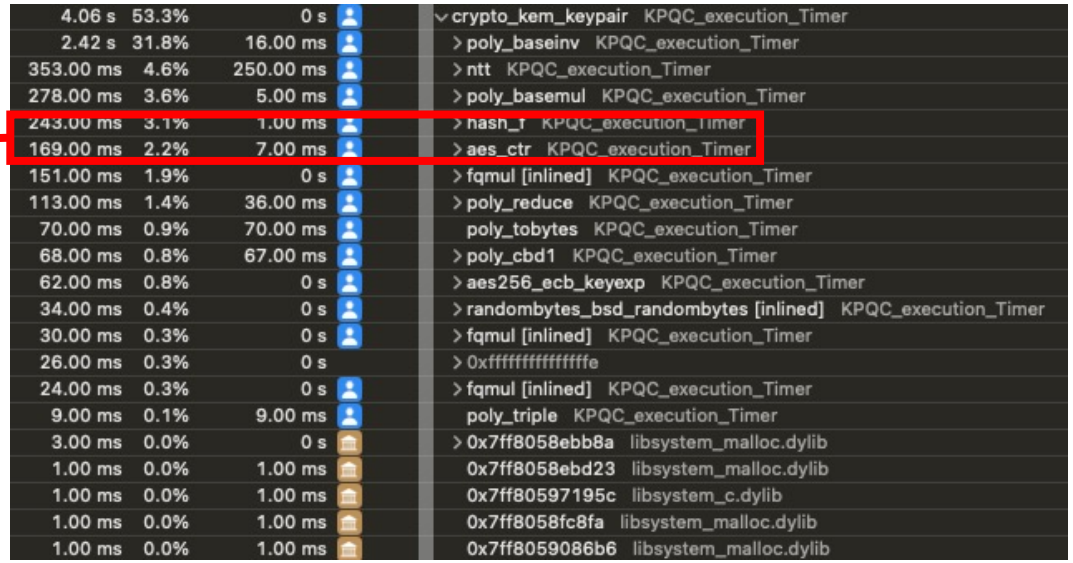
즉, sha256 실행시간은 sha256 + sha256_inc_finalize + crypto_hashblocks_sha256 + … = 238ms

