Energy Consumption of Candidate Algorithms for NIST PQC Standards

Tanushree Banerjee and M. Anwar Hasan
Department of Electrical and Computer Engineering
University of Waterloo
{tanushree.banerjee, ahasan}@uwaterloo.ca

Abstract

In 2016, NIST (National Institute of Standards and Technology) announced a formal call for submissions of public key post-quantum cryptoschemes. This is part of a process for NIST to develop and standardize one or more quantum-resistant public-key cryptographic algorithms on the basis of their security, performance and other properties. For battery operated devices such as mobile phones and sensors, energy consumption due to execution of cryptographic algorithms implemented in software is a very important consideration. In this article, we report the energy consumption of all the submissions, while they are executed on 64 bit Intel 6700 Skylake Processor, 3.4 GHz. We consolidate our energy consumption data based on security level and cryptographic operation. An overwhelming majority of the candidate algorithms are categorized as either lattice, code or multi-variate based, and we identify leading energy efficient schemes from each category.

1 Introduction

Quantum-safe cryptoschemes refer to the cryptographic algorithms that are secure against both classical and quantum computers. In the recent years a lot of research has been done on post-quantum cryptography. The motive behind these research is that, if large scale quantum computers become a reality, then current cryptographic algorithms would require replacement by quantum-safe cryptoschemes. This is because quantum computers would completely break many public-key cryptosystems, including RSA, DSA, and elliptic curve cryptosystems. Therefore, before this situation turns more critical, NIST decided the process of developing standards for post-quantum cryptography [1]. Currently there are quite a few post quantum cryptoschemes such as lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, hash-based signatures, etc. The new post-quantum cryptography standards will be used as quantum resistant counterparts to existing standards, including digital signature schemes specified in Federal Information Processing Standards Publication (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SP) 800-56 A and B. Further, this process would also help in the transition from usage of public key cryptoschemes to post quantum cryptoschemes, before quantum computers come into physical existence.

All the submissions to the NIST post-quantum standardization process are available for public scrutiny and are being evaluated based on security, performance and other properties by various stakeholders including the cryptographic community. Although not explicitly part of the evaluation criteria, energy consumption due to the execution of cryptographic algorithms is a very important consideration for battery operated devices such as mobile phones and sensors. If an algorithm's energy consumption on a certain platform is known, then one can easily estimate how many times the algorithm can be executed on the platform before its battery is completely exhausted, providing an added aspect to be considered while deciding the deployment of the algorithm in energy constrained environments. Therefore, the idea of this investigation is to measure the energy efficicency of each of these candidate algorithms. In this article, we execute the software implementation of all the submissions on a x64 Intel Skylake 6700 processor and monitor the amount of power they are using. This in turn gives us the average energy consumption of these crypto algorithms. We also consolidate our energy consumption data based on security levels and cryptographic functions of the submissions. More than fifty submissions are categorized as either lattice, code or multivariate based, and we identify leading energy efficient schemes from each category.

All submissions are available on the NIST website [2] and include detailed description of the proposed algorithms along with reference to relevant articles. For brevity, overviews of those algorithms are not provided here and the rest of the article is organised as follows. The next section mentions the methodology used in this investigation. Section 3 provides the energy consumption values corresponding to all these implementations in tabular form alongwith some comments. Lastly, concluding remarks are provided in Section 4.

2 Methodology

Initially there had been 69 submissions, out of which 5 were broken in terms of security by the time NIST held the first post-quantum cryptography standardization conference in April 2018. In this study, we omit those five submissions. All candidate algorithms include the software implementations for different security levels mentioned by NIST. In this investigation, these codes are built on Linux Subsystem (with Ubuntu 16.04), which is a compatibility layer for running Linux binary executables natively on Windows, with gcc 5.4. The processor used is a 64 bit Intel 6700 Skylake processor, 3.4 GHz with 4 cores and 8 MB smart cache. Power usage during execution of these programs are measured using Intel Power Gadget 3.5. It is a software-based power usage monitoring tool enabled for Intel Core processors. It supports Windows OS, where a set of driver and libraries can access the processor energy counter to calculate the power usage in Watts, which is collected at an user defined sampling rate and logged onto a .csv file. Intel Power Gadget has only its Windows version available for this particular Skylake processor. Therefore, the C implementations are built on Linux Subsystem and the corresponding power is measured on the gadget. It has been tested that with respect to execution time of the implementations, they are exactly same irrespective of execution on an independent Ubuntu operating system or Linux Subsystem. All the implemented algorithms are executed for 100 times to measure their execution time and also record their average power usage. Energy consumption is computed using the execution time and power usage data. In all the tables in this article, execution time is reported in milliseconds and energy consumption is reported in milliJoules.

According to the criteria set by NIST, there are broadly three different kinds of submissions:

- Public Key Signatures
- Public Key Encryption
- Key Encapsulation Mechanism

In signature schemes the subroutines that are benchmarked, their definitions are given below:

```
int crypto_sign_keypair(unsigned char *pk,
unsigned char *sk)

int crypto_sign(unsigned char *sm,
unsigned long long *smlen,const
unsigned char *m, unsigned long long mlen,
const unsigned char *sk)

int crypto_sign_open(
unsigned char *m, unsigned long long *mlen,
const unsigned char *sm,
unsigned long long smlen,
const unsigned char *pk)
```

They are responsible for private and public keypair generation, signing of message, followed by verification of the signature. Similarly, key encryption scheme is supposed to include keypair generation, encryption of the message to generate cipher text and then decryption of the cipher as follows :

```
int crypto_encrypt_keypair(
unsigned char *pk,
unsigned char *sk)

int crypto_sign(
unsigned char *sm,
unsigned long long *smlen,
const unsigned char *m,
unsigned long long mlen,
const unsigned char *sk)
```

```
int crypto_sign_open(
unsigned char *m,
unsigned long long *mlen,
const unsigned char *sm,
unsigned long long smlen,
const unsigned char *pk)
```

Lastly, encapsulation scheme includes key pair generation, encapsulation of the message and finally decapsulation as shown below :

```
 int crypto_kem_keypair(
unsigned char *pk,
unsigned char *sk)

int crypto_kem_enc(
unsigned char *ct,
unsigned char *ss,
const unsigned char *pk)

int crypto_kem_dec(
unsigned char *ss,
const unsigned char *ct,
const unsigned char *sk)
```

NIST has also recommended some guidelines and format for all of these subroutines such as additional functions that are to be used in these subroutines. The key pair generation subroutines require random input generation which is done using the SUPERCOP package [66]. In this study when these subroutines for key generation, encryption, encapsulation, signing etc are benchmarked on the above mentioned processor, the whole subroutine's power usage and execution time is used to report the energy consumption. That is in the power usage and energy consumption results, the subroutine for random number generation's contribution is also there. Moreover, NIST has provided its classification on the range of security strengths offered by the existing NIST standards in symmetric cryptography, which is expected to offer significant resistance to quantum cryptanalysis. 5 main security levels [1] have been provided for this purpose as follows :

- Level I: It should be at least as hard as that of breaking the security of block cipher using exhaustive key search with 128 bit key, example AES 128.
- Level II: It should be at least as hard as that of breaking the security of hash function using collision search with 256 bit hashed message digest, example SHA256/ SHA3-256
- Level III: It should be at least as hard as that of breaking the security of block cipher using exhaustive key search with 192 bit key, example AES 192.
- Level IV: It should be at least as hard as that of breaking the security of hash function using collision search with 384 bit hashed message digest, example SHA384/ SHA3-384
- Level V: It should be at least as hard as that of breaking the security of block cipher using exhaustive key search with 256 bit key, example AES 256.

