Energy Consumption of Round 2 Submissions for NIST PQC Standards

Crystal Roma
Electrical and Computer Engineering
University of Waterloo
Waterloo
caroma@uwaterloo.ca

Chi-En Amy Tai
Management Sciences
University of Waterloo
Waterloo
catai@edu.uwaterloo.ca

M. Anwar Hasan
Electrical and Computer Engineering
University of Waterloo
Waterloo
ahasan@uwaterloo.ca

UNIVERSITY OF WATERLOO

Motivation

- Round 2 candidates for NIST Post-Quantum Cryptography (PQC) standardization process includes 17 Key Encapsulation Mechanisms (KEM) and 9 Digital Signature schemes for consideration

- Submissions to be evaluated based on correctness, speed, and storage requirements

- Due to increased use of battery-operated devices and growing interest in green-computing, energy consumed by candidate submissions is also important to consider

Motivation

Our study aims to answer the following questions:

1. Which PQC Round 2 submissions are the most energy efficient?

2. Is there a trend between the underlying mathematics on which the scheme is based and the energy consumption profile?

3. Which subroutines contribute most to the energy consumption of a given scheme?

4. Based on the energy consumption, are certain schemes preferred in different applications?

Motivation

Goal

To profile all Round 2 PQC submissions for energy consumption, categorized by proposed security level, from which we can rank the candidates and determine which schemes are most energy efficient

Outline

1. Goal and Motivation
2. Categorization of NIST PQC Round 2 Candidates
3. Methodology
4. Energy Profile of Optimized C Implementations
5. Energy Profile of Assembly Optimized Implementations
6. Ranking of Optimized C Implementations vs. Ranking of Assembly Optimized Implementations
7. Summary and Future Work

Categorization of KEM/PKE Submissions

Scheme	Lattice	Code	Isogeny	Rank
BIKE		✓		
Classic McEliece		✓		
CRYSTALS-Kyber	✓			
FrodoKEM	✓			
HQC		✓		
LAC	✓			
LEDAcrypt		✓		
NewHope	✓			
NTRU	✓			
NTRU Prime	✓			
NTS-KEM		✓		
ROLLO				✓
Round5	✓			
RQC				✓
SABER	✓			
SIKE			✓	
Three Bears	✓			

Table 1: Categorization of **Key Encapsulation / Public-Key Encryption** schemes based on the mathematics of the cryptosystem

Categorization of Digital Signature Submissions

Scheme	Lattice	Multivariate	Other
CRYSTALS-Dilithium	✓		
Falcon	✓		
GeMSS		✓	
LUOV		✓	
MQDSS		✓	
Picnic			✓
qTESLA	✓		
Rainbow		✓	
SPHINCS+			✓

Table 2: Categorization of **Digital Signature** schemes based on the mathematics of the cryptosystem

Additional Implementations of KEM/PKE Submissions

- According to NIST's guidelines, any of these three cryptographic mechanisms must be demonstrated by an implementation written in portable ANSI C

- Some have added extra implementations to better showcase their proposal's performance, like providing implementations using vectorized assembly instructions and versions which use hardware-accelerated symmetric primitives

- Based on this categorization, we decide which implementations to profile

Additional Implementations of KEM/PKE Submissions

Scheme	x86 Assembly Optimization			Other Hardware		
	SIMD	AES-NI	Other	ARM	FPGA	ASIC
BIKE	✓	✓	✓		✓	
Classic McEliece	✓					
CRYSTALS-Kyber	✓	✓				
FrodoKEM	✓	✓		✓		
HQC	✓					
LAC	✓					
LEDAcrypt	✓					
NewHope	✓					
NTRU	✓					
NTRU Prime						
NTS-KEM	✓		✓			
ROLLO						
Round5	✓					
RQC						
SABER	✓	✓				
SIKE			✓	✓	✓	✓
Three Bears			✓			

Table 3: Additional implementations submitted in Round 2 packages of **Key Encapsulation / Public-Key Encryption** schemes

Additional Implementations of Digital Signature Submissions

Scheme	x86 Assembly Optimization			Other Hardware		
	SIMD	AES-NI	Other	ARM	FPGA	ASIC
CRYSTALS-Dilithium	✓	✓				
Falcon						
GeMSS	✓		✓			
LUOV	✓					
MQDSS	✓					
Picnic	✓			✓		
qTESLA	✓					
Rainbow	✓					
SPHINCS+	✓	✓				

Table 4: Additional implementations submitted in Round 2 packages of **Digital Signature** schemes

Methodology

- Based on the previous tables, it can be seen that many submissions have included an assembly optimized implementation in their Round 2 package, but not all

- To make a fair comparison, we first profile the basic C implementations which all submissions have included. This will be referred to as the *Optimized C Implementation*

Methodology

- Based on the previous tables, it can be seen that many submissions have included an assembly optimized implementation in their Round 2 package, but not all

- To make a fair comparison, we first profile the basic C implementations which all submissions have included. This will be referred to as the *Optimized C Implementation*

- The profiling process is then repeated on those submissions which have included an assembly optimized implementation. This will be referred to as the *Assembly Optimized Implementation*

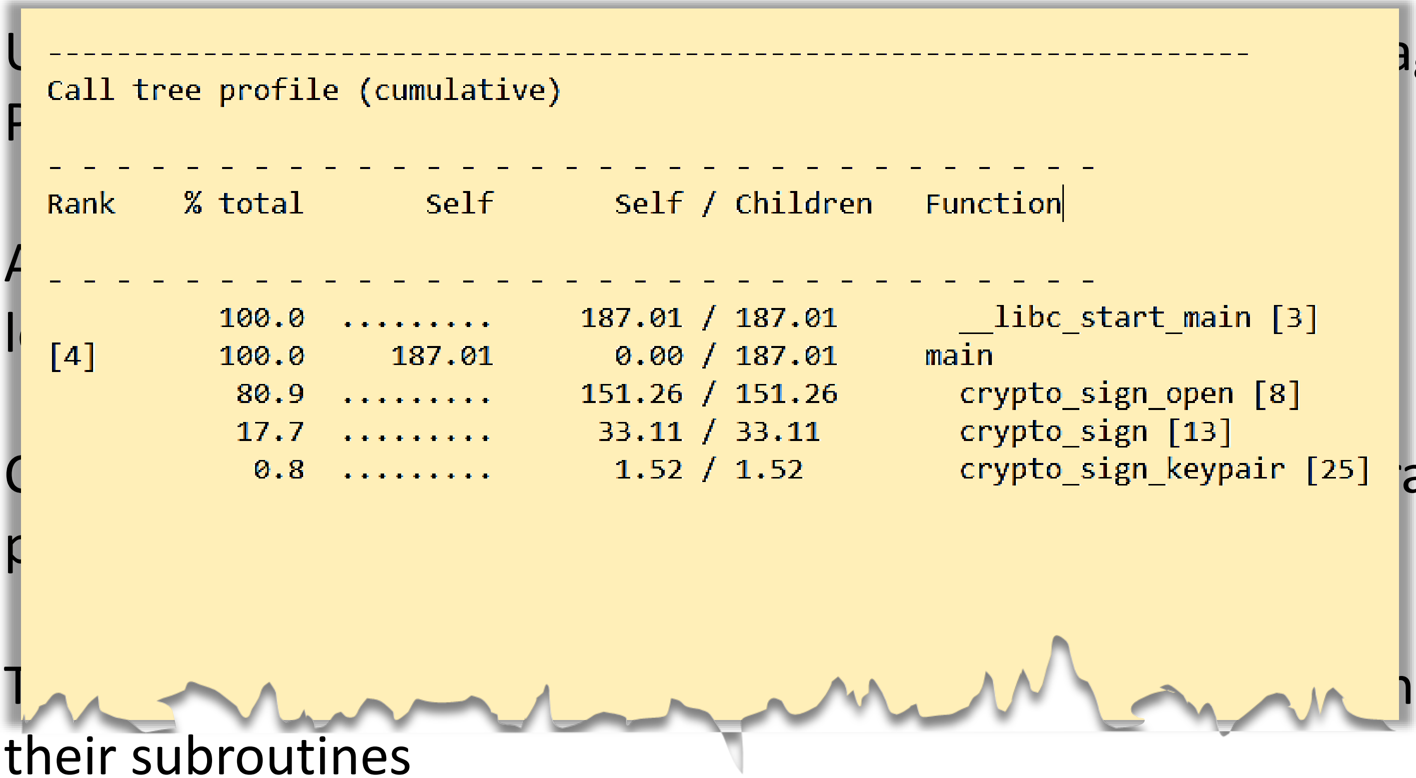
- Profiles are subdivided by their proposed security level and cryptographic functionality. Results are separated by the triple of subroutines as specified by NIST's API specifications

Methodology

- IgProf lightweight profiler used to capture energy measurements which operates on the principal of statistical sampling
- Uses PAPI to obtain measurements from the Running Average Power Limit at a fixed interval
- Attributes the current energy measurement to the present location of execution of the code being profiled
- Creates a flat cumulative profile, flat self profile, and call graph profile
- This can help pinpoint most energy consuming functions and their subroutines