측정 전 준비

- Xcode에서 동작될 수 있도록 알고리즘 별 구현
- 알고리즘 별로 특정 함수가 어떤 연산인지 대략적으로 분석할 예정

Algorithm 8 $\mathsf{Gen}(1^\lambda)$: key generation

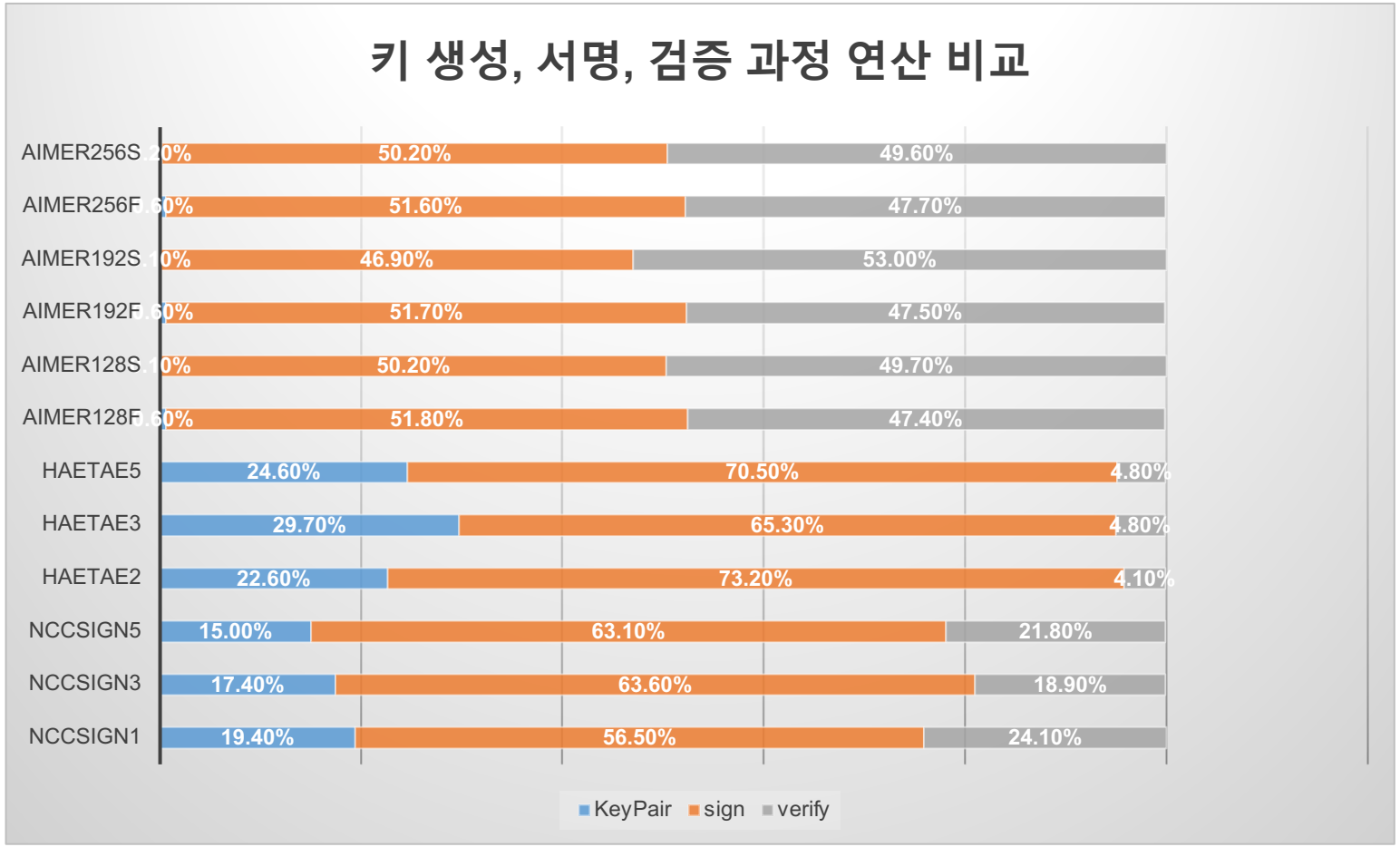
Ensure: Public key $pk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/8}$
Ensure: Secret key $sk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/4}$
1: $d \leftarrow \mathcal{B}^{32}$
2: $(f, g) := \mathsf{XOF}(d, n/2)$
3: $\mathbf{f}' := \mathsf{CBD}_1(f)$
4: $\mathbf{g}' := \mathsf{CBD}_1(g)$
5: $\mathbf{f} = 3\mathbf{f}' + 1$
6: $\mathbf{g} = 3\mathbf{g}'$
7: $\hat{\mathbf{f}} = \mathsf{NTT}(\mathbf{f})$
8: $\hat{\mathbf{g}} = \mathsf{NTT}(\mathbf{g})$
9: **if** $\hat{\mathbf{f}}$, $\hat{\mathbf{g}}$ are not invertible in R_q
10: restart
11: $\hat{\mathbf{h}} = \hat{\mathbf{g}} \circ \hat{\mathbf{f}}^{-1}$
12: $pk := \mathsf{Encode}_q(\hat{\mathbf{h}})$
13: $sk := \mathsf{Encode}_q(\hat{\mathbf{f}}) || \mathsf{Encode}_q(\hat{\mathbf{h}}^{-1})$
14: **return** (pk, sk)