Now, not all the candidate algorithms have implementations corresponding to the 5 above mentioned security levels. In order to make a fair comparison of the schemes on the basis of their power usage and energy consumptions, they are grouped into different categories that is encapsulation/encryption or signature and also in different security levels according to availability in the submissions, as shown in the next section. It should be noted that different schemes use different lengths of message according to their structure. Also in signtaure scheme's execution time and power usage depends on the length of the message getting signed. For the purpose of a fair comparison, the largest message block size mentioned in the supporting documentation, is considered during the benchmarking of the signature scheme codes and also for its corresponding energy consumption.

The implementations submitted in this event include C codes as well as vectorised codes. Again not all submissions have provided with vectorised instructions for speed ups. Therefore in order to make a reasonable comparison, the "optimised implementation" of all the submissions are considered which only includes C implementation without any vectorization. Some of the encryption/encapsulation submissions have provided implementations which are secure specifically against chosen ciphertext attack or chosen plaintext attack. These

Table 1: Energy consumption during **Key Generation of Public Key Signature schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
CRYSTALSDilithium [3]	24.98	0.04	0.99	25.17	0.06	1.51	25.21	0.09	2.26	24.6	0.12	2.96	-	-	-
DRS [4]	25.34	452.02	11454. 18	-	-	-	25.77	454.12	11702.67	-	-	-	25.61	456.78	11698.13
DualModeMS [5]	26.41	698131	**18437639.71**	-	-	-	-	-	-	-	-	-	-	-	-
FALCON [6]	25.32	6.29	159.26				26.05	11.6	302.18				25.12	19.04	497.32
GeMSS [7]	26.67	33.43	891.57	-	-	-	25.93	142.34	3690.87	-	-	-	26.18	358.94	9397.04
Gravity SPHINCS [8]	-	-	-	26.57	388.23	10315.27	-	-	-	-	-	-	-	-	-
Gui [9]	26.34	623	16409.82	-	-	-	26.12	25337	**661802.44**	-	-	-	25.7	92346	**2373292.2**
HiMQ3 [10]	24.88	0.02	0.49	-	-	-	-	-	-	-	-	-	-	-	-
HiMQ3F	24.78	0.03	0.74	-	-	-	-	-	-	-	-	-	-	-	-
LUOV [11]	-	-	-	26.67	7	186.69	-	-	-	26.55	31.2	828.36	26.93	57.8	1556.554
MQDSS [12]	-	-	-	26.12	0.85	22.2	-	-	-	26.62	1.97	52.44	-	-	-
pqNTRUSign Gaussian	-	-	-	-	-	-	-	-	-	-	-	-	27.13	48.75	1322.58
pqNTRUSign Uniform	-	-	-	-	-	-	-	-	-	-	-	-	27.05	47.34	1280.54
Picnic-FS [13]	25.67	0.005	0.13	-	-	-	25.92	0.016	**0.41**	-	-	-	25.34	0.032	**0.81**
Picnic-UR	27.05	0.004	**0.1**	-	-	-	26.93	0.017	0.46	-	-	-	27.13	0.04	1.08
Post-Quantum RSA Sign [14]	-	-	-	27.45	1350.26	3706463.7	-	-	-	-	-	-	-	-	-
pqsigRM [15]	26.78	5260	140862.8	-	-	-	26.79	1026.17	27491.09	-	-	-	27.1	13553.2	367291.72
qTESLA [16]	26.85	0.94	25.23	-	-	-	26.66	1.39	37.05	-	-	-	27.11	2.94	79.7
RaCoSS [17]	25.74	200.4	5158.296	-	-	-	-	-	-	-	-	-	-	-	-
Rainbow [18]	27.13	367.33	9965.66	26.97	1449.09	39081.95	27.43	21248.7	582851.84	27.11	13801.8	374166.79	27.52	47220.97	1299521.09
SPHINCS Plus(SHA256F) [19]	26.38	2.75	72.545	-	-	-	26.86	4.99	134.03	-	-	-	27.11	18.76	508.58
SPHINCS Plus(SHA256S)	25.99	84.43	2194.33	-	-	-	26.32	163.73	4309.37	-	-	-	27.05	299.53	8102.28
SPHINCS Plus(SHAKE256F)	27.36	5.28	144.46	-	-	-	27.84	7.87	219.1	-	-	-	27.33	22.64	618.75
SPHINCS Plus(SHAKE256S)	26.98	171.35	4623.02	-	-	-	27.02	250.7	6773.91	-	-	-	26.94	320.33	8629.69
Walnut BKL [20]	26.53	0.27	7.16	-	-	-	26.67	0.6	16	-	-	-	-	-	-
Walnut StochasticWrite	26.45	0.27	7.14	-	-	-	26.92	0.6	16.15	-	-	-	-	-	-
Walnut Dehornoy	25.81	0.27	6.96	-	-	-	26.32	0.63	16.58	-	-	-	-	-	-

Table 2: Energy consumption during **Signing of Public Key Signature schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
CRYSTALSDilithium	26.78	0.18	4.82	27.32	0.3	8.19	26.89	0.42	11.29	25.12	0.41	10.29	-	-	-
DRS	27.34	22.9	626	-	-	-	26.81	25.51	683.91	-	-	-	27.11	26.28	712.45
DualModeMS	26.27	1846	48494.42	-	-	-	-	-	-	-	-	-	-	-	-
FALCON	26.73	0.145	3.87	-	-	-	26.88	0.23	**6.18**	-	-	-	27.01	0.28	**7.56**
GeMSS	26.79	318.96	8544.93	-	-	-	26.52	729.75	19352.97	-	-	-	27.18	1106.32	30069.77
Gravity SPHINCS	-	-	-	26.73	1.68	44.9	-	-	-	-	-	-	-	-	-
Gui	25.83	31.4	811.06	-	-	-	26.12	11343	**296279.16**	-	-	-	26.78	474589	**12709493.42**
HiMQ3	25.87	0.012	**0.31**	-	-	-	-	-	-	-	-	-	-	-	-
HiMQ3F	25.02	0.035	0.87	-	-	-	-	-	-	-	-	-	-	-	-
LUOV	-	-	-	25.88	26.8	693.58	-	-	-	26.11	80.6	2104.46	26.32	163.3	4298.05
MQDSS	-	-	-	26.33	70.36	1852.57	-	-	-	26.48	222.43	5889.94	-	-	-
pqNTRUSign Gaussian	-	-	-	-	-	-	-	-	-	-	-	-	26.65	107.81	2873.13
pqNTRUSign Uniform	-	-	-	-	-	-	-	-	-	-	-	-	26.94	63.59	1713.11
Picnic-FS	27.54	3.2	88.12	-	-	-	26.33	12.38	325.96	-	-	-	26.94	47.25	1272.91
Picnic-UR	26.5	4.2	111.3	-	-	-	26.78	16.2	433.83	-	-	-	27.11	50.34	1364.71
Post-Quantum RSA Sign	-	-	-	28.01	43.42	1216.19	-	-	-	-	-	-	-	-	-
pqsigRM	26.46	25684.8	**679619.80**	-	-	-	26.53	1846.5	49462.5	-	-	-	26.82	1754.8	47063.73
qTESLA	26.39	0.62	16.36	-	-	-	25.94	3.59	93.12	-	-	-	26.07	6.79	177.01
RaCoSS	26.26	10.15	266.53	-	-	-	-	-	-	-	-	-	-	-	-
Rainbow	25.72	0.21	5.4	26.01	0.53	13.78	25.97	3.2	83.1	26.14	2.31	60.38	26.1	3.87	101
SPHINCS Plus(SHA256F)	26.89	86.91	2337	-	-	-	26.2	137.33	3598.04	-	-	-	25.72	426.53	10970.35
SPHINCS Plus(SHA256S)	27.04	1298.11	35100.89	-	-	-	26.79	3527.1	94491	-	-	-	26.78	3641.14	97509.73
SPHINCS Plus(SHAKE256F)	28.06	153.93	4319.27	-	-	-	27.96	208.62	5833.01	-	-	-	28.12	512.84	14421.06
SPHINCS Plus(SHAKE256S)	25.74	2399.61	61765.96	-	-	-	26.14	5057.47	132202.26	-	-	-	26.37	3627.23	95650.055
Walnut BKL	27.15	20.19	548.15	-	-	-	26.73	69.71	1863.34	-	-	-	-	-	-
Walnut StochasticWrite	26.93	9.56	257.45	-	-	-	27.18	25.47	692.27	-	-	-	-	-	-
Walnut Dehornoy	27.43	9.1	249.61	-	-	-	26.87	24.4	655.62	-	-	-	-	-	-

schemes are separately evaluated based on their security against the attacks as shown in the tables below. Also quite a few of the submissions have provided both encryption and encapsulation algorithms, hence it can be seen that their submission names are repeated in the tables for encapsulation and encryption. It should be noted in few of the submissions, there are algorithms with same security levels but different probability of error in decryption or verification etc. For such submissions, the algorithm with least probability of error is considered in this article.