Methodology

- IgProf lightweight profiler used to capture energy measurements
- Operates on the principal of statistical sampling
- U age
  P
- A
  l
- C aph
  p
- T nd
  their subroutines



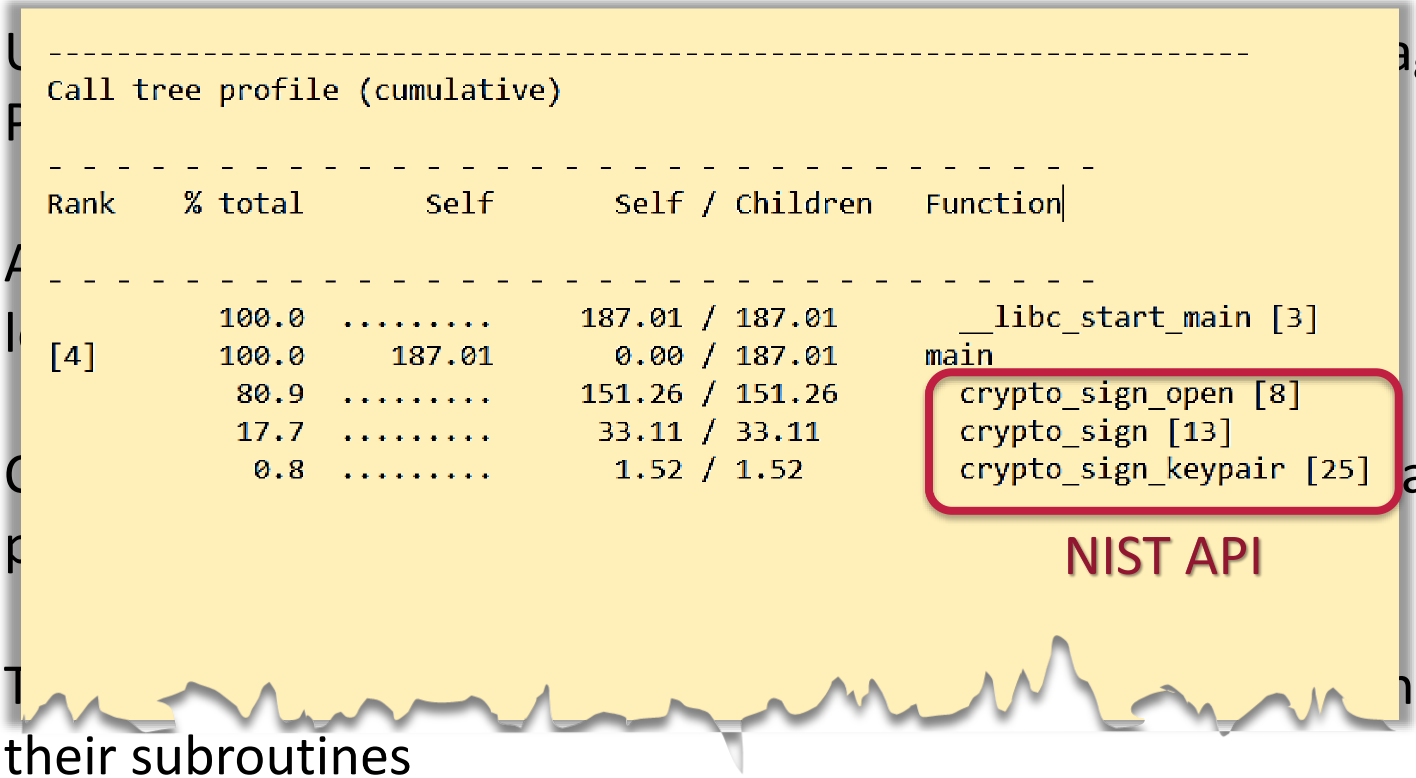
```
----------------------------------------------------------------------
Call tree profile (cumulative)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Rank    % total       Self       Self / Children   Function

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
          100.0  .........     187.01 / 187.01       __libc_start_main [3]
[4]       100.0     187.01       0.00 / 187.01     main
           80.9  .........     151.26 / 151.26       crypto_sign_open [8]
           17.7  .........      33.11 / 33.11        crypto_sign [13]
            0.8  .........       1.52 / 1.52         crypto_sign_keypair [25]
```

Methodology

- IgProf lightweight profiler used to capture energy measurements
- Operates on the principal of statistical sampling
- U age F
- A l
- C aph p
- T nd their subroutines



```
-----------------------------------------------------------------------
Call tree profile (cumulative)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 
Rank     % total        Self        Self / Children    Function

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 
          100.0  .........      187.01 / 187.01        __libc_start_main [3]
[4]       100.0     187.01        0.00 / 187.01      main
           80.9  .........      151.26 / 151.26        crypto_sign_open [8]
           17.7  .........       33.11 / 33.11         crypto_sign [13]
            0.8  .........        1.52 / 1.52          crypto_sign_keypair [25]
```

NIST API

Methodology

- Optimized C implementations were built on a 64-bit processor Intel Xeon E3-1270 CPU @ 3.40GHz with 8GB of RAM running Ubuntu 16.04 LTS

- Assembly optimized implementations were built on a 64-bit processor Intel Core i7-6700 CPU @ 3.40GHz with 8GB of RAM running Ubuntu 16.04 LTS

Methodology

- Optimized C implementations were built on a 64-bit processor Intel Xeon E3-1270 CPU @ 3.40GHz with 8GB of RAM running Ubuntu 16.04 LTS

- Assembly optimized implementations were built on a 64-bit processor Intel Core i7-6700 CPU @ 3.40GHz with 8GB of RAM running Ubuntu 16.04 LTS

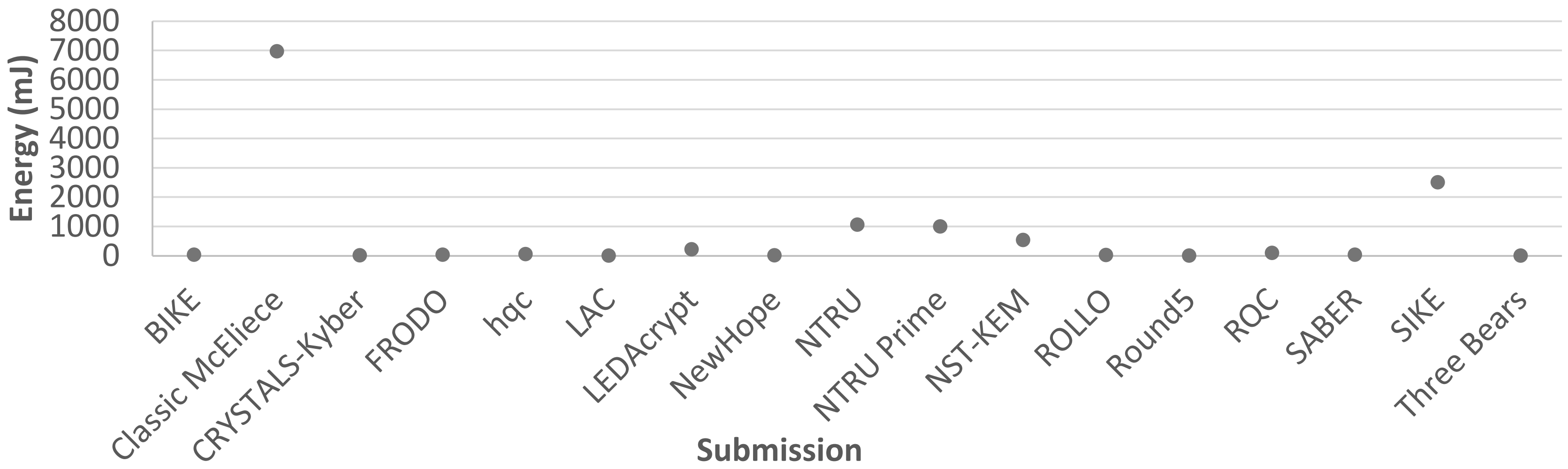
- For operations requiring a message, 100 random messages were created of fixed length, where the length was chosen to be approximately the same as the maximum tested in NIST'S provided KAT scripts
  - 32 byte messages for PKE schemes
  - 3300 byte messages for Digital Signature schemes