특이 사항으로 inlined으로 구현된 함수는 각각 측정되서 수동으로 더해줘야 할 것으로 보임

키 생성, 서명, 검증 과정의 연산 비율

- 키 생성, 서명, 검증 과정의 연산 시간을 비율로 비교하였을 때

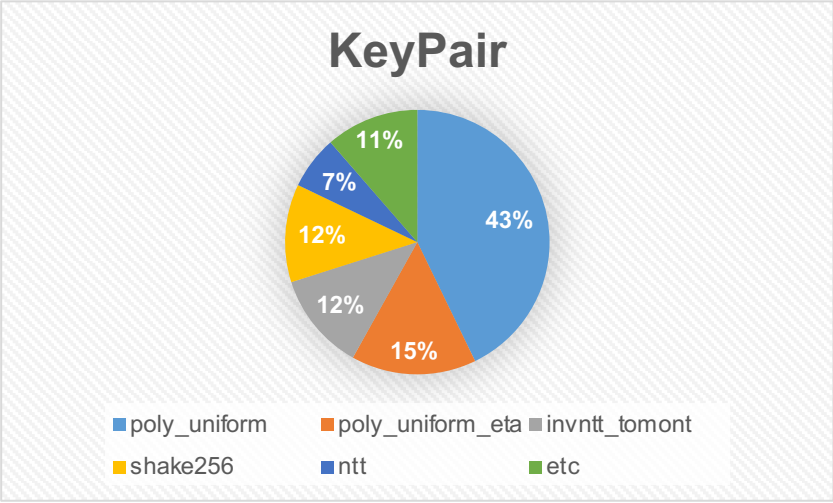


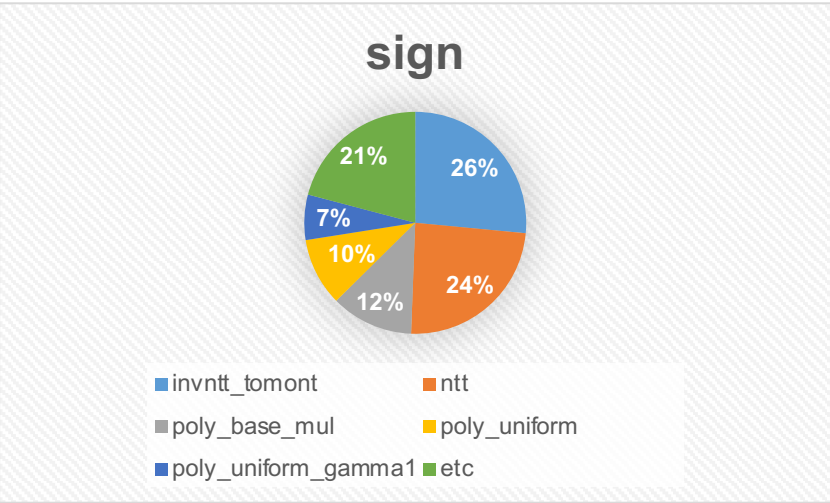
- NCCsign3

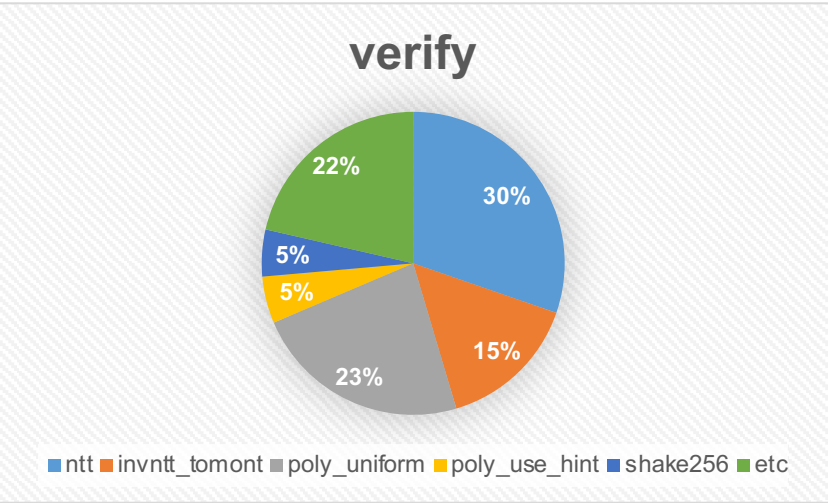
91.00 ms	100.0%	0 s	crypto_sign_keypair NCCsign
39.00 ms	42.8%	0 s	poly_uniform NCCsign
14.00 ms	15.3%	0 s	poly_uniform_eta NCCsign
11.00 ms	12.0%	2.00 ms	invntt_tomont NCCsign
11.00 ms	12.0%	0 s	shake256 NCCsign
6.00 ms	6.5%	4.00 ms	ntt NCCsign
3.00 ms	3.2%	0 s	poly_base_mul NCCsign
2.00 ms	2.1%	2.00 ms	poly_caddq NCCsign
2.00 ms	2.1%	0 s	randombytes_bsd_randombytes [inlined] NCCsign
1.00 ms	1.0%	1.00 ms	base_mul NCCsign
1.00 ms	1.0%	0 s	shake256_squeezeblocks [inlined] NCCsign
1.00 ms	1.0%	1.00 ms	poly_power2round NCCsign