3 Energy efficiency

3.1 Public Key Signatures

Amongst the 64 valid candidate algorithms, 19 include signing and verification schemes as shown below in Tables 1, 2 and 3. These tables provide the energy consumption of the algorithms when they were executed on a 64 bit processor laptop (Intel 6700 Skylake). We have observed that their power usages do not vary much across all these schemes. It is around 24-28 Watts in general. The energy consumption of the implementations are mostly influenced by their execution times. Some of the submissions such as pqNTRUSign, SPHINCS Plus, Walnut, as it can be seen have provided multiple variants of the same algorithm using different parameters.

Table 3: Energy consumption during **Verification of Public Key Signature schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
CRYSTALSDilithium	26.13	0.04	1.04	25.97	0.07	1.81	25.38	0.10	2.53	24.67	0.13	3.2	-	-	-
DRS	26.34	222.71	5866.18	-	-	-	26.17	224.68	**5879.87**	-	-	-	25.69	226.95	**5830.34**
DualModeMS	26.36	1913	**50426.68**	-	-	-	-	-	-	-	-	-	-	-	-
FALCON	25.83	0.025	**0.64**	-	-	-	26.13	0.044	**1.15**	-	-	-	26.93	0.052	**1.4**
GeMSS	27.19	0.067	1.82	-	-	-	26.82	0.143	3.83	-	-	-	26.87	0.394	10.58
Gravity SPHINCS	-	-	-	26.69	0.01	0.26	-	-	-	-	-	-	-	-	-
Gui	27.25	0.045	1.23	-	-	-	26.88	0.347	9.32	-	-	-	27.12	0.689	18.68
HiMQ3	26.82	0.075	2.01	-	-	-	-	-	-	-	-	-	-	-	-
HiMQ3F	24.89	0.087	2.16	-	-	-	-	-	-	-	-	-	-	-	-
LUOV	-	-	-	25.93	16.5	427.84	-	-	-	26.05	44.5	1159.22	26.31	83.9	2207.4
MQDSS	-	-	-	27.11	52.35	1419.2	-	-	-	26.98	167.18	4510.51	-	-	-
pqNTRUSign Gaussian	-	-	-	-	-	-	-	-	-	-	-	-	27.11	1.25	33.88
pqNTRUSign Uniform	-	-	-	-	-	-	-	-	-	-	-	-	26.45	1.87	49.46
Picnic-FS	26.11	2.2	57.44	-	-	-	25.67	8.34	214.08	-	-	-	26.06	30.9	805.25
Picnic-UR	27.43	3.11	85.3	-	-	-	26.97	11.36	306.37	-	-	-	27.05	34.64	937.01
Post-Quantum RSA Sign	-	-	-	28.05	5.78	162.13	-	-	-	-	-	-	-	-	-
pqsigRM	26.12	81.1	2118.33	-	-	-	26.45	58.57	1549.17	-	-	-	26.67	298.92	7972.19
qTESLA	27.32	0.12	3.28	-	-	-	27.26	0.25	6.81	-	-	-	26.96	0.32	8.63
RaCoSS	26.58	9.86	262.07	-	-	-	-	-	-	-	-	-	-	-	-
Rainbow	26.13	0.11	2.87	26.45	0.43	11.37	26.82	3.1	83.14	26.23	1.52	39.86	26.71	3.28	87.6
SPHINCS Plus(SHA256F)	26.63	3.65	97.2	-	-	-	26.41	7.37	194.64	-	-	-	25.89	10.57	273.65
SPHINCS Plus(SHA256S)	27.11	1.44	39.03	-	-	-	26.94	2.92	78.66	-	-	-	27.04	5.54	149.8
SPHINCS Plus(SHAKE256F)	25.34	6.57	166.48	-	-	-	26.08	11.2	292.09	-	-	-	26.12	12.2	318.66
SPHINCS Plus(SHAKE256S)	26.87	3.04	81.68	-	-	-	26.31	4.45	117.07	-	-	-	25.89	5.3	137.21
Walnut BKL	26.42	0.22	5.81	-	-	-	26.78	0.77	20.62	-	-	-	-	-	-
Walnut StochasticWrite	27.02	0.11	2.97	-	-	-	27.31	0.31	8.46	-	-	-	-	-	-
Walnut Dehornoy	26.91	0.12	3.23	-	-	-	27.33	0.35	9.56	-	-	-	-	-	-

Table 4: Energy consumption during **Keypair generation of Public Key Encryption schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
Compact LWE [21]	-	-	-	-	-	-	26.93	0.163	4.39	-	-	-	-	-	-
GiophantusR [22]	26.34	12.14	319.76	-	-	-	26.78	22.03	589.96	-	-	-	27.04	32.16	869.6
Guess Again [23]	-	-	-	-	-	-	-	-	-	-	-	-	27.67	38.7	1070.82
AKCN MLWE [24]	-	-	-	-	-	-	-	-	-	26.89	0.153	4.11	-	-	-
KINDI-ENCRYPT [25]	-	-	-	-	-	-	26.53	0.07	**1.85**	-	-	-	26.71	0.16	4.27
LAC [26]	-	-	-	28.1	0.026	0.73	-	-	-	27.88	0.085	2.36	27.87	0.088	**2.45**
LEDA PKC [27]	26.89	16.66	447.98	-	-	-	26.34	70.31	1851.96	-	-	-	26.88	201.562	5417.93
LIMA CCA [28]	27.17	0.42	11.41	27.03	0.77	20.81	27.56	0.86	23.7	-	-	-	27.45	1.53	41.99
LIMA CPA	26.94	0.42	11.31	27.04	0.77	20.82	26.76	0.86	23.01	-	-	-	27.02	1.53	41.34
Lizard CCA [29]	26.54	10.78	286.1	-	-	-	26.98	24.06	649.13	-	-	-	27.05	42.81	1158.01
RLizard CCA	26.78	0.04	**1.07**	-	-	-	26.93	0.08	2.15	-	-	-	27.04	0.1	2.7
LOTUS Encrypt [30]	27.09	9.79	265.21	-	-	-	26.63	18.91	503.57	-	-	-	27.15	26.34	715.13
McNIE 3Q [31]	27.17	109.1	**2964.24**	-	-	-	27.52	193.2	**5316.86**	-	-	-	28.2	336.78	**9497.2**
McNIE 4Q	26.89	95.02	2555.08	-	-	-	27.34	166.32	4547.18	-	-	-	27.97	336.72	9418.05
NTRUEncrypt PKE [32]	26.72	0.33	8.81	-	-	-	25.94	1.04	26.97	-	-	-	26.37	39.58	1043.72
Round2-u Encrypt [33]	27.14	0.25	6.78	26.88	0.42	11.29	27.07	0.58	15.7	27.45	0.6	16.47	27.62	0.62	17.12
Round2-n Encrypt	28.32	2.58	73.06	28.05	3.76	105.46	27.96	4.02	112.4	27.59	6.06	167.19	28.32	8.34	236.18
Titanium CPA [34]	27.14	0.61	16.55	-	-	-	27.39	0.6	16.43	-	-	-	27.26	0.85	23.17