- Minimum of 100 iterations

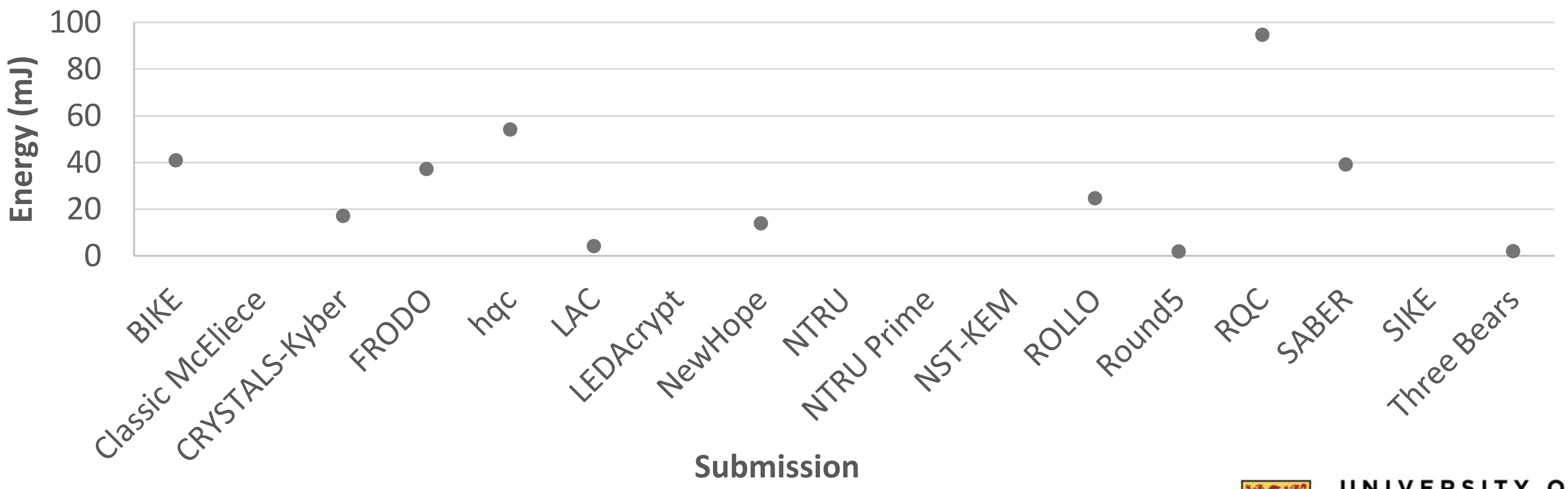
Results for Optimized C Implementation

Key Encapsulation Mechanisms

Total Energy Consumed by KEM Targeting Level 1



Total Energy Consumed by KEM Targeting Level 1 (below 100 mJ)



Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	5.63	-	17.62	-	39.37
BIKE-1 CPA	5.02	-	13.62	-	24.25
BIKE-2 CCA	11.85	-	38.29	-	85.95
BIKE-2 CPA	10.51	-	28.85	-	49.29
BIKE-3 CCA	3.29	-	10.67	-	22.66
BIKE-3 CPA	3.15	-	8.05	-	18.28
Classic McEliece	6384.90	-	11632.40	-	38234.60
CRYSTALS-Kyber	4.15	-	7.20	-	11.29
CRYSTALS-Kyber-90s	6.86	-	12.58	-	21.03
FRODO AES	10.27	-	30.20	-	28.07
FRODO SHAKE	9.36	-	29.22	-	28.51
hqc-1	8.76	-	23.41	-	35.62
hqc-2	-	-	25.68	-	43.83
hqc-3	-	-	-	-	49.80
LAC	0.88	-	2.63	-	2.80
LEDAcrypt N02	407.20	-	860.30	-	1799.00
LEDAcrypt N03	103.00	-	387.80	-	1024.80
LEDAcrypt N04	102.40	-	333.30	-	771.00
LEDAcrypt LT DFR64	9359.50	-	30104.60	-	96421.70
LEDAcrypt LT DFRSL	15088.90	-	55077.80	-	155391.90
NewHope CCA	5.42	-	-	-	10.76
NewHope CPA	4.99	-	-	-	9.94
NTRU-HPS	989.52	-	1784.32	-	2673.23
NTRU-HRSS	-	-	1922.05	-	-
sNTRU Prime	-	1600.31	2102.77	2628.83	-
NTRU LPrime	-	182.74	242.94	313.77	-
NTS-KEM	535.30	-	1863.40	-	2886.20
ROLLO-I	16.37	-	26.18	-	31.83
ROLLO-II	116.18	-	127.65	-	126.03
ROLLO-III	3.45	-	4.82	-	6.75
Round5 Ring	0.57	-	1.87	-	2.36
Round5 Ring 5	0.67	-	1.26	-	2.29
Round5 Ring Long Key	0.73	-	-	-	-
Round5 Non-Ring	52.83	-	133.90	-	236.69
RQC	6.30	-	10.51	-	16.83
SABER	1.13	-	2.40	-	3.95
SIKE	573.80	884.70	1682.90	-	2859.90
SIKE Compressed	1461.90	2102.40	4034.50	-	6750.80
Three Bears	-	0.73	-	1.41	2.35
Three Bears Eph.	-	0.74	-	1.45	2.55

Table 5: Energy consumption of `crypto_kem_keypair` function for **Keypair Generation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	5.63	-	17.62	-	39.37
BIKE-1 CPA	5.02	-	13.62	-	24.25
BIKE-2 CCA	11.85	-	38.29	-	85.95
BIKE-2 CPA	10.51	-	28.85	-	49.29
BIKE-3 CCA	3.29	-	10.67	-	22.66
BIKE-3 CPA	3.15	-	8.05	-	18.28
Classic McEliece	6384.90	-	11632.40	-	38234.60
CRYSTALS-Kyber	4.15	-	7.20	-	11.29
CRYSTALS-Kyber-90s	6.86	-	12.58	-	21.03
FRODO AES	10.27	-	30.20	-	28.07
FRODO SHAKE	9.36	-	29.22	-	28.51
hqc-1	8.76	-	23.41	-	35.62
hqc-2	-	-	25.68	-	43.83
hqc-3	-	-	-	-	49.80
LAC	0.88	-	2.63	-	2.80
LEDAcrypt N02	407.20	-	860.30	-	1799.00
LEDAcrypt N03	103.00	-	387.80	-	1024.80
LEDAcrypt N04	102.40	-	333.30	-	771.00
LEDAcrypt LT DFR64	9359.50	-	30104.60	-	96421.70
LEDAcrypt LT DFRSL	15088.90	-	55077.80	-	155391.90
NewHope CCA	5.42	-	-	-	10.76
NewHope CPA	4.99	-	-	-	9.94
NTRU-HPS	989.52	-	1784.32	-	2673.23
NTRU-HRSS	-	-	1922.05	-	-
sNTRU Prime	-	1600.31	2102.77	2628.83	-
NTRU LPrime	-	182.74	242.94	313.77	-
NTS-KEM	535.30	-	1863.40	-	2886.20
ROLLO-I	16.37	-	26.18	-	31.83
ROLLO-II	116.18	-	127.65	-	126.03
ROLLO-III	3.45	-	4.82	-	6.75
Round5 Ring	0.57	-	1.87	-	2.36
Round5 Ring 5	0.67	-	1.26	-	2.29
Round5 Ring Long Key	0.73	-	-	-	-
Round5 Non-Ring	52.83	-	133.90	-	236.69
RQC	6.30	-	10.51	-	16.83
SABER	1.13	-	2.40	-	3.95
SIKE	573.80	884.70	1682.90	-	2859.90
SIKE Compressed	1461.90	2102.40	4034.50	-	6750.80
Three Bears	-	0.73	-	1.41	2.35
Three Bears Eph.	-	0.74	-	1.45	2.55

Table 5: Energy consumption of `crypto_kem_keypair` function for **Keypair Generation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Keypair Generation

- Best Lattice-Based: **Round5 Ring**
  - L1: 0.57mJ
  - L3: 1.26mJ
  - L5: 2.28mJ

- Best Code-Based: **BIKE3 CPA**
  - L1: 3.12mJ
  - L3: 8.05mJ
  - L5: 18.28mJ

- Best Other: **ROLLO-III**
  - L1: 3.45mJ
  - L3: 4.82mJ
  - L5: 6.75mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	6.83	-	20.21	-	48.65
BIKE-1 CPA	5.94	-	15.20	-	26.53
BIKE-2 CCA	2.70	-	8.75	-	21.54
BIKE-2 CPA	2.36	-	5.86	-	11.06
BIKE-3 CCA	5.55	-	18.82	-	45.70
BIKE-3 CPA	4.85	-	13.74	-	34.70
Classic McEliece	1.84	-	3.09	-	4.81
CRYSTALS-Kyber	6.00	-	9.13	-	14.62
CRYSTALS-Kyber-90s	7.62	-	13.94	-	21.10
FRODO AES	14.71	-	32.20	-	47.96
FRODO SHAKE	13.97	-	30.88	-	48.53
hqc-1	18.42	-	42.92	-	65.85
hqc-2	-	-	41.81	-	76.53
hqc-3	-	-	-	-	87.53
LAC	1.28	-	3.53	-	4.58
LEDAcrypt N02	20.14	-	47.00	-	81.90
LEDAcrypt N03	15.90	-	38.10	-	88.00
LEDAcrypt N04	20.87	-	49.70	-	101.90
LEDAcrypt LT DFR64	70.50	-	137.40	-	234.00
LEDAcrypt LT DFRSL	115.50	-	291.00	-	526.30
NewHope CCA	8.19	-	-	-	16.57
NewHope CPA	7.47	-	-	-	12.56
NTRU-HPS	22.21	-	36.35	-	48.03
NTRU-HRSS	-	-	33.59	-	-
sNTRU Prime	-	177.50	236.95	300.36	-
NTRU LPrime	-	330.60	450.95	586.52	-
NTS-KEM	0.92	-	3.55	-	4.66
ROLLO-I	3.63	-	5.21	-	6.62
ROLLO-II	18.71	-	25.06	-	22.81
ROLLO-III	8.60	-	10.24	-	16.02
Round5 Ring	0.93	-	3.09	-	3.88
Round5 Ring 5	1.14	-	1.86	-	3.38
Round5 Ring Long Key	1.18	-	-	-	-
Round5 Non-Ring	47.47	-	118.22	-	222.17
RQC	12.86	-	23.67	-	36.61
SABER	19.04	-	29.63	-	46.32
SIKE	934.10	1444.90	3056.10	-	4598.90
SIKE Compressed	1747.20	2619.30	4808.90	-	8492.00
Three Bears	-	0.98	-	1.52	2.52
Three Bears Eph.	-	0.93	-	1.83	2.41

