Supporting Document of Performance Analysis and KAT

1 Detailed performance analysis (2.B.2)

1.1 Description of Platform

We collect our analysing data on a computer with an Intel Core (TM) i5-5200U (broadwell) CPU running at 2.2 GHz, Turbo Boost is disabled. The computer has 4GB of RAM and runs Ubuntu 16.04. Our gcc compiler version is gcc 5.4.0 20160609. The compiler list is reduced to just gcc -g -Wall -O3.

1.2 Time

To get the speed result of our four KEM schemes, we run each function 50000 times and take their average CPU running cycles. We record CPU cycles of key generation (Keypair), encapsulation (Enc) and decapsulation (Dec) functions for different schemes in the following table.

	Keypair	Enc	Dec
$OKCN\text{–}MLWE$	343023	411204	85215
$AKCN\text{–}MLWE$	338215	395116	83455
$OKCN\text{–}RLWE$	428257	703104	176481
$AKCN\text{–}RLWE$	433536	715307	192306

Table 1. Average CPU running cycles for functions in different schemes.

To get the speed result of our CCA-Secure PKE scheme, we also run each function 50000 times and take their average CPU running cycles. We record CPU cycles of key generation (Keypair), encrypt and decrypt functions for different message length (Bytes) in the following table.

Message Length	Keypair	encrypt	decrypt
16	489406	566745	646412
24	473845	562880	636398
32	481881	568461	630891
5000	473558	695933	815433
10000	484476	865030	1081841
15000	480951	975064	1178312
20000	474667	1156497	1392171

Table 2. Average CPU running cycles of functions for different message length.

1.3 Space

Sizes for important variables are straightforwardly calculated from parameters. Specifically, bytes are given for public key, secret key, cipher text and shared secret (pk, sk, ct and ss) for different KEM schemes in the following table.

	pk	sk	ct	ss
$OKCN\text{–}MLWE$	992	288	1120	32
$AKCN\text{–}MLWE$	991	288	1120	32
$OKCN\text{–}RLWE$	1696	1664	1955	95
$AKCN\text{–}RLWE$	1696	1664	2083	95

Table 3. Sizes for public key, secret key, cipher text and shared secret (pk, sk, ct and ss).

For our CCA-Secure PKE scheme, bytes for the public key, secret key and maxim length of overhead in an encrypted message compared to the original message are 992, 1312 and 1168, respectively.

2 Known Answer Test (KAT) (2.B.3)

There are KAT files for each scheme in the KAT folder. We generate all KAT require and response files according to the NIST instructions. We also provide KAT input output tuples files for 3 aspects (keypair generation, encapsulation and decapsulation) of our kem schemes and 3 aspects (keypair generation, encryption and decryption) of our CCA-Secure PKE scheme. We believe they are informative for debugging and understanding our implementation.