Table 5: Energy consumption during **Keypair encryption of Public Key Encryption schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
Compact LWE	-	-	-	-	-	-	26.44	2.87	75.88	-	-	-	-	-	-
GiophantusR	26.36	22.01	**580.18**	-	-	-	26.4	49.88	**1316.83**	-	-	-	26.43	78.99	2097.7
Guess Again	-	-	-	-	-	-	-	-	-	-	-	-	27.06	2634	**71276.04**
AKCN MLWE	-	-	-	-	-	-	-	-	-	25.49	0.38	9.68	-	-	-
KINDI-ENCRYPT	-	-	-	-	-	-	27.11	0.09	2.43	-	-	-	26.68	0.2	5.33
LAC	-	-	-	26.59	0.04	1.28	-	-	-	26.83	0.13	3.38	26.4	0.16	4.32
LEDA PKC	27.08	4.68	126.73	-	-	-	26.95	15.1	406.94	-	-	-	27.34	40.1	1096.33
LIMA CCA	26.33	0.37	9.74	26.67	0.68	18.13	26.7	0.75	20.02	-	-	-	26.73	1.41	37.68
LIMA CPA	27.53	0.38	10.46	27.74	0.69	19.14	27.56	0.77	21.22	-	-	-	27.5	1.4	38.5
Lizard CCA	26.89	0.02	**0.54**	-	-	-	27.45	0.048	**1.31**	-	-	-	27.32	0.07	**1.91**
RLizard CCA	27.16	0.02	**0.54**	-	-	-	27.2	0.05	1.36	-	-	-	27.35	0.07	**1.91**
LOTUS Encrypt	26.12	0.08	2.09	-	-	-	26.31	0.11	2.89	-	-	-	27.07	0.19	5.14
McNIE 3Q	26.81	1.03	27.61	-	-	-	26.53	2.09	55.44	-	-	-	26.71	3.12	83.33
McNIE 4Q	27.13	0.12	3.25	-	-	-	26.97	1.54	41.53	-	-	-	27.02	3.32	89.7
NTRUEncrypt PKE	26.86	0.06	1.61	-	-	-		0.09	2.41	-	-	-	26.49	61.66	1633.37
Round2-u Encrypt	27.68	0.31	8.58	27.21	0.52	14.15	27.32	0.69	18.85	27.16	0.74	20.09	27.54	0.77	21.2
Round2-n Encrypt	26.88	5.37	144.34	26.74	7.87	210.44	26.85	8.6	230.91	26.94	13.98	376.62	27.03	12.21	330.03
Titanium CPA	26.85	0.56	15.036	-	-	-	26.92	0.56	15.07	-	-	-	26.86	0.82	22.02

Table 6: Energy consumption during **Keypair decryption of Public Key Encryption schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
Compact LWE	-	-	-	-	-	-	26.59	0.35	9.3	-	-	-	-	-	-
GiophantusR	26.56	41.31	**1097.2**	-	-	-	26.73	94.37	**2522.51**	-	-	-	26.83	151.34	4060.45
Guess Again	-	-	-	-	-	-	-	-	-	-	-	-	27.23	1.38	37.57
AKCN MLWE	-	-	-	-	-	-	-	-	-	25.78	0.451	11.6	-	-	-
KINDI-ENCRYPT	-	-	-	-	-	-	26.83	0.11	2.95	-	-	-	25.94	0.25	6.48
LAC	-	-	-	27.12	0.03	0.76	-	-	-	26.94	0.096	2.58		27.57 0.104	2.8
LEDA PKC	27.49	28.12	773	-	-	-	27.56	61.979	1708.14	-	-	-	27.72	167.18	**4634.22**
LIMA CCA	26.75	0.47	12.57	26.84	0.9	24.16	26.92	0.96	25.84	-	-	-	27.03	1.84	49.73
LIMA CPA	27.34	0.125	3.41	27.42	0.22	6.03	27.38	0.23	6.3	-	-	-	26.85	0.45	12.08
Lizard CCA	27.12	0.03	**0.81**	-	-	-	26.98	0.06	**1.51**	-	-	-	27.14	0.09	**2.44**
RLizard CCA	27.24	0.03	0.82	-	-	-	27.35	0.07	1.91	-	-	-	27.32	0.1	2.73
LOTUS Encrypt	26.43	0.13	3.43	-	-	-	26.37	0.24	6.32	-	-	-	26.61	0.41	10.91
McNIE 3Q	26.73	2.02	53.99	-	-	-	26.92	3.04	81.83	-	-	-	27.05	5.11	138.22
McNIE 4Q	27.32	1.05	28.68	-	-	-	27.35	2.04	55.79	-	-	-	27.29	5.04	137.54
NTRUEncrypt PKE	26.12	0.07	1.83	-	-	-	26.31	0.2	5.26	-	-	-	26.55	104.58	2776.59
Round2-u Encrypt	27.58	0.06	1.65	27.67	0.08	2.21	27.7	0.08	2.21	28.22	0.09	2.54	28.14	0.11	3.09
Round2-n Encrypt	26.89	8.1	217.8	26.92	11.96	321.96	27.02	12.67	342.34	27.56	19.95	549.82	27.45	19.1	524.3
Titanium CPA	27.13	0.09	2.44	-	-	-	27.31	0.1	2.73	-	-	-	26.98	0.15	4.05