Table 6: Energy consumption of `crypto_kem_enc` function for **Encapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

UNIVERSITY OF WATERLOO

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	6.83	-	20.21	-	48.65
BIKE-1 CPA	5.94	-	15.20	-	26.53
BIKE-2 CCA	2.70	-	8.75	-	21.54
BIKE-2 CPA	2.36	-	5.86	-	11.06
BIKE-3 CCA	5.55	-	18.82	-	45.70
BIKE-3 CPA	4.85	-	13.74	-	34.70
Classic McEliece	1.84	-	3.09	-	4.81
CRYSTALS-Kyber	6.00	-	9.13	-	14.62
CRYSTALS-Kyber-90s	7.62	-	13.94	-	21.10
FRODO AES	14.71	-	32.20	-	47.96
FRODO SHAKE	13.97	-	30.88	-	48.53
hqc-1	18.42	-	42.92	-	65.85
hqc-2	-	-	41.81	-	76.53
hqc-3	-	-	-	-	87.53
LAC	1.28	-	3.53	-	4.58
LEDAcrypt N02	20.14	-	47.00	-	81.90
LEDAcrypt N03	15.90	-	38.10	-	88.00
LEDAcrypt N04	20.87	-	49.70	-	101.90
LEDAcrypt LT DFR64	70.50	-	137.40	-	234.00
LEDAcrypt LT DFRSL	115.50	-	291.00	-	526.30
NewHope CCA	8.19	-	-	-	16.57
NewHope CPA	7.47	-	-	-	12.56
NTRU-HPS	22.21	-	36.35	-	48.03
NTRU-HRSS	-	-	33.59	-	-
sNTRU Prime	-	177.50	236.95	300.36	-
NTRU LPrime	-	330.60	450.95	586.52	-
NTS-KEM	0.92	-	3.55	-	4.66
ROLLO-I	3.63	-	5.21	-	6.62
ROLLO-II	18.71	-	25.06	-	22.81
ROLLO-III	8.60	-	10.24	-	16.02
Round5 Ring	0.93	-	3.09	-	3.88
Round5 Ring 5	1.14	-	1.86	-	3.38
Round5 Ring Long Key	1.18	-	-	-	-
Round5 Non-Ring	47.47	-	118.22	-	222.17
RQC	12.86	-	23.67	-	36.61
SABER	19.04	-	29.63	-	46.32
SIKE	934.10	1444.90	3056.10	-	4598.90
SIKE Compressed	1747.20	2619.30	4808.90	-	8492.00
Three Bears	-	0.98	-	1.52	2.52
Three Bears Eph.	-	0.93	-	1.83	2.41

Table 6: Energy consumption of **`crypto_kem_enc`** function for **Encapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Key Encapsulation

- Best Lattice-Based: **Three Bears**
  - L1: 0.93mJ
  - L3: 1.52mJ
  - L5: 2.41mJ

- Best Code-Based: **NTS-KEM & Classic McEliece**
  - *L1: 0.92mJ* L1: 1.84mJ
  - L3: 3.55mJ *L3: 3.09mJ*
  - *L5: 4.66mJ* L5: 4.81mJ

- Best Other: **ROLLO-I**
  - L1: 3.63mJ
  - L3: 5.21mJ
  - L5: 6.62mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	60.10	-	132.60	-	364.80
BIKE-1 CPA	29.10	-	89.00	-	213.90
BIKE-2 CCA	46.30	-	119.60	-	270.70
BIKE-2 CPA	31.80	-	83.00	-	185.00
BIKE-3 CCA	57.90	-	140.00	-	331.70
BIKE-3 CPA	33.00	-	97.60	-	216.60
Classic McEliece	588.10	-	1497.50	-	2625.30
CRYSTALS-Kyber	7.05	-	10.51	-	14.62
CRYSTALS-Kyber-90s	9.47	-	16.10	-	23.25
FRODO AES	12.28	-	29.30	-	41.20
FRODO SHAKE	15.90	-	33.90	-	40.10
hqc-1	27.03	-	64.69	-	100.60
hqc-2	-	-	70.26	-	124.78
hqc-3	-	-	-	-	145.55
LAC	2.14	-	5.56	-	7.00
LEDAcrypt N02	105.30	-	225.10	-	391.70
LEDAcrypt N03	98.80	-	240.20	-	496.70
LEDAcrypt N04	148.50	-	354.20	-	539.40
LEDAcrypt LT DFR64	96.90	-	196.10	-	380.00
LEDAcrypt LT DFRSL	105.50	-	279.80	-	534.10
NewHope CCA	8.10	-	-	-	18.76
NewHope CPA	1.45	-	-	-	2.78
NTRU-HPS	54.36	-	98.28	-	137.03
NTRU-HRSS	-	-	100.51	-	-
sNTRU Prime	-	507.96	703.16	877.00	-
NTRU LPrime	-	483.38	657.76	851.96	-
NTS-KEM	6.32	-	12.76	-	27.74
ROLLO-I	13.31	-	25.09	-	40.53
ROLLO-II	52.76	-	64.58	-	75.37
ROLLO-III	12.63	-	25.55	-	40.03
Round5 Ring	0.39	-	1.73	-	2.24
Round5 Ring 5	0.66		1.04		1.78
Round5 Ring Long Key	0.54	-	-	-	-
Round5 Non-Ring	2.98	-	4.91	-	1.87
RQC	75.54	-	176.17	-	273.43
SABER	19.04	-	33.22	-	51.68
SIKE	999.30	1543.40	3104.50	-	4983.70
SIKE Compressed	1648.10	2417.50	4636.90	-	7880.20
Three Bears	-	1.40	-	2.25	3.54
Three Bears Eph.	-	0.44	-	0.63	0.71

Table 7: Energy consumption of `crypto_kem_dec` function for **Decapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE-1 CCA	60.10	-	132.60	-	364.80
BIKE-1 CPA	29.10	-	89.00	-	213.90
BIKE-2 CCA	46.30	-	119.60	-	270.70
BIKE-2 CPA	31.80	-	83.00	-	185.00
BIKE-3 CCA	57.90	-	140.00	-	331.70
BIKE-3 CPA	33.00	-	97.60	-	216.60
Classic McEliece	588.10	-	1497.50	-	2625.30
CRYSTALS-Kyber	7.05	-	10.51	-	14.62
CRYSTALS-Kyber-90s	9.47	-	16.10	-	23.25
FRODO AES	12.28	-	29.30	-	41.20
FRODO SHAKE	15.90	-	33.90	-	40.10
hqc-1	27.03	-	64.69	-	100.60
hqc-2	-	-	70.26	-	124.78
hqc-3	-	-	-	-	145.55
LAC	2.14	-	5.56	-	7.00
LEDAcrypt N02	105.30	-	225.10	-	391.70
LEDAcrypt N03	98.80	-	240.20	-	496.70
LEDAcrypt N04	148.50	-	354.20	-	539.40
LEDAcrypt LT DFR64	96.90	-	196.10	-	380.00
LEDAcrypt LT DFRSL	105.50	-	279.80	-	534.10
NewHope CCA	8.10	-	-	-	18.76
NewHope CPA	1.45	-	-	-	2.78
NTRU-HPS	54.36	-	98.28	-	137.03
NTRU-HRSS	-	-	100.51	-	-
sNTRU Prime	-	507.96	703.16	877.00	-
NTRU LPrime	-	483.38	657.76	851.96	-
NTS-KEM	6.32	-	12.76	-	27.74
ROLLO-I	13.31	-	25.09	-	40.53
ROLLO-II	52.76	-	64.58	-	75.37
ROLLO-III	12.63	-	25.55	-	40.03
Round5 Ring	0.39	-	1.73	-	2.24
Round5 Ring 5	0.66		1.04		1.78
Round5 Ring Long Key	0.54	-	-	-	-
Round5 Non-Ring	2.98	-	4.91	-	1.87
RQC	75.54	-	176.17	-	273.43
SABER	19.04	-	33.22	-	51.68
SIKE	999.30	1543.40	3104.50	-	4983.70
SIKE Compressed	1648.10	2417.50	4636.90	-	7880.20
Three Bears	-	1.40	-	2.25	3.54
Three Bears Eph.	-	0.44	-	0.63	0.71

Table 7: Energy consumption of `crypto_kem_dec` function for **Decapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Key Decapsulation

- Best Lattice-Based: **Round5 Ring & Three Bears Eph.**
  - *L1: 0.39mJ* L1: 0.44mJ
  - L3: 1.04mJ *L3: 0.63mJ*
  - L5: 1.78mJ *L5: 0.71mJ*