331.00 ms	100.0%	1.00 ms	crypto_sign_signature NCCsign
88.00 ms	26.5%	43.00 ms	invntt_tomont NCCsign
80.00 ms	24.1%	47.00 ms	ntt NCCsign
40.00 ms	12.0%	2.00 ms	poly_base_mul NCCsign
33.00 ms	9.9%	0 s	poly_uniform NCCsign
22.00 ms	6.6%	0 s	poly_uniform_gamma1 NCCsign
14.00 ms	4.2%	10.00 ms	poly_caddq NCCsign
11.00 ms	3.3%	11.00 ms	keccak_inc_absorb NCCsign
10.00 ms	3.0%	1.00 ms	poly_decompose NCCsign
8.00 ms	2.4%	7.00 ms	poly_reduce NCCsign
7.00 ms	2.1%	7.00 ms	poly_chknorm NCCsign
5.00 ms	1.5%	5.00 ms	KeccakF1600_StatePermute NCCsign
3.00 ms	0.9%	1.00 ms	pack_sig NCCsign
3.00 ms	0.9%	2.00 ms	poly_make_hint NCCsign
2.00 ms	0.6%	1.00 ms	poly_challenge NCCsign
1.00 ms	0.3%	1.00 ms	poly_add NCCsign
1.00 ms	0.3%	1.00 ms	poly_sub NCCsign
1.00 ms	0.3%	0 s	unpack_sk NCCsign
1.00 ms	0.3%	0 s	shake256_squeezeblocks [inlined] NCCsign

99.00 ms	100.0%	0 s	crypto_sign_open NCCsign
99.00 ms	100.0%	0 s	crypto_sign_verify NCCsign
30.00 ms	30.3%	16.00 ms	ntt NCCsign
23.00 ms	23.2%	0 s	poly_uniform NCCsign
15.00 ms	15.1%	10.00 ms	invntt_tomont NCCsign
6.00 ms	6.0%	6.00 ms	KeccakF1600_StatePermute NCCsign
5.00 ms	5.0%	0 s	poly_use_hint NCCsign
5.00 ms	5.0%	0 s	poly_base_mul NCCsign
5.00 ms	5.0%	0 s	shake256 NCCsign
4.00 ms	4.0%	2.00 ms	poly_caddq NCCsign
4.00 ms	4.0%	1.00 ms	unpack_sig NCCsign
1.00 ms	1.0%	1.00 ms	polyw1_pack NCCsign
1.00 ms	1.0%	1.00 ms	keccak_inc_absorb NCCsign