Table 7: Energy consumption during **Keypair generation of Public Key Encapsulation schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
BIGQUAKE [35]	26.36	301	7934.36	-	-	-	26.48	2754	**72925.92**	-	-	-	26.44	5171	**136721.24**
BIKE [36]	25.88	0.24	6.21	-	-	-	26.08	5.81	151.52	-	-	-	25.97	0.64	16.62
CFPKM [37]	26.71	183	4887.93	-	-	-	26.53	490	12999.7	-	-	-	-	-	-
Classic McEliece [38]	-	-	-	-	-	-	-	-	-	-	-	-	27.59	936.11	25827.27
CRYSTALSKyber [39]	26.34	0.15	3.95	-	-	-	25.98	0.255	6.62	-	-	-	25.58	0.37	9.46
DAGS [40]	-	-	-	-	-	-	26.43	11.35	299.98	-	-	-	26.82	107.73	2889.31
DING [41]	27.17	1.42	38.58	-	-	-	-	-	-	-	-	-	26.98	2.77	74.73
DME [42]	-	-	-	-	-	-	25.72	25.79	663.31	-	-	-	25.82	95.51	2466.06
EMBLEM [43]	24.97	0.039	0.97	-	-	-	-	-	-	-	-	-	-	-	-
FRODO [44]	26.13	0.373	9.74	-	-	-	26.57	0.745	19.79	-	-	-	-	-	-
Hila5 [45]	-	-	-	-	-	-	-	-	-	-	-	-	27.05	1.29	34.89
HQC [46]	26.63	0.16	4.26	-	-	-	26.51	0.53	14.05	-	-	-	26.32	0.68	17.89
AKCN MLWE	-	-	-	-	-	-	-	-	-	26.71	0.1	2.67	-	-	-
OKCN MLWE	-	-	-	-	-	-	-	-	-	26.58	0.1	2.65	-	-	-
OKCN SEC	-	-	-	-	-	-	-	-	-		-	-	25.93	0.13	3.37
AKCN SEC	-	-	-	-	-	-	-	-	-		-	-	26.04	0.13	3.38
KINDI-KEM	-	-	-	-	-	-	27.13	0.07	1.89	-	-	-	27.04	0.16	4.32
LAKE [47]	26.73	0.61	16.3	-	-	-	26.19	0.7	18.33	-	-	-	26.81	0.65	17.42
LEDA KEM [48]	26.78	14.06	376.52	-	-	-	26.49	57.81	1531.38	-	-	-	26.79	176.042	4716.16
Lepton [49]	26.82	0.0084	**0.22**	-	-	-	26.92	0.0246	**0.64**	-	-	-	27.01	0.025	**0.67**
LIMA CCA	27.51	0.42	11.55	27.13	0.85	23.06	27.62	0.9	24.85	-	-	-	27.44	1.56	42.8
LIMA CPA	26.82	0.43	11.53	27.04	0.79	21.36	26.95	0.9	24.25	-	-	-	27.11	1.56	42.29
Lizard KEM	26.39	2.5	65.97	-	-	-	26.58	10.46	278.02	-	-	-	26.77	5.78	154.73
RLizard KEM	27.33	0.04	1.09	-	-	-	27.26	0.08	2.18	-	-	-	27.24	0.107	2.62
LOCKER [50]	27.14	2.96	80.33	-	-	-	26.92	3.35	90.18	-	-	-	27.05	3.6	97.38
LOTUS Kem	26.78	10.02	268.33	-	-	-	27.13	18.13	491.86	-	-	-	26.81	26.44	708.85
Mersenne-756839 [51]	-	-	-	-	-	-	-	-	-	-	-	-	26.81	6.02	161.39
NewHope CCA [52]	27.1	0.16	4.33	-	-	-	-	-	-	-	-	-	27.05	0.33	8.92
NewHope CPA	26.94	0.154	4.14	-	-	-	-	-	-	-	-	-	26.89	0.3	8.06
NTRUEncrypt KEM	26.71	0.33	8.81	-	-	-	26.77	0.83	21.41	-	-	-	28.68	39.79	1061.59
NTRU-HRSS-KEM [53]	27.11	53.74	1456.89	-	-	-	-	-	-	-	-	-	-	-	-
NTRU Prime [54]	-	-	-	-	-	-	-	-	-	-	-	-	27.03	3.03	81.9
NTS-KEM [55]	26.93	16.54	445.42	-	-	-	26.58	44.98	1195.56	-	-	-	26.94	87.92	2368.56
Old Manhattan [56]	26.88	72.1	1938.04	-	-	-	27.05	139.2	3765.36	-	-	-	27.12	238.2	6459.98
Quroboros-R [57]	26.11	0.1	2.61	-	-	-	26.38	0.11	2.63	-	-	-	26.17	0.14	3.66
Post-Quantum RSA KEM	-	-	-	26.53	1336.76	35464.24	-	-	-	-	-	-	-	-	-
QC-MDPC [58], [59]	-	-	-	-	-	-	26.67	87.03	2321.09	-	-	-	-	-	-
Ramstake [60]	27.18	2.35	63.87	-	-	-	26.94	10.88	293.1	-	-	-	-	-	-
RLCE-KEM [61]	26.85	390.06	**10473.11**	-	-	-	26.45	1554.88	41126.576	-	-	-	26.78	3853.39	103193.78
Round2-u KEM	26.41	0.14	3.69	26.11	0.14	3.65	26.32	0.65	17.10	26.57	0.5	13.28	26.39	0.29	7.65
Round2-n KEM	27.15	2.56	69.5	26.89	2.88	77.44	27.08	3.83	103.71	27.22	5.3	144.26	26.98	5.24	141.37
RQC [62]	27.06	0.27	7.3	-	-	-	26.82	0.45	12.06	-	-	-	27.14	0.76	20.62
SABER [63]	26.44	0.08	2.11	-	-	-	26.62	0.18	4.79	-	-	-	26.34	0.32	8.42
SIKE [64]	26.59	26.4	701.97	-	-	-	27.18	85.99	2337.2	-	-	-	-	-	-
Three Bears [65]	-	-	-	26.97	0.02	0.54	-	-	-	27.05	0.03	0.81	27.1	0.06	1.62
Titanium CCA	26.66	0.64	17.06	-	-	-	26.53	0.73	19.36	-	-	-	26.88	0.97	26.07

Table 8: Energy consumption during **Key Encapsulation of Public Key Encapsulation schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
BIGQUAKE	26.47	1.3	34.41	-	-	-	26.71	3.2	85.47	-	-	-	26.54	4.5	119.43
BIKE	25.88	0.229	5.95	-	-	-	26.11	0.23	6	-	-	-	26.08	1.1	28.68
CFPKM	26.41	188	**4965.08**	-	-	-	27.16	492	**13362.72**	-	-	-	-	-	-
Classic McEliece	-	-	-	-	-	-	-	-	-	-	-	-	27.16	0.34	9.23
CRYSTALSKyber	27.12	0.22	5.96	-	-	-	27.98	0.336	9.4	-	-	-	27.08	0.47	12.72
DAGS	-	-	-	-	-	-	26.66	0.0096	**0.256**	-	-	-	25.89	0.026	**0.673**
DING	26.98	2.01	54.22	-	-	-	-	-	-	-	-	-	27.12	4.01	108.75
DME	-	-	-	-	-	-	26.18	0.12	3.19	-	-	-	26.07	0.847	22.08
EMBLEM	25.52	0.928	23.47	-	-	-	-	-	-	-	-	-	-	-	-
FRODO	25.74	0.522	13.43	-	-	-	26.13	1.028	26.65	-	-	-	-	-	-
Hila5	-	-	-	-	-	-	-	-	-	-	-	-	26.69	1.23	32.82
HQC	25.73	0.4	10.29	-	-	-	26.18	0.94	24.6	-	-	-	26.42	1.3	34.34
AKCN MLWE	-	-	-	-	-	-	-	-	-	27.1	0.12	3.25	-	-	-
OKCN MLWE	-	-	-	-	-	-	-	-	-	26.49	0.13	3.44	-	-	-
OKCN SEC	-	-	-	-	-	-	-	-	-	-	-	-	26.53	0.21	5.57
AKCN SEC	-	-	-	-	-	-	-	-	-	-	-	-	26.79	0.23	6.16
KINDI-KEM	-	-	-	-	-	-	27.31	0.09	2.45	-	-	-	26.91	0.21	5.65
LAKE	25.92	0.11	2.85	-	-	-	26.31	0.11	2.89	-	-	-	26.44	0.12	3.17
LEDA KEM	25.84	2.083	53.82	-	-	-	26.21	13.542	354.93	-	-	-	26.1	35.417	924.38
Lepton	26.55	0.02	0.56	-	-	-	26.34	0.06	1.63	-	-	-	26.72	0.06	1.6
LIMA CCA	25.88	0.37	9.57	26.23	0.73	19.14	26.11	0.76	19.84	-	-	-	27.08	1.56	42.24
LIMA CPA	25.74	0.37	9.52	25.11	0.7	17.57	25.49	0.84	21.41	-	-	-	26.17	1.43	37.42
Lizard KEM	26.44	0.31	8.19	-	-	-	26.61	0.54	14.36	-	-	-	26.38	0.69	18.2
RLizard KEM	26.87	0.02	**0.53**	-	-	-	27.17	0.06	1.63	-	-	-	27.35	0.08	2.18
LOCKER	26.23	0.47	12.33	-	-	-	26.18	0.48	12.56	-	-	-	26.35	0.52	13.7
LOTUS Kem	26.72	0.08	2.13	-	-	-	26.63	0.11	2.92	-	-	-	27.91	0.19	5.3
Mersenne-756839	-	-	-	-	-	-	-	-	-	-	-	-	26.71	9.23	246.53
NewHope CCA	27.32	0.25	6.83	-	-	-	-	-	-	-	-	-	26.85	0.5	13.425
NewHope CPA	26.59	0.22	5.84	-	-	-	-	-	-	-	-	-	27.16	0.4	10.86
NTRUEncrypt KEM	28.13	0.06	1.68	-	-	-	27.11	0.12	3.25	-	-	-	26.52	61.83	1639.73
NTRU-HRSS-KEM	26.53	1.23	32.63	-	-	-	-	-	-	-	-	-	-	-	-
NTRU Prime	-	-	-	-	-	-	-	-	-	-	-	-	27.15	6.26	169.95
NTS-KEM	26.55	0.02	0.53	-	-	-	26.43	0.12	3.17	-	-	-	27.08	0.15	4.06
Old Manhattan	26.76	36.2	968.71	-	-	-	27.2	66.8	1816.96	-	-	-	27.23	147.34	**4012.06**
Quroboros-R	26.38	0.18	4.74	-	-	-	26.11	0.22	5.74	-	-	-	26.79	0.26	6.96
Post-Quantum RSA KEM	-	-	-	26.66	8.39	223.67	-	-	-	-	-	-	-	-	-
QC-MDPC	-	-	-	-	-	-	26.52	6.05	160.44	-	-	-	-	-	-
Ramstake	27.21	4.34	118.09	-	-	-	26.52	19.82	525.62	-	-	-	-	-	-
RLCE-KEM	26.21	1.78	46.65	-	-	-	26.38	4.02	106.04	-	-	-	26.78	11.74	314.39
Round2-u KEM	27.18	0.34	9.24	26.87	0.57	15.31	27.24	2.71	73.82	27.18	0.44	11.95	26.95	0.59	15.9
Round2-n KEM	28.1	5.38	151.17	27.33	6.09	166.43	27.21	7.68	208.97	26.82	10.68	286.43	27.06	10.98	297.11
RQC	26.78	0.58	15.53	-	-	-	27.13	1.46	39.6	-	-	-	26.86	1.72	46.19
SABER	26.67	0.22	5.86	-	-	-	26.68	0.34	9.07	-	-	-	27.11	0.53	14.36
SIKE	27.06	43.22	1169.53	-	-	-	26.63	140.98	3754.29	-	-	-	-	-	-
Three Bears	-	-	-	26.54	0.04	1.06	-	-	-	26.68	0.04	1.06	26.32	0.08	2.1
Titanium CCA	25.86	0.59	15.25	-	-	-	26.14	0.67	17.51	-	-	-	26.44	0.92	24.32