- Best Code-Based: **NTS-KEM**
  - L1: 6.32mJ
  - L3: 12.76mJ
  - L5: 27.74mJ

- Best Other: **ROLLO-I, -III**
  - L1: 13.31mJ *L1: 12.63mJ*
  - *L3: 25.09mJ* L3: 25.55mJ
  - L5: 40.53mJ *L5: 40.03mJ*

UNIVERSITY OF WATERLOO

Results for Optimized C Implementation

Public-Key Encryption Schemes

Table 8: Energy consumption of `crypto_encrypt_keypair` function for **Keypair Generation** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	7944.20	29007.10	85229.90
LEDAcrypt DFRSL	11944.40	42496.40	127181.70
LAC	0.85	2.61	2.83

Table 9: Energy consumption of `crypto_encrypt` function for **Encryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	10.98	18.76	33.99
LEDAcrypt DFRSL	15.26	36.86	57.75
LAC	1.43	3.32	4.63

Table 10: Energy consumption of `crypto_encrypt_open` function for **Decryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	30.95	57.40	113.34
LEDAcrypt DFRSL	44.40	94.63	179.09
LAC	0.66	2.39	2.12

Table 8: Energy consumption of `crypto_encrypt_keypair` function for **Keypair Generation** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	7944.20	29007.10	85229.90
LEDAcrypt DFRSL	11944.40	42496.40	127181.70
LAC	0.85	2.61	2.83

Table 9: Energy consumption of `crypto_encrypt` function for **Encryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	10.98	18.76	33.99
LEDAcrypt DFRSL	15.26	36.86	57.75
LAC	1.43	3.32	4.63

🟥 Highest energy per level

🟩 Lowest energy per level

Table 10: Energy consumption of `crypto_encrypt_open` function for **Decryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	30.95	57.40	113.34
LEDAcrypt DFRSL	44.40	94.63	179.09
LAC	0.66	2.39	2.12

Results for Optimized C Implementation

Digital Signature Schemes

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	1.51	1.65	1.49	1.47	-
CRYSTALS-Dilithium AES	3.28	5.44	8.73	11.46	-
Falcon	189.80	-	-	-	537.60
GeMSS	552.20	-	3255.20	-	9738.20
BlueGeMSS	539.10	-	3106.30	-	9076.60
RedGeMSS	512.20	-	2798.60	-	8520.70
Luov Small Sig Chacha	-	105.80	-	412.50	745.20
Luov Small Sig Keccak	-	126.80	-	496.90	828.20
Luov Large Sig Chacha	-	69.30	-	187.50	455.80
Luov Large Sig Keccak	-	82.90	-	218.40	532.30
MQDSS	-	27.63	-	57.60	-
Picnic UR	0.23	-	0.33	-	0.45
Picnic FS	0.24	-	0.33	-	0.44
Picnic2 FS	0.22	-	0.34	-	0.45
qTESLA	10.04	50.24	28.36	-	146.03
qTESLA-s	10.25	51.06	28.78	-	152.73
qTESLA-p	63.55	-	226.51	-	-
qTESLA-size	-	-	-	-	228.22
qTESLA-size-s	-	-	-	-	209.51
Rainbow Classic	229.50	-	3361.80	-	8411.50
Rainbow Compressed/Cyclic	253.50	-	3714.70	-	9010.50
Rainbow Cyclic	272.80	-	4058.50	-	9320.00
SPHINCS+ SHA256 s simple	1761.00	-	2524.20	-	3501.40
SPHINCS+ SHA256 s robust	3516.90	-	5296.00	-	9586.10
SPHINCS+ SHA256 f simple	48.10	-	81.10	-	212.00
SPHINCS+ SHA256 f robust	108.70	-	151.80	-	615.40
SPHINCS+ SHAKE256 s simple	3019.90	-	4044.10	-	5446.20
SPHINCS+ SHAKE256 s robust	5174.00	-	7608.60	-	10754.80
SPHINCS+ SHAKE256 f simple	83.80	-	123.60	-	342.20
SPHINCS+ SHAKE256 f robust	171.80	-	237.90	-	652.00
SPHINCS+ HARAKA s simple	4745.70	6759.60	-	-	-
SPHINCS+ HARAKA s robust	6965.70	10444.40	-	-	-
SPHINCS+ HARAKA f simple	143.80	214.80	-	-	-
SPHINCS+ HARAKA f robust	219.30	320.10	-	-	-

Table 11: Energy consumption of `crypto_sign_keypair` function for **Keypair Generation** of Round 2 **Digital Signatures**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	1.51	1.65	1.49	1.47	-
CRYSTALS-Dilithium AES	3.28	5.44	8.73	11.46	-
Falcon	189.80	-	-	-	537.60
GeMSS	552.20	-	3255.20	-	9738.20
BlueGeMSS	539.10	-	3106.30	-	9076.60
RedGeMSS	512.20	-	2798.60	-	8520.70
Luov Small Sig Chacha	-	105.80	-	412.50	745.20
Luov Small Sig Keccak	-	126.80	-	496.90	828.20
Luov Large Sig Chacha	-	69.30	-	187.50	455.80
Luov Large Sig Keccak	-	82.90	-	218.40	532.30
MQDSS	-	27.63	-	57.60	-
Picnic UR	0.23	-	0.33	-	0.45
Picnic FS	0.24	-	0.33	-	0.44
Picnic2 FS	0.22	-	0.34	-	0.45
qTESLA	10.04	50.24	28.36	-	146.03
qTESLA-s	10.25	51.06	28.78	-	152.73
qTESLA-p	63.55	-	226.51	-	-
qTESLA-size	-	-	-	-	228.22
qTESLA-size-s	-	-	-	-	209.51
Rainbow Classic	229.50	-	3361.80	-	8411.50
Rainbow Compressed/Cyclic	253.50	-	3714.70	-	9010.50
Rainbow Cyclic	272.80	-	4058.50	-	9320.00
SPHINCS+ SHA256 s simple	1761.00	-	2524.20	-	3501.40
SPHINCS+ SHA256 s robust	3516.90	-	5296.00	-	9586.10
SPHINCS+ SHA256 f simple	48.10	-	81.10	-	212.00
SPHINCS+ SHA256 f robust	108.70	-	151.80	-	615.40
SPHINCS+ SHAKE256 s simple	3019.90	-	4044.10	-	5446.20
SPHINCS+ SHAKE256 s robust	5174.00	-	7608.60	-	10754.80
SPHINCS+ SHAKE256 f simple	83.80	-	123.60	-	342.20
SPHINCS+ SHAKE256 f robust	171.80	-	237.90	-	652.00
SPHINCS+ HARAKA s simple	4745.70	6759.60	-	-	-
SPHINCS+ HARAKA s robust	6965.70	10444.40	-	-	-
SPHINCS+ HARAKA f simple	143.80	214.80	-	-	-
SPHINCS+ HARAKA f robust	219.30	320.10	-	-	-

Table 11: Energy consumption of `crypto_sign_keypair` function for **Keypair Generation** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥 Highest energy per level

🟩 Lowest energy per level

Comparison of Results: Keypair Generation

- Best Lattice-Based: **CRYSTALS-Dilithium SHAKE & qTESLA**
  - *L1: 1.51mJ* L1: 10.04mJ
  - *L3: 1.49mJ* L3: 28.36mJ
  - L5: N/A *L5: 146.03mJ*

- Best Multivariate-Based: **MQDSS & LUOV L. Signature ChaCha**
  - *L1: 27.63mJ* L1: 69.30mJ
  - *L3: 57.60mJ* L3: 187.50mJ
  - L5: N/A *L5: 455.80mJ*

- Best Other: **Picnic**
  - L1: 0.22mJ
  - L3: 0.33mJ
  - L5: 0.44mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	7.92	8.63	8.09	8.02	-
CRYSTALS-Dilithium AES	11.82	19.56	30.75	29.34	-
Falcon	6.40	-	-	-	16.61
GeMSS	17800.40	-	69223.60	-	142192.80
BlueGeMSS	2733.50	-	10449.80	-	17805.80
RedGeMSS	66.20	-	255.20	-	497.60
Luov Small Sig Chacha	-	39.80	-	98.20	176.20
Luov Small Sig Keccak	-	66.50	-	171.40	267.90
Luov Large Sig Chacha	-	207.40	-	568.00	1286.90
Luov Large Sig Keccak	-	222.60	-	623.10	1406.90
MQDSS	-	1219.10	-	3800.20	-
Picnic UR	137.10	-	365.90	-	673.10
Picnic FS	103.80	-	262.70	-	477.00
Picnic2 FS	3865.00	-	11413.50	-	24415.60
qTESLA	5.12	13.68	8.47	-	23.30
qTESLA-s	5.39	14.43	8.66	-	24.21
qTESLA-p	30.77	-	82.96	-	
qTESLA-size	-	-	-	-	31.30
qTESLA-size-s	-	-	-	-	33.17
Rainbow Classic	2.89	-	25.53	-	51.66
Rainbow Compressed/Cyclic	3.83	-	1902.70	-	4482.50
Rainbow Cyclic	3.22	-	24.75	-	54.97
SPHINCS+ SHA256 s simple	26494.90	-	63668.10	-	45710.80
SPHINCS+ SHA256 s robust	49013.50	-	120274.90	-	118541.20
SPHINCS+ SHA256 f simple	1799.70	-	2368.80	-	5236.80
SPHINCS+ SHA256 f robust	3446.70	-	4422.90	-	14426.20
SPHINCS+ SHAKE256 s simple	43964.30	-	86931.90	-	65658.40
SPHINCS+ SHAKE256 s robust	73310.80	-	148952.00	-	121794.40
SPHINCS+ SHAKE256 f simple	2926.10	-	3638.40	-	8049.60
SPHINCS+ SHAKE256 f robust	5257.30	-	6715.30	-	14767.70
SPHINCS+ HARAKA s simple	85968.10	184990.60	-	-	-
SPHINCS+ HARAKA s robust	130367.00	320977.50	-	-	-
SPHINCS+ HARAKA f simple	5367.00	6287.40	-	-	-
SPHINCS+ HARAKA f robust	8171.70	9742.30	-	-	-

Table 12: Energy consumption of `crypto_sign` function for **Signing** of Round 2 **Digital Signatures**. Energy is in milliJoules.