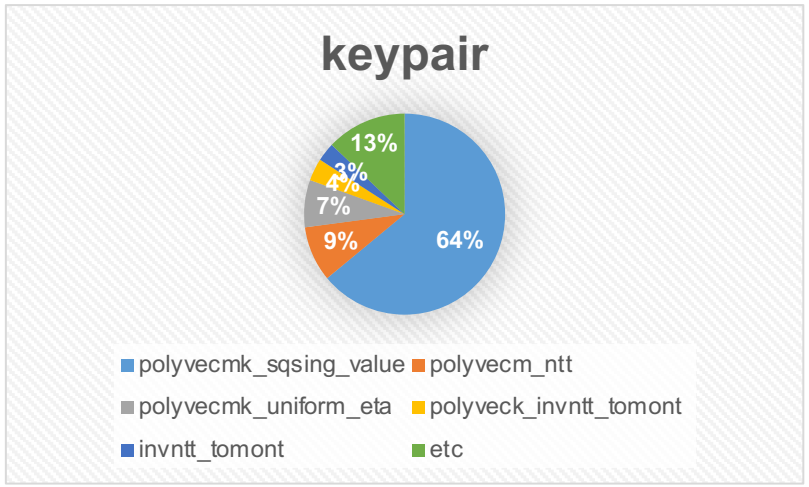


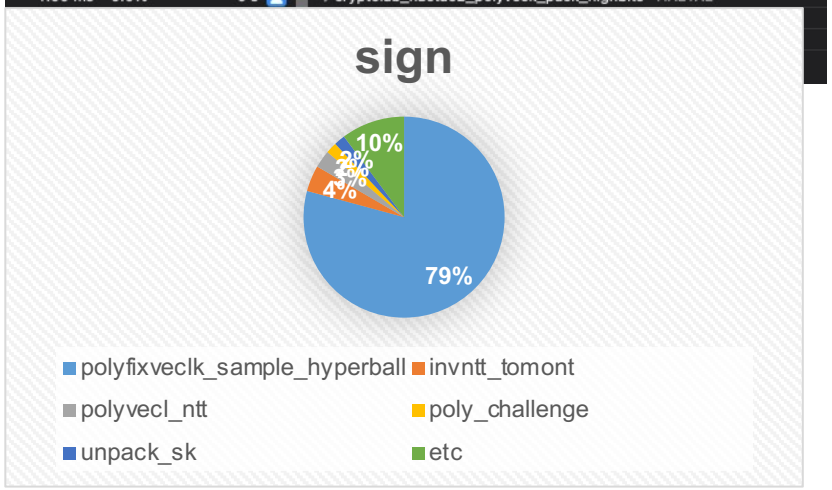
- HAETAE2

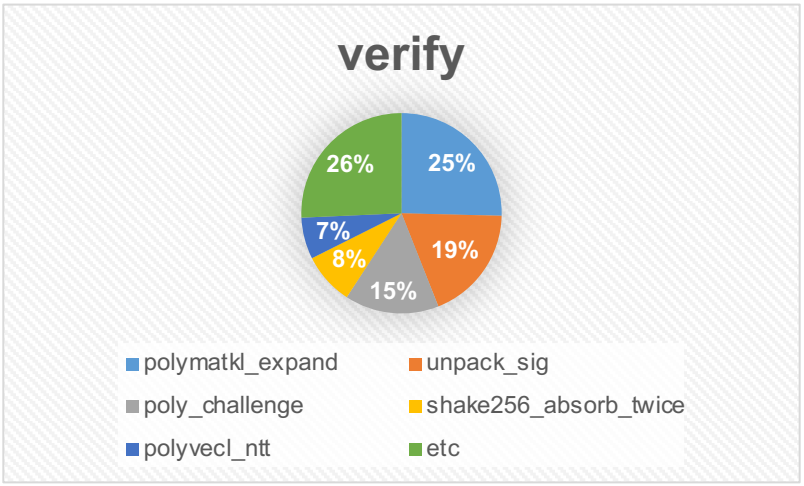
325.00 ms	100.0%	0 s	crypto_sign_keypair HAETAE
208.00 ms	64.0%	2.00 ms	cryptolab_haetae2_polyvecmk_sqsing_value HAETAE
29.00 ms	8.9%	0 s	cryptolab_haetae2_polyvecm_ntt HAETAE
25.00 ms	7.6%	0 s	cryptolab_haetae2_polyvecmk_uniform_eta HAETAE
12.00 ms	3.6%	0 s	cryptolab_haetae2_polyveck_invntt_tomont HAETAE
10.00 ms	3.0%	6.00 ms	cryptolab_haetae2_invntt_tomont HAETAE
8.00 ms	2.4%	0 s	cryptolab_haetae2_polymatkm_expand HAETAE
7.00 ms	2.1%	0 s	cryptolab_haetae2_polyvecm_pointwise_acc_montgomery HAETAE
7.00 ms	2.1%	0 s	cryptolab_haetae2_polymatkm_pointwise_montgomery HAETAE
5.00 ms	1.5%	0 s	cryptolab_haetae2_polyveck_expand HAETAE
4.00 ms	1.2%	2.00 ms	cryptolab_haetae2_polyveck_decompose_vk HAETAE
4.00 ms	1.2%	1.00 ms	cryptolab_haetae2_poly_freeze HAETAE
2.00 ms	0.6%	0 s	cryptolab_haetae2_pack_pk HAETAE
1.00 ms	0.3%	1.00 ms	cryptolab_haetae2_poly_sub HAETAE
1.00 ms	0.3%	0 s	cryptolab_haetae2_pack_sk HAETAE
1.00 ms	0.3%	0 s	cryptolab_haetae2_polyveck_freeze HAETAE
1.00 ms	0.3%	1.00 ms	cryptolab_haetae2_poly_add HAETAE