Table 9: Energy consumption during **Key Decapsulation of Public Key Encapsulation schemes** where time is in milliseconds, power in Watts and energy in milliJoules

Scheme	Security level I			Security level II			Security level III			Security level IV			Security level V		
	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy	Power	Time	Energy
BIGQUAKE	26.53	1.6	42.44	-	-	-	26.38	10.2	269.07	-	-	-	26.57	14.7	390.58
BIKE	25.62	0.99	25.36	-	-	-	26.47	2.48	65.64	-	-	-	26.18	6.13	160.48
CFPKM	26.73	176	**4704.48**	-	-	-	26.52	502	**13313.04**	-	-	-	-	-	-
Classic McEliece	-	-	-	-	-	-	-	-	-	-	-	-	27.24	82.78	2254.92
CRYSTALSKyber	25.92	0.266	6.89	-	-	-	26.08	0.404	10.53	-	-	-	25.28	0.555	14.03
DAGS	-	-	-	-	-	-	26.36	0.046	**1.21**	-	-	-	26.57	0.17	4.51
DING	26.56	1.33	35.32	-	-	-	-	-	-	-	-	-	26.73	2.59	69.23
DME	-	-	-	-	-	-	26.24	0.59	15.48	-	-	-	26.45	4.19	110.82
EMBLEM	25.77	0.96	2.73	-	-	-	-	-	-	-	-	-	-	-	-
FRODO	26.14	0.52	13.59	-	-	-	26.26	1.03	27.04	-	-	-	-	-	-
Hila5	-	-	-	-	-	-	-	-	-	-	-	-	26.58	0.02	**0.53**
HQC	26.17	0.92	24.07	-	-	-	26.78	1.7	45.52	-	-	-	26.34	2.56	67.43
AKCN MLWE	-	-	-	-	-	-	-	-	-	26.85	0.02	0.53	-	-	-
OKCN MLWE	-	-	-	-	-	-	-	-	-	27.27	0.02	0.54	-	-	-
OKCN SEC	-	-	-	-	-	-	-	-	-	-	-	-	26.67	0.05	1.33
AKCN SEC	-	-	-	-	-	-	-	-	-	-	-	-	28.05	0.04	1.4
KINDI-KEM	-	-	-	-	-	-	26.81	0.12	3.21	-	-	-	26.86	0.25	6.71
LAKE	25.84	0.48	12.4	-	-	-	26.17	0.8	20.93	-	-	-	26.38	1.07	28.22
LEDA KEM	26.58	28.12	747.42	-	-	-	26.73	55.20	1475.49	-	-	-	26.37	154.16	4065.19
Lepton	26.83	0.02	**0.53**	-	-	-	26.71	0.07	1.87	-	-	-	26.93	0.07	1.88
LIMA CCA	25.94	0.47	12.19	26.16	0.94	24.59	26.47	0.98	25.94	-	-	-	25.83	1.9	49.07
LIMA CPA	26.68	0.125	3.33	26.43	0.23	6.07	27.11	0.24	6.5	-	-	-	26.86	0.45	12.08
Lizard KEM	26.47	0.36	9.52	-	-	-	26.73	0.66	17.64	-	-	-	27.23	0.81	22.05
RLizard KEM	27.13	0.03	0.81	-	-	-	27.23	0.07	1.9	-	-	-	26.93	0.11	2.96
LOCKER	26.46	1.73	45.77	-	-	-	26.38	1.78	46.95	-	-	-	26.51	2.39	63.35
LOTUS Kem	26.47	0.12	3.17	-	-	-	26.72	0.23	6.14	-	-	-	26.88	0.43	11.55
Mersenne-756839	-	-	-	-	-	-	-	-	-	-	-	-	27.16	18.18	493.76
NewHope CCA	27.08	0.28	7.58	-	-	-	-	-	-	-	-	-	27.11	0.57	15.72
NewHope CPA	26.83	0.04	1.07	-	-	-	-	-	-	-	-	-	26.49	0.08	2.11
NTRUEncrypt KEM	27.87	0.08	2.22	-	-	-	27.43	0.17	4.66	-	-	-	27.71	109.1	3023.16
NTRU-HRSS-KEM	26.85	3.58	96.12	-	-	-	-	-	-	-	-	-	-	-	-
NTRU Prime	-	-	-	-	-	-	-	-	-	-	-	-	27.23	9.35	254.6
NTS-KEM	26.48	0.2	5.29	-	-	-	26.67	0.36	9.6	-	-	-	26.95	0.83	22.36
Old Manhattan	27.16	40.17	1091.01	-	-	-	27.32	79.8	2180.13	-	-	-	26.85	163.32	**4385.14**
Quroboros-R	26.56	0.41	10.88	-	-	-	26.47	0.78	20.64	-	-	-	26.81	1.12	30.02
Post-Quantum RSA KEM	-	-	-	26.75	46.99	1256.98	-	-	-	-	-	-	-	-	-
QC-MDPC	-	-	-	-	-	-	27.13	71.8	1947.93	-	-	-	-	-	-
Ramstake	27.02	8.92	241.01	-	-	-	27.31	38.46	1050.34	-	-	-	-	-	-
RLCE-KEM	26.86	3.48	93.47	-	-	-	26.53	8.29	219.93	-	-	-	26.57	26.51	704.37
Round2-u KEM	27.04	0.13	3.51	27.12	0.35	9.49	26.96	1.93	52.03	27.15	0.34	9.23	27.26	0.28	7.63
Round2-n KEM	27.86	2.62	72.99	28.12	3.66	102.91	27.94	4.03	112.6	28.14	5.84	164.34	28.23	5.71	161.2
RQC	26.73	1.54	41.16	-	-	-	26.37	3.95	104.16	-	-	-	27.08	4.88	132.15
SABER	27.17	0.27	7.33	-	-	-	26.84	0.52	13.95	-	-	-	27.18	0.71	19.29
SIKE	26.86	46.11	1238.51	-	-	-	27.24	151.85	4136.4	-	-	-	-	-	-
Three Bears	-	-	-	26.76	0.05	1.34	-	-	-	26.92	0.06	1.61	26.58	1.06	28.17
Titanium CCA	26.13	0.68	17.76	-	-	-	26.57	0.77	20.45	-	-	-	25.93	1.07	27.74