UNIVERSITY OF WATERLOO

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	7.92	8.63	8.09	8.02	-
CRYSTALS-Dilithium AES	11.82	19.56	30.75	29.34	-
Falcon	6.40	-	-	-	16.61
GeMSS	17800.40	-	69223.60	-	142192.80
BlueGeMSS	2733.50	-	10449.80	-	17805.80
RedGeMSS	66.20	-	255.20	-	497.60
Luov Small Sig Chacha	-	39.80	-	98.20	176.20
Luov Small Sig Keccak	-	66.50	-	171.40	267.90
Luov Large Sig Chacha	-	207.40	-	568.00	1286.90
Luov Large Sig Keccak	-	222.60	-	623.10	1406.90
MQDSS	-	1219.10	-	3800.20	-
Picnic UR	137.10	-	365.90	-	673.10
Picnic FS	103.80	-	262.70	-	477.00
Picnic2 FS	3865.00	-	11413.50	-	24415.60
qTESLA	5.12	13.68	8.47	-	23.30
qTESLA-s	5.39	14.43	8.66	-	24.21
qTESLA-p	30.77	-	82.96	-	
qTESLA-size	-	-	-	-	31.30
qTESLA-size-s	-	-	-	-	33.17
Rainbow Classic	2.89	-	25.53	-	51.66
Rainbow Compressed/Cyclic	3.83	-	1902.70	-	4482.50
Rainbow Cyclic	3.22	-	24.75	-	54.97
SPHINCS+ SHA256 s simple	26494.90	-	63668.10	-	45710.80
SPHINCS+ SHA256 s robust	49013.50	-	120274.90	-	118541.20
SPHINCS+ SHA256 f simple	1799.70	-	2368.80	-	5236.80
SPHINCS+ SHA256 f robust	3446.70	-	4422.90	-	14426.20
SPHINCS+ SHAKE256 s simple	43964.30	-	86931.90	-	65658.40
SPHINCS+ SHAKE256 s robust	73310.80	-	148952.00	-	121794.40
SPHINCS+ SHAKE256 f simple	2926.10	-	3638.40	-	8049.60
SPHINCS+ SHAKE256 f robust	5257.30	-	6715.30	-	14767.70
SPHINCS+ HARAKA s simple	85968.10	184990.60	-	-	-
SPHINCS+ HARAKA s robust	130367.00	320977.50	-	-	-
SPHINCS+ HARAKA f simple	5367.00	6287.40	-	-	-
SPHINCS+ HARAKA f robust	8171.70	9742.30	-	-	-

Table 12: Energy consumption of `crypto_sign` function for **Signing** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

UNIVERSITY OF WATERLOO

Comparison of Results: Signing

- Best Lattice-Based: **qTESLA-s, CRYSTALS-Dilithium SHAKE & Falcon**

L1: 5.39mJ	L1:7.92mJ	L1:6.40mJ
L3: 8.66mJ	*L3: 8.09mJ*	L3: N/A
L5: 24.21mJ	L5: N/A	*L5: 16.61mJ*

- Best Multivariate-Based: **Rainbow Classic & Cyclic**

L1: 2.89mJ	L1: 3.22mJ
L3: 25.53mJ	*L2: 24.75mJ*
L5: 51.66mJ	L5: 54.97mJ

- Best Other: **Picnic FS**
  - L1: 103.80mJ
  - L3: 262.70mJ
  - L5: 477.00mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	2.39	2.08	2.46	2.47	-
CRYSTALS-Dilithium AES	3.73	5.70	8.58	12.04	-
Falcon	1.41	-	-	-	2.73
GeMSS	1.70	-	4.10	-	8.29
BlueGeMSS	1.60	-	3.97	-	8.48
RedGeMSS	4.48	-	5.94	-	14.08
Luov Small Sig Chacha	-	31.70	-	78.70	138.20
Luov Small Sig Keccak	-	46.10	-	146.40	231.10
Luov Large Sig Chacha	-	134.00	-	370.80	653.10
Luov Large Sig Keccak	-	150.00	-	403.70	724.50
MQDSS	-	893.40	-	2825.10	-
Picnic UR	119.90	-	310.80	-	539.30
Picnic FS	97.90	-	227.60	-	416.40
Picnic2 FS	1853.80	-	4290.90	-	7862.40
qTESLA	1.23	2.85	2.12	-	4.37
qTESLA-s	1.15	2.90	2.34	-	4.43
qTESLA-p	6.94	-	19.46	-	-
qTESLA-size	-	-	-	-	6.20
qTESLA-size-s	-	-	-	-	6.07
Rainbow Classic	2.37	-	34.30	-	55.79
Rainbow Compressed/Cyclic	31.45	-	188.87	-	436.90
Rainbow Cyclic	31.62	-	183.00	-	460.50
SPHINCS+ SHA256 s simple	29.48	-	48.20	-	62.00
SPHINCS+ SHA256 s robust	59.13	-	99.37	-	185.20
SPHINCS+ SHA256 f simple	71.16	-	121.46	-	113.30
SPHINCS+ SHA256 f robust	151.26	-	237.49	-	353.40
SPHINCS+ SHAKE256 s simple	47.87	-	70.58	-	90.90
SPHINCS+ SHAKE256 s robust	92.77	-	132.04	-	179.60
SPHINCS+ SHAKE256 f simple	114.99	-	186.72	-	172.20
SPHINCS+ SHAKE256 f robust	221.60	-	346.07	-	376.60
SPHINCS+ HARAKA s simple	89.60	146.50	-	-	-
SPHINCS+ HARAKA s robust	136.80	231.50	-	-	-
SPHINCS+ HARAKA f simple	218.60	357.50	-	-	-
SPHINCS+ HARAKA f robust	355.10	533.90	-	-	-

Table 13: Energy consumption of `crypto_sign_open` function for **Verification** of Round 2 **Digital Signatures**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	2.39	2.08	2.46	2.47	-
CRYSTALS-Dilithium AES	3.73	5.70	8.58	12.04	-
Falcon	1.41	-	-	-	2.73
GeMSS	1.70	-	4.10	-	8.29
BlueGeMSS	1.60	-	3.97	-	8.48
RedGeMSS	4.48	-	5.94	-	14.08
Luov Small Sig Chacha	-	31.70	-	78.70	138.20
Luov Small Sig Keccak	-	46.10	-	146.40	231.10
Luov Large Sig Chacha	-	134.00	-	370.80	653.10
Luov Large Sig Keccak	-	150.00	-	403.70	724.50
MQDSS	-	893.40	-	2825.10	-
Picnic UR	119.90	-	310.80	-	539.30
Picnic FS	97.90	-	227.60	-	416.40
Picnic2 FS	1853.80	-	4290.90	-	7862.40
qTESLA	1.23	2.85	2.12	-	4.37
qTESLA-s	1.15	2.90	2.34	-	4.43
qTESLA-p	6.94	-	19.46	-	-
qTESLA-size	-	-	-	-	6.20
qTESLA-size-s	-	-	-	-	6.07
Rainbow Classic	2.37	-	34.30	-	55.79
Rainbow Compressed/Cyclic	31.45	-	188.87	-	436.90
Rainbow Cyclic	31.62	-	183.00	-	460.50
SPHINCS+ SHA256 s simple	29.48	-	48.20	-	62.00
SPHINCS+ SHA256 s robust	59.13	-	99.37	-	185.20
SPHINCS+ SHA256 f simple	71.16	-	121.46	-	113.30
SPHINCS+ SHA256 f robust	151.26	-	237.49	-	353.40
SPHINCS+ SHAKE256 s simple	47.87	-	70.58	-	90.90
SPHINCS+ SHAKE256 s robust	92.77	-	132.04	-	179.60
SPHINCS+ SHAKE256 f simple	114.99	-	186.72	-	172.20
SPHINCS+ SHAKE256 f robust	221.60	-	346.07	-	376.60
SPHINCS+ HARAKA s simple	89.60	146.50	-	-	-
SPHINCS+ HARAKA s robust	136.80	231.50	-	-	-
SPHINCS+ HARAKA f simple	218.60	357.50	-	-	-
SPHINCS+ HARAKA f robust	355.10	533.90	-	-	-