1.05 s	100.0%	0 s	crypto_sign HAETAE
1.05 s	100.0%	1.00 ms	crypto_sign_signature HAETAE
835.00 ms	79.2%	8.00 ms	cryptolab_haetae2_polyfixveclk_sample_hyperball HAETAE
46.00 ms	4.3%	34.00 ms	cryptolab_haetae2_invntt_tomont HAETAE
30.00 ms	2.8%	1.00 ms	cryptolab_haetae2_polyvecl_ntt HAETAE
20.00 ms	1.8%	1.00 ms	cryptolab_haetae2_poly_challenge HAETAE
20.00 ms	1.8%	0 s	cryptolab_haetae2_unpack_sk HAETAE
16.00 ms	1.5%	0 s	cryptolab_haetae2_polyveck_invntt_tomont HAETAE
12.00 ms	1.1%	8.00 ms	cryptolab_haetae2_ntt HAETAE
8.00 ms	0.7%	0 s	cryptolab_haetae2_polymatkl_pointwise_montgomery HAETAE
7.00 ms	0.6%	0 s	cryptolab_haetae2_pack_sig HAETAE
6.00 ms	0.5%	0 s	cryptolab_haetae2_polyfixvecl_round HAETAE
6.00 ms	0.5%	0 s	cryptolab_haetae2_polyvecl_pointwise_acc_montgomery HAETAE
5.00 ms	0.4%	0 s	cryptolab_haetae2_haetae_shake256_absorb_twice HAETAE
5.00 ms	0.4%	1.00 ms	cryptolab_haetae2_polyfixveck_round HAETAE
5.00 ms	0.4%	5.00 ms	cryptolab_haetae2_polyfixvecl_double HAETAE
5.00 ms	0.4%	1.00 ms	cryptolab_haetae2_poly_pointwise_montgomery HAETAE
4.00 ms	0.3%	4.00 ms	cryptolab_haetae2_polyfixveclk_sqnorm2 HAETAE
3.00 ms	0.2%	3.00 ms	cryptolab_haetae2_poly_pack_lsb HAETAE
2.00 ms	0.1%	0 s	cryptolab_haetae2_polyveck_highbits_hint HAETAE
2.00 ms	0.1%	0 s	cryptolab_haetae2_polyvecm_ntt HAETAE
2.00 ms	0.1%	0 s	cryptolab_haetae2_polyveck_freeze2q HAETAE
2.00 ms	0.1%	0 s	cryptolab_haetae2_polyfixvecl_add HAETAE
2.00 ms	0.1%	0 s	cryptolab_haetae2_polyvecl_highbits HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_poly_freeze2q HAETAE
1.00 ms	0.0%	1.00 ms	KeccakF1600_StatePermute HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_polyfixveck_add HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_polyvecl_lowbits HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_polyfixfixvecl_sub HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_polyveck_add HAETAE
1.00 ms	0.0%	0 s	cryptolab_haetae2_polyveck_pack_highbits HAETAE

59.00 ms	100.0%	0 s	crypto_sign_open HAETAE
59.00 ms	100.0%	0 s	crypto_sign_verify HAETAE
15.00 ms	25.4%	0 s	cryptolab_haetae2_polymatkl_expand HAETAE
11.00 ms	18.6%	0 s	cryptolab_haetae2_unpack_sig HAETAE
9.00 ms	15.2%	1.00 ms	cryptolab_haetae2_poly_challenge HAETAE
5.00 ms	8.4%	0 s	cryptolab_haetae2_haetae_shake256_absorb_twice HAETAE
4.00 ms	6.7%	0 s	cryptolab_haetae2_polyvecl_ntt HAETAE
3.00 ms	5.0%	0 s	cryptolab_haetae2_polymatkl_pointwise_montgomery HAETAE
3.00 ms	5.0%	0 s	cryptolab_haetae2_polyveck_expand HAETAE
2.00 ms	3.3%	0 s	cryptolab_haetae2_polyveck_ntt HAETAE
1.00 ms	1.6%	0 s	cryptolab_haetae2_polyvecl_pointwise_acc_montgomery HAETAE
1.00 ms	1.6%	0 s	cryptolab_haetae2_poly_reduce2q HAETAE
1.00 ms	1.6%	1.00 ms	cryptolab_haetae2_invntt_tomont HAETAE
1.00 ms	1.6%	1.00 ms	cryptolab_haetae2_poly_compose HAETAE
1.00 ms	1.6%	0 s	cryptolab_haetae2_polyveck_invntt_tomont HAETAE
1.00 ms	1.6%	0 s	cryptolab_haetae2_polyveck_sub HAETAE
1.00 ms	1.6%	1.00 ms	cryptolab_haetae2_poly_add HAETAE