Table 10: The energy efficient lattice based cryptographic algorithm submissions

Signing			Encapsulation/Encryption		
Key Generation	Sign	Verify	Key Generation	Enc	Dec
CRYSTALSDilithium	CRYSTALSDilithium	CRYSTALSDilithium	EMBLEM, KCL,	Lizard, Lepton,	Lepton, KCL
-	-	-	Lizard, Lepton,	LAC, KINDI,	New Hope CPA,
-	-	-	Round 2, LAC	LOTUS	Lizard, Round 2-u

This report provides the energy efficiency for all those variants as well. In a particular security level, amongst all the algorithms submitted in the categories of signing, encryption or encapsulation etc, the most energy efficient and the least ones are in bold characters. There are few submissions in both signature schemes and encryption/encapuslation techniques, who have provided implementation for the security levels of II and IV. Therefore, we did not mark the most energy efficient or the least ones in those categories. It should also be noted that there are instances when multiple algorithms require almost similar execution time. This leads to energy consumption values which are quite close, depending also upon their power usage values. In that case we have provided top 5 efficient algorithms in Tables 11, 10 and 12 with comparable energy consumption values.

3.2 Public Key Encryption/Encapsulation

14 submissions focus on implementing public key encryption schemes with quantum safe algorithms. Tables 4, 5 and 6 provide the values of power usage, execution time and energy consumption of these implemented schemes. As mentioned in the previous subsection, the most/least energy efficient in a particular group has been indicated with bold characters.

Around 39 schemes implemented public key encapsulation in this PQC standardization process. Tables

Table 11: The energy efficient code based cryptographic algorithm submissions

Encapsulation/Encryption schemes		
Key Generation	Enc	Dec
OuroborosR, HQC, BIKE, RQC, LAKE	NTS-KEM, LAKE, OuroborosR, BIKE, Classic McEliece, DAGS	OuroborosR, LAKE, Hila5, DAGS, NTS-KEM

Table 12: The energy efficient multivariate based cryptographic algorithm submissions

Signature schemes		
Key Generation	Sign	Verify
HiMQ3, HiMQ3F	Rainbow, HiMQ3, HiMQ3F	Gui, GeMSS, HiMQ3, HiMQ3F

7, 8 and 9 provide the values of energy consumption corresponding for these schemes. Some of the candidate algorithms provide both encapsulation and encryption techniques. So the same submission name has been reported for the different tables with the tags of -ENCRYPT or -KEM accordingly.

3.3 Other observations

In the previous subsections we have seen categorization of the submitted algorithms based on their energy efficiency for a particular security level. Furthermore, broadly all these algorithms come under the categories of well known post quantum crypto techniques such as lattice based, code based, multivariate, hash based etc. A small number of submissions also correspond to some different technique other than the aforementioned ones such as GiophantusR which deals with the underlying problem of solving indeterminate equations. In addition to that, the submissions such as Guess Again, Mersenne-756839, Picnic, Postquantum RSA, Walnut etc are based on some novel problem which has not been explored before in any post-quantum cryptoschemes. Therefore, based on these underlying problem, Tables 10, 11 and 12 again categorises the submitted algorithms and mentions the top 5 in each group which seems to be energy efficient. It should be noted that these tables report the efficient algorithms considering all the 5 security levels. In case of code based cryptography there are only 2 signature schemes pqsigRM and RaCoSS, both of which require significant amount of energy for their algorithm execution. Hence, they are not reported in Table 11. Also, for multivariate based cryptosystems, there are only two encapsulation scheme submissions that is CFPKM and DME, again with the same issue of high energy consumption and as a result ommission from Table 12. In the category of hash-based cryptoschemes, there are two submissions namely Gravity - SPHINCS and SPHINCS Plus, both consuming quite an amount of energy. And SIKE is the only submission for Supersingular elliptic curve isogeny cryptography (SIDH).

4 Remarks

There have been reports published, analyzing the technicalities of these submissions such as Martin et al. [67] investigated the lattice based cryptoschemes' asymptotic runtime. However, except for [68] where we compare energy efficiency of the classical elliptic curve Diffie-Hellman (ECDH) relative to SIDH/SIKE, there has not been any evaluation of energy consumption of the NIST Round 1 post-quantum candidate algorithms yet. In certain applications, energy constrained devices will perform signing and decryption operations while the more powerful servers will verify and encrypt. From Table 2, one can compute the median energy consumption for Level I signing algorithms to be 266.53 milli Joules and the corresponding algorithm is RaCoSS. A practical experiment was performed to find out the number of signing operations for this particular submission RaCoSS, that can be performed on the same processor (as mentioned in Section 2 with a battery capacity of 60 Watt hours or 216 KJoules) till its battery gets exhausted. The experimental results showed around 800,000 signing operations, which is consistent with the Intel Power Gadget based results reported in the table.

As seen the previous section, the variations in power usages by the post-quantum cryptographic considered here are relatively small. An algorithm's energy consumption is the product of its average power usage and the execution time. We do not expect the power usages to vary considerably if an algorithm undergoes further optimization. As a result, algorithm optimization based reduction in execution time is likely to yield roughly a proportionate reduction in energy consumption, assuming the same C based implementation.

Vectorized and/or floating point instruction based implementations add another degree of freedom to the effort of reducing execution time and energy consumption. Vectorized and floating point instructions use some part of the processor that are not used by regular integer instructions. It remains to be investigated the impact of vectorized and floating point instructions on the energy consumptions of the post-quantum candidates.

Acknowledgements

This research was supported in part through an NSERC grant awarded to Dr. Hasan. The authors would like to thank Dr. David Jao for his initial discussion with Dr. Hasan and also his comments on an earlier version of this manuscript.

References

[1] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[2] "NIST Round 1 Submissions." National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[3] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: a lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018.

[4] T. Plantard, A. Sipasseuth, C. Dumondelle, and W. Susilo, "Diagonal dominant reduction for lattice-based signature." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[5] J.-C. Faugère, L. Perret, and J. Ryckeghem, *DualModeMS: A Dual Mode for Multivariate-based Signature 20170918 draft*. PhD thesis, UPMC-Paris 6 Sorbonne Universités; INRIA Paris; CNRS, 2017.

[6] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "Falcon: fast-fourier, lattice-based, compact signatures over ntru," *Submission to NIST Post-Quantum Competition*, vol. 17, 2017.

[7] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, *GeMSS: A Great Multivariate Short Signature*. PhD thesis, UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France; LIP6-Laboratoire d'Informatique de Paris 6, 2017.

[8] G. E. Jean-Philippe Aumasson, "Gravity-sphincs." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[9] A. Petzoldt, M.-S. Chen, J. Ding, and B.-Y. Yang, "HMFEv-an efficient multivariate signature scheme," in *International workshop on post-quantum cryptography*, pp. 205–223, Springer, 2017.

[10] K.-A. Shim, C.-M. Park, and N. Koo, "An existential unforgeable signature scheme based on multivariate quadratic equations," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 37–64, Springer, 2017.

[11] W. Beullens, B. Preneel, A. Szepieniec, and F. Vercauteren, "LUOV." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[12] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe, "From 5-pass MQ - based identification to MQ - based signatures," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 135–165, Springer, 2016.

[13] M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha, "Post-quantum zero-knowledge and signatures from symmetric-key primitives," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1825–1842, ACM, 2017.