Table 13: Energy consumption of `crypto_sign_open` function for **Verification** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Verification

- Best Lattice-Based: **qTESLA, qTESLA-s, & Falcon**

L1: 1.23mJ	*L1: 1.15mJ*	L1: 1.41mJ
L3: 2.12mJ	L3: 2.34mJ	L3: N/A
L5: 4.37mJ	L5: 4.43mJ	*L5: 2.73mJ*

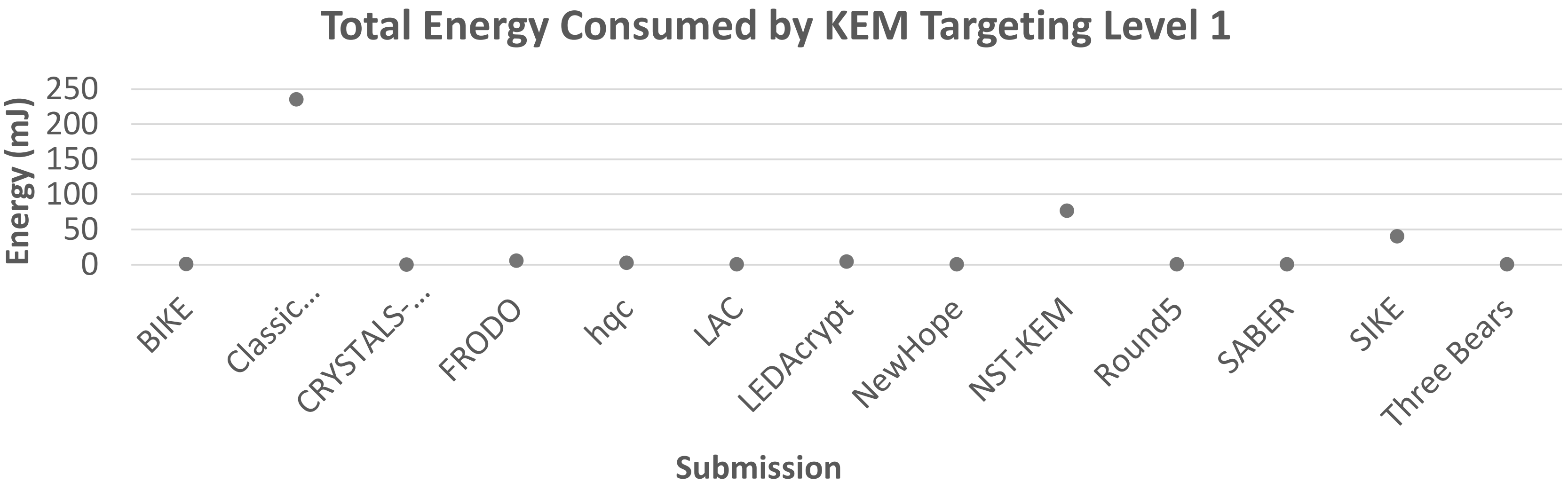
- Best Multivariate-Based: **BlueGeMSS & GeMSS**

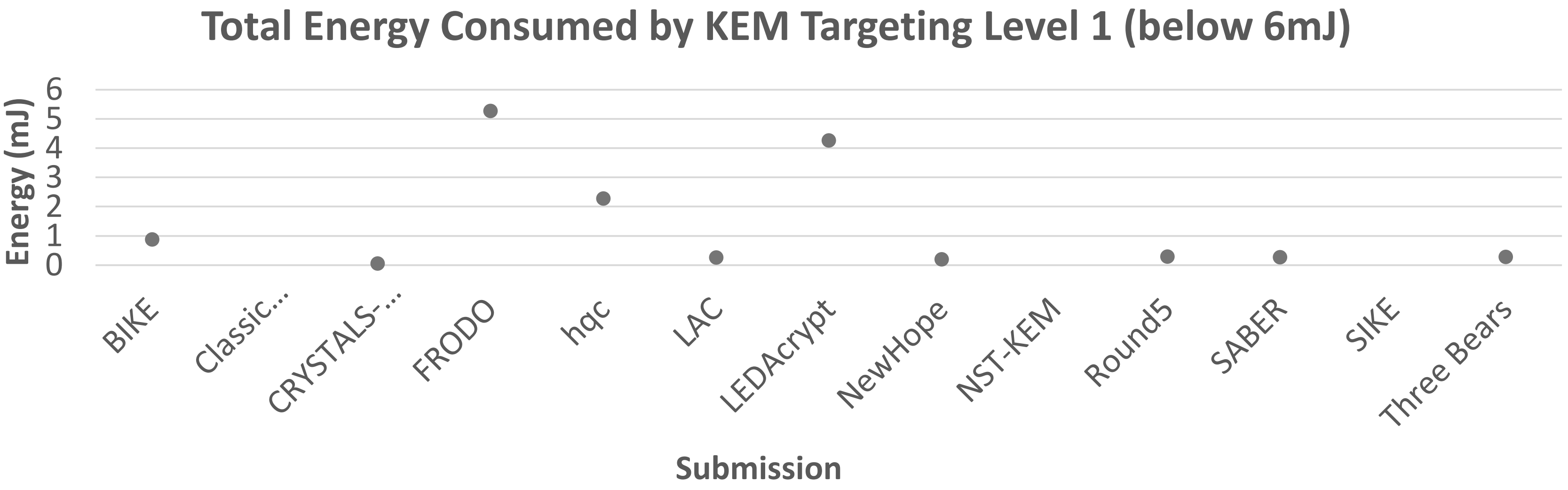
L1: 1.60mJ	L1: 1.70mJ
L3: 3.97mJ	L2: 4.10mJ
L5: 8.48mJ	*L5: 8.29mJ*

- Best Other: **SPHINCS+ SHA256 s simple**
  - L1: 29.48mJ
  - L3: 48.20mJ
  - L5: 62.00mJ

Results for Assembly Optimized Implementation

Key Encapsulation Mechanisms





UNIVERSITY OF WATERLOO

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.304	-	0.922	-	2.138
BIKE2	22.535	-	82.097	-	230.485
BIKE3	0.185	-	0.591	-	1.375
Classic McEliece AVX	234.940	-	857.444	-	1735.456
Classic McEliece SSE	463.182	-	1507.966	-	2429.805
CRYSTALS-Kyber	0.021	-	0.083	-	0.117
CRYSTALS-Kyber-90s	0.014	-	0.018	-	0.026
FRODO AES	1.582	-	2.981	-	3.481
FRODO SHAKE	6.121	-	12.927	-	22.985
hqc-1	0.317	-	0.599	-	0.955
hqc-2	-	-	0.649	-	0.964
hqc-3	-	-	-	-	1.009
LAC	0.064	-	0.112	-	0.145
LEDAcrypt N02	5.756	-	17.681	-	36.900
LEDAcrypt N03	2.501	-	8.418	-	22.711
LEDAcrypt N04	4.135	-	11.942	-	24.722
LEDAcrypt DFR64	1417.029	-	4680.601	-	14371.200
LEDAcrypt DFRSL	2087.827	-	7311.765	-	20787.330
NewHope CCA	0.094	-	-	-	0.178
NewHope CPA	0.068	-	-	-	0.145
NTRU-HRSS	-	-	0.325	-	-
NTS-KEM AVX	75.823	-	242.256	-	434.092
NTS-KEM SSE	79.173	-	241.025	-	443.702
Round5 Ring	0.078	-	0.282	-	0.360
Round5 Ring 5	0.113	-	0.187	-	0.331
Round5 Non-Ring	0.846	-	1.522	-	3.753
Round 5 LongKey	0.143	-	-	-	-
SABER	0.064	-	0.139	-	0.198
SIKE	9.287	13.075	22.065	-	37.085
SIKE Compressed	24.768	33.980	58.277	-	90.272
Three Bears	-	0.097	-	0.180	0.292
Three Bears Eph.	-	0.098	-	0.189	0.295

Table 14: Energy consumption of **`crypto_kem_keypair`** function for **Keypair Generation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.304	-	0.922	-	2.138
BIKE2	22.535	-	82.097	-	230.485
BIKE3	0.185	-	0.591	-	1.375
Classic McEliece AVX	234.940	-	857.444	-	1659.074
Classic McEliece SSE	463.182	-	1507.966	-	2274669
CRYSTALS-Kyber	0.021	-	0.083	-	0.117
CRYSTALS-Kyber-90s	0.014	-	0.018	-	0.026
FRODO AES	1.582	-	2.981	-	3.481
FRODO SHAKE	6.121	-	12.927	-	22.985
hqc-1	0.317	-	0.599	-	0.955
hqc-2	-	-	0.649	-	0.964
hqc-3	-	-	-	-	1.009
LAC	0.064	-	0.112	-	0.145
LEDAcrypt N02	5.756	-	17.681	-	36.900
LEDAcrypt N03	2.501	-	8.418	-	22.711
LEDAcrypt N04	4.135	-	11.942	-	24.722
LEDAcrypt DFR64	1417.029	-	4680.601	-	14371.200
LEDAcrypt DFRSL	2087.827	-	7311.765	-	20787.330
NewHope CCA	0.094	-	-	-	0.178
NewHope CPA	0.068	-	-	-	0.145
NTRU-HRSS	-	-	0.325	-	-
NTS-KEM AVX	75.823	-	242.256	-	434.092
NTS-KEM SSE	79.173	-	241.025	-	443.702
Round5 Ring	0.078	-	0.282	-	0.360
Round5 Ring 5	0.113	-	0.187	-	0.331
Round5 Non-Ring	0.846	-	1.522	-	3.753
Round 5 LongKey	0.143	-	-	-	-
SABER	0.064	-	0.139	-	0.198
SIKE	9.287	13.075	22.065	-	37.085
SIKE Compressed	24.768	33.980	58.277	-	90.272
Three Bears	-	0.097	-	0.180	0.292
Three Bears Eph.	-	0.098	-	0.189	0.295