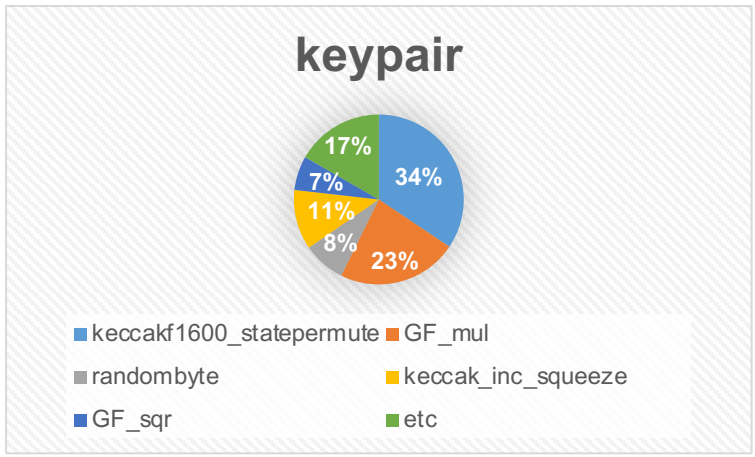


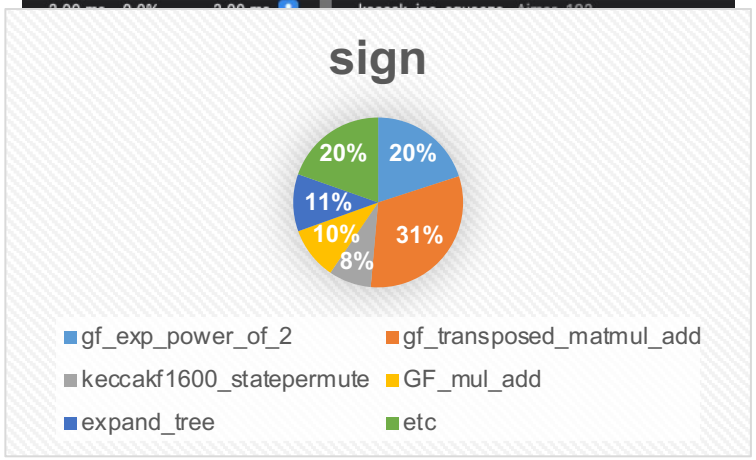
- Aimer192s

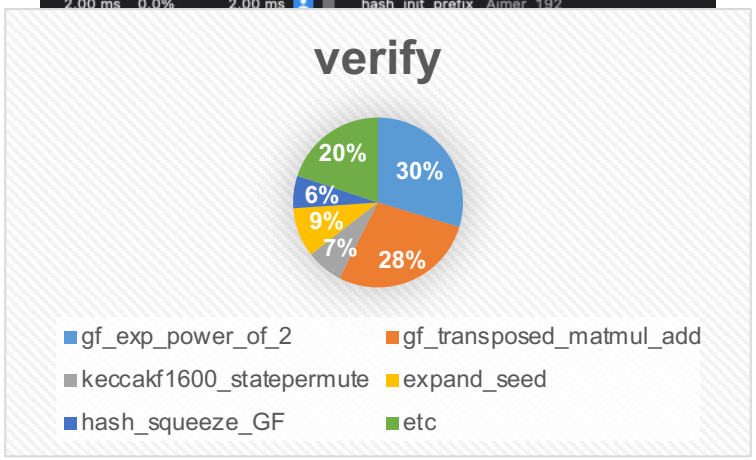
61.00 ms	100.0%	0 s	crypto_sign_keypair Aimer_192
56.00 ms	91.8%	0 s	aim2 Aimer_192
35.00 ms	57.3%	5.00 ms	generate_matrices_L_and_U Aimer_192
21.00 ms	34.4%	21.00 ms	KeccakF1600_StatePermute Aimer_192
7.00 ms	11.4%	7.00 ms	keccak_inc_squeeze Aimer_192
1.00 ms	1.6%	0 s	shake256_inc_init Aimer_192
1.00 ms	1.6%	1.00 ms	GF_from_bytes Aimer_192
20.00 ms	32.7%	1.00 ms	GF_exp Aimer_192
14.00 ms	22.9%	0 s	GF_mul Aimer_192
4.00 ms	6.5%	4.00 ms	GF_sqr Aimer_192
1.00 ms	1.6%	1.00 ms	poly64_mul Aimer_192
1.00 ms	1.6%	0 s	GF_transposed_matmul Aimer_192
5.00 ms	8.1%	0 s	randombytes_bsd_randombytes [inlined] Aimer_192