[14] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-quantum RSA," in *International Workshop on Post-Quantum Cryptography*, pp. 311–329, Springer, 2017.

[15] W. Lee, Y.-S. Kim, and J.-S. No, “A new signature scheme based on punctured Reed–Muller code with random insertion,” *arXiv preprint arXiv:1711.00159*, 2017.

[16] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega, “Revisiting TESLA in the quantum random oracle model,” in *International Workshop on Post-Quantum Cryptography*, pp. 143–162, Springer, 2017.

[17] K. Morozov, P. S. Roy, and K. Sakurai, “On unconditionally binding code-based commitment schemes,” in *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, p. 101, ACM, 2017.

[18] J. Ding and A. Petzoldt, “Current state of multivariate cryptography,” *IEEE Security & Privacy*, vol. 15, no. 4, pp. 28–36, 2017.

[19] D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, *et al.*, “Sphincs,” 2017.

[20] D. Goldfeld, “Walnut digital signature algorithm,”

[21] D. Liu, N. Li, J. Kim, and S. Nepal, “Compact-LWE: Enabling practically lightweight public key encryption for leveled IoT device authentication,” tech. rep., Cryptology ePrint Archive, Report 2017/685, 2017. http://eprint. iacr. org/2017/685.

[22] K. Akiyama, Y. Goto, S. Okumura, T. Takagi, K. Nuida, G. Hanaoka, H. Shimizu, and Y. Ikematsu, “A public-key encryption scheme based on non-linear indeterminate equations (Giophantus),”

[23] V. Shpilrain, M. Bessonov, A. Gribov, and D. Grigoriev, “Guess Again.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[24] Y. Zhao, Z. Jin, B. Gong, and G. Sui, “OKCN/AKCN/CNKE: A modular and systematic approach to key establishment and public-key encryption based on LWE and its variants.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[25] R. E. Bansarkhani, “KINDI.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[26] X. Lu1, Y. Liu, D. Jia, H. Xue, J. He, and Z. Zhang, “LAC.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[27] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, “LEDA.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[28] E. O. Martin R. Albrecht, Yehuda Lindell, V. Osheter, K. G. Paterson, G. Peer, and N. P. Smart, “LIMA : A PQC encryption scheme.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[29] J. H. Cheon, D. Kim, J. Lee, and Y. Song, “Lizard public key encryption.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[30] L. T. Phong, T. Hayashi, Y. Aono, and S. Moriai, “LOTUS.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[31] L. Galvez, J.-L. Kim, M. J. Kim, Y.-S. Kim, and N. Lee, “McNie: Compact McEliece-Niederreiter Cryptosystem.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[32] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, “NTRUEncrypt : A lattice based encryption algorithm.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[33] H. Baan, S. Bhattacharya, Garcia-Morchon, R. Rietman, L. Toihuizen, J. Torre-Arce, and Z. Zhamig, “Round2: KEM and PKE based on GLWR.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[34] R. Steinfeld, A. Sakzad, and R. K. Zhao, "Titanium: Proposal for a nist post-quantum public-key encryption and kem standard," 2017.

[35] M. Bardet, E. Barelli, O. Blazy, R. Canto, A. Couvreur, P. Gaborit, A. Otmani, N. Sendrier, and J.-P. Tillich, "BIG QUAKE." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[36] N. Aragon, P. S. L. M. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. GÃijneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, and I. Gilles ZÃľmor, "BIKE." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[37] O. Chakraborty, J.-C. Faugère, and L. Perret, *CFPKM: A Key Encapsulation Mechanism based on Solving System of non-linear multivariate Polynomials 20171129*. PhD thesis, UPMC-Paris 6 Sorbonne Universités; INRIA Paris; CNRS, 2017.

[38] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang, "Classic McEliece." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[39] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé, "Crystals–Kyber: a CCA-secure module-lattice-based KEM," *IACR Cryptology ePrint Archive*, vol. 2017, p. 634, 2017.

[40] G. Banegas, P. S. L. M. Barreto, B. O. Boidje, P.-L. Cayrel, G. N. Dione, K. Gaj, C. T. Gueye, R. Haeussler, J. B. Klamti, O. NâĂŹdiaye, D. T. Nguyen, E. Persichetti, and J. E. Ricardini, "DAGS." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[41] J. Ding, T. Takagi, Y. Wang, and X. Gao, "DING." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[42] I. Luengo, "DME : A public key, signature and kem system based on double exponentiation with matrix exponents," *preprint*, 2017.

[43] M. Seo, J. H. Park, D. H. Lee, S. Kim, and S.-J. Lee, "Emblem : Error-blocked multi-bit LWE based KEM." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[44] M. Naehrig, E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila, "FrodoKEM : Learning with errors key encapsulation." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[45] M.-J. O. Saarinen, "HILA5: On reliability, reconciliation, and error correction for ring-lwe encryption," in *International Conference on Selected Areas in Cryptography*, pp. 192–212, Springer, 2017.

[46] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and I.-C. Bourges, "Hamming quasi-cyclic (HQC),"

[47] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor, "LAKE–low rank parity check codes key exchange at first round submission to the nist post-quantum cryptography call," 2017.

[48] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "LEDAkem: a post-quantum key encapsulation mechanism based on qc-ldpc codes," in *International Conference on Post-Quantum Cryptography*, pp. 3–24, Springer, 2018.

[49] Y. Yu and J. Zhang, "Lepton : Key Encapsulation mechanisms from a variant of learning parity with noise." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[50] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor, "LOCKER." Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[51] D. Aggarwal, A. Joux, A. Prakash, and M. Santha, “A new public-key cryptosystem via mersenne numbers,” tech. rep., Cryptology ePrint Archive, Report 2017/481, 2017. http://eprint. iacr. org/2017/481, 2017.

[52] E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, T. PÃűppelmann, P. Schwabe, and D. Stebila, “NewHope.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[53] A. Hulsing, J. Rijneveld, J. M. Schanck, and P. Schwabe, “NTRU-HRSS-KEM.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[54] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, “NTRU Prime.,” *IACR Cryptology ePrint Archive*, vol. 2016, p. 461, 2016.

[55] M. Albrecht, C. Cid, K. G. Paterson, C. J. Tjhai, and M. Tomlinson, “NTS-KEM.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[56] T. PLANTARD, “Odd Manhattan.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[57] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, G. Zémor, and I.-C. Bourges, “Ouroboros-R,” 2017.

[58] A. Yamada, “Key encapsulation mechanisms,” Mar. 6 2018. US Patent 9,912,479.

[59] A. Yamada, E. Eaton, K. Kalach, P. Lafrance, and A. Parent, “QC-MDPC.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[60] A. Szepieniec, “Ramstake.” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[61] W. Yongge, “Quantum resistant random linear code based public key encryption scheme RLCE,” in *Information Theory (ISIT), 2016 IEEE International Symposium on*, pp. 2519–2523, IEEE, 2016.

[62] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Zémor, “Rank quasi cyclic (RQC).” Technical report, National Institute of Standards and Technology, 2017 available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

[63] J.-P. D’Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, “Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure kem,” in *International Conference on Cryptology in Africa*, pp. 282–305, Springer, 2018.

[64] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, *et al.*, “Supersingular Isogeny Key Encapsulation,” 2017.

[65] M. Hamburg, “Module-LWE key exchange and encryption: The three bears,”

[66] D. J. Bernstein, “SUPERCOP: System for unified performance evaluation related to cryptographic operations and primitives,” 2009.

[67] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer, “Estimate all the LWE, NTRU schemes!.” Available at `https://github.com/estimate-all-the-lwe-ntru-schemes`, 2017.

[68] T. Banerjee and M. A. Hasan, “Energy Efficiency Analysis of Elliptic Curve based Cryptosystems,” in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2018 IEEE 17th International Conference*, IEEE, (to appear)2018.