35.88 s	100.0%	0 s	crypto_sign Aimer_192
35.88 s	99.9%	0 s	aimer_sign Aimer_192
31.65 s	88.2%	33.00 ms	run_phase_1 Aimer_192
19.34 s	53.9%	43.00 ms	aim2_mpc Aimer_192
11.29 s	31.4%	8.67 s	GF_transposed_matmul_add Aimer_192
7.18 s	20.0%	342.00 ms	GF_exp_power_of_2 Aimer_192
771.00 ms	2.1%	175.00 ms	GF_mul_add Aimer_192
43.00 ms	0.1%	43.00 ms	poly64_mul Aimer_192
21.00 ms	0.0%	21.00 ms	GF_copy Aimer_192
6.50 s	18.1%	28.00 ms	commit_to_seed_and_expand_tape Aimer_192
2.49 s	6.9%	35.00 ms	hash_squeeze_GF Aimer_192
2.21 s	6.1%	2.21 s	KeccakF1600_StatePermute Aimer_192
1.10 s	3.0%	0 s	hash_init [inlined] Aimer_192
454.00 ms	1.2%	454.00 ms	keccak_inc_absorb Aimer_192
191.00 ms	0.5%	191.00 ms	keccak_inc_squeeze Aimer_192
14.00 ms	0.0%	0 s	shake256_inc_finalize Aimer_192
9.00 ms	0.0%	0 s	hash_update [inlined] Aimer_192
2.00 ms	0.0%	2.00 ms	hash_init_prefix Aimer_192
1.00 ms	0.0%	1.00 ms	shake256_inc_init Aimer_192
3.92 s	10.9%	3.00 ms	expand_tree Aimer_192
730.00 ms	2.0%	730.00 ms	KeccakF1600_StatePermute Aimer_192
378.00 ms	1.0%	378.00 ms	keccak_inc_absorb Aimer_192
364.00 ms	1.0%	52.00 ms	GF_mul_add Aimer_192
215.00 ms	0.5%	0 s	generate_matrix_LU Aimer_192
83.00 ms	0.2%	83.00 ms	GF_add Aimer_192
18.00 ms	0.0%	18.00 ms	GF_copy Aimer_192
16.00 ms	0.0%	16.00 ms	GF_exp_power_of_2 Aimer_192
15.00 ms	0.0%	1.00 ms	GF_exp Aimer_192
14.00 ms	0.0%	14.00 ms	poly64_mul Aimer_192
13.00 ms	0.0%	0 s	aim2_sbox_outputs Aimer_192
6.00 ms	0.0%	6.00 ms	hash_squeeze_GF Aimer_192
3.00 ms	0.0%	3.00 ms	hash_init_prefix Aimer_192

40.53 s	100.0%	0 s	crypto_sign_open Aimer_192
40.49 s	99.8%	93.00 ms	aimer_verify Aimer_192
24.28 s	59.8%	61.00 ms	aim2_mpc Aimer_192
12.06 s	29.7%	328.00 ms	GF_exp_power_of_2 Aimer_192
11.27 s	27.8%	8.71 s	GF_transposed_matmul_add Aimer_192
816.00 ms	2.0%	70.00 ms	GF_mul_add Aimer_192
44.00 ms	0.1%	44.00 ms	GF_copy Aimer_192
20.00 ms	0.0%	20.00 ms	poly64_mul Aimer_192
6.56 s	16.1%	23.00 ms	commit_to_seed_and_expand_tape Aimer_192
2.53 s	6.2%	22.00 ms	hash_squeeze_GF Aimer_192
2.13 s	5.2%	2.13 s	KeccakF1600_StatePermute Aimer_192
1.13 s	2.7%	0 s	hash_init [inlined] Aimer_192
483.00 ms	1.1%	483.00 ms	keccak_inc_absorb Aimer_192
231.00 ms	0.5%	231.00 ms	keccak_inc_squeeze Aimer_192
12.00 ms	0.0%	0 s	shake256_inc_finalize Aimer_192
9.00 ms	0.0%	0 s	hash_update [inlined] Aimer_192
3.00 ms	0.0%	2.00 ms	hash_init_prefix Aimer_192
3.85 s	9.5%	7.00 ms	reconstruct_seed_tree Aimer_192
2.93 s	7.2%	286.00 ms	GF_mul_add Aimer_192
1.18 s	2.9%	13.00 ms	hash_update_GF Aimer_192
732.00 ms	1.8%	732.00 ms	KeccakF1600_StatePermute Aimer_192
414.00 ms	1.0%	414.00 ms	keccak_inc_absorb Aimer_192
226.00 ms	0.5%	1.00 ms	generate_matrix_LU Aimer_192
116.00 ms	0.2%	116.00 ms	poly64_mul Aimer_192
50.00 ms	0.1%	50.00 ms	GF_copy Aimer_192
17.00 ms	0.0%	17.00 ms	GF_add Aimer_192
14.00 ms	0.0%	7.00 ms	hash_squeeze_GF Aimer_192
13.00 ms	0.0%	13.00 ms	GF_exp_power_of_2 Aimer_192
8.00 ms	0.0%	8.00 ms	_platform_memset libsystem_platform.dylib
3.00 ms	0.0%	3.00 ms	expand_seed Aimer_192
2.00 ms	0.0%	0 s	hash_init [inlined] Aimer_192







Q & A