Table 14: Energy consumption of **`crypto_kem_keypair`** function for **Keypair Generation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Keypair Generation

- Best Lattice-Based: **CRYSTALS-Kyber 90s**
  - L1: 0.014mJ
  - L3: 0.018mJ
  - L5: 0.026mJ

- Best Code-Based: **BIKE3 & hqc-1**
  - *L1: 0.185mJ* L1: 0.317mJ
  - *L3: 0.591mJ* L2: 0.599mJ
  - L5: 1.375mJ *L3: 0.955mJ*

- Best Other: **SIKE**
  - L1: 9.287mJ
  - L3: 22.065mJ
  - L5: 37.085mJ

UNIVERSITY OF WATERLOO

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.358	-	1.046	-	2.368
BIKE2	0.187	-	0.442	-	1.135
BIKE3	0.337	-	1.130	-	2.790
Classic McEliece AVX	0.059	-	0.111	-	0.087
Classic McEliece SSE	0.062	-	0.114	-	0.143
CRYSTALS-Kyber	0.090	-	0.108	-	0.145
CRYSTALS-Kyber-90s	0.018	-	0.020	-	0.039
FRODO AES	1.917	-	3.474	-	5.279
FRODO SHAKE	6.687	-	14.067	-	24.482
hqc-1	0.647	-	1.160	-	1.734
hqc-2	-	-	1.227	-	1.899
hqc-3	-	-	-	-	2.004
LAC	0.087	-	0.146	-	0.244
LEDAcrypt N02	0.223	-	0.469	-	0.856
LEDAcrypt N03	0.164	-	0.381	-	0.865
LEDAcrypt N04	0.188	-	0.528	-	1.004
LEDAcrypt DFR64	0.675	-	1.296	-	2.830
LEDAcrypt DFRSL	0.803	-	2.770	-	4.230
NewHope CCA	0.137	-	-	-	0.251
NewHope CPA	0.102	-	-	-	0.194
NTRU-HRSS	-	-	0.131	-	-
NTS-KEM AVX	0.161	-	0.682	-	0.932
NTS-KEM SSE	0.164	-	0.683	-	0.941
Round5 Ring	0.145	-	0.470	-	0.606
Round5 Ring 5	0.194	-	0.342	-	0.548
Round5 Non-Ring	0.913	-	1.631	-	3.795
Round 5 LongKey	0.191	-	-	-	-
SABER	0.110	-	0.166	-	0.234
SIKE	15.006	21.113	40.641	-	60.455
SIKE Compressed	29.527	39.560	69.651	-	114.244
Three Bears	-	0.135	-	0.210	0.339
Three Bears Eph.	-	0.126	-	0.210	0.342

Table 15: Energy consumption of `crypto_kem_enc` function for **Encapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.358	-	1.046	-	2.368
BIKE2	0.187	-	0.442	-	1.135
BIKE3	0.337	-	1.130	-	2.790
Classic McEliece AVX	0.059	-	0.111	-	0.087
Classic McEliece SSE	0.062	-	0.114	-	0.143
CRYSTALS-Kyber	0.090	-	0.108	-	0.145
CRYSTALS-Kyber-90s	0.018	-	0.020	-	0.039
FRODO AES	1.917	-	3.474	-	5.279
FRODO SHAKE	6.687	-	14.067	-	24.482
hqc-1	0.647	-	1.160	-	1.734
hqc-2	-	-	1.227	-	1.899
hqc-3	-	-	-	-	2.004
LAC	0.087	-	0.146	-	0.244
LEDAcrypt N02	0.223	-	0.469	-	0.856
LEDAcrypt N03	0.164	-	0.381	-	0.865
LEDAcrypt N04	0.188	-	0.528	-	1.004
LEDAcrypt DFR64	0.675	-	1.296	-	2.830
LEDAcrypt DFRSL	0.803	-	2.770	-	4.230
NewHope CCA	0.137	-	-	-	0.251
NewHope CPA	0.102	-	-	-	0.194
NTRU-HRSS	-	-	0.131	-	-
NTS-KEM AVX	0.161	-	0.682	-	0.932
NTS-KEM SSE	0.164	-	0.683	-	0.941
Round5 Ring	0.145	-	0.470	-	0.606
Round5 Ring 5	0.194	-	0.342	-	0.548
Round5 Non-Ring	0.913	-	1.631	-	3.795
Round 5 LongKey	0.191	-	-	-	-
SABER	0.110	-	0.166	-	0.234
SIKE	15.006	21.113	40.641	-	60.455
SIKE Compressed	29.527	39.560	69.651	-	114.244
Three Bears	-	0.135	-	0.210	0.339
Three Bears Eph.	-	0.126	-	0.210	0.342

Table 15: Energy consumption of **`crypto_kem_enc`** function for **Encapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Key Encapsulation

- Best Lattice-Based: **CRYSTALS-Kyber 90s**
  - L1: 0.018mJ
  - L3: 0.020mJ
  - L5: 0.039mJ

- Best Code-Based: **Classic McEliece AVX**
  - L1: 0.059mJ
  - L3: 0.111mJ
  - L5: 0.087mJ

- Best Other: **SIKE**
  - L1: 15.006mJ
  - L3: 40.641mJ
  - L5: 60.455mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.457	-	1.152	-	2.660
BIKE2	0.254	-	0.726	-	1.489
BIKE3	0.354	-	0.887	-	2.099
Classic McEliece AVX	0.190	-	0.179	-	0.264
Classic McEliece SSE	0.160	-	0.201	-	0.162
CRYSTALS-Kyber	0.047	-	0.081	-	0.135
CRYSTALS-Kyber-90s	0.014	-	0.028	-	0.043
FRODO AES	1.763	-	3.086	-	4.975
FRODO SHAKE	6.515	-	13.629	-	24.725
hqc-1	1.310	-	2.018	-	3.012
hqc-2	-	-	2.189	-	3.195
hqc-3	-	-	-	-	3.310
LAC	0.103	-	0.263	-	0.320
LEDAcrypt N02	1.254	-	3.137	-	5.973
LEDAcrypt N03	1.596	-	3.764	-	7.140
LEDAcrypt N04	4.203	-	9.427	-	15.056
LEDAcrypt DFR64	1.598	-	3.655	-	6.450
LEDAcrypt DFRSL	2.265	-	5.064	-	9.380
NewHope CCA	0.146	-	-	-	0.253
NewHope CPA	0.022	-	-	-	0.034
NTRU-HRSS	-	-	0.053	-	-
NTS-KEM AVX	0.805	-	1.471	-	2.611
NTS-KEM SSE	1.337	-	2.413	-	4.707
Round5 Ring	0.066	-	0.256	-	0.321
Round5 Ring 5	0.088	-	0.168	-	0.290
Round5 Non-Ring	0.378	-	0.515	-	1.969
Round 5 LongKey	0.061	-	-	-	-
SABER	0.092	-	0.156	-	0.249
SIKE	15.823	22.772	40.642	-	65.121
SIKE Compressed	27.293	37.180	66.586	-	104.814
Three Bears	-	0.192	-	0.316	0.461
Three Bears Eph.	-	0.051	-	0.070	0.076

Table 16: Energy consumption of `crypto_kem_dec` function for **Decapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
BIKE1	0.457	-	1.152	-	2.660
BIKE2	0.254	-	0.726	-	1.489
BIKE3	0.354	-	0.887	-	2.099
Classic McEliece AVX	0.190	-	0.179	-	0.264
Classic McEliece SSE	0.160	-	0.201	-	0.162
CRYSTALS-Kyber	0.047	-	0.081	-	0.135
CRYSTALS-Kyber-90s	0.014	-	0.028	-	0.043
FRODO AES	1.763	-	3.086	-	4.975
FRODO SHAKE	6.515	-	13.629	-	24.725
hqc-1	1.310	-	2.018	-	3.012
hqc-2	-	-	2.189	-	3.195
hqc-3	-	-	-	-	3.310
LAC	0.103	-	0.263	-	0.320
LEDAcrypt N02	1.254	-	3.137	-	5.973
LEDAcrypt N03	1.596	-	3.764	-	7.140
LEDAcrypt N04	4.203	-	9.427	-	15.056
LEDAcrypt DFR64	1.598	-	3.655	-	6.450
LEDAcrypt DFRSL	2.265	-	5.064	-	9.380
NewHope CCA	0.146	-	-	-	0.253
NewHope CPA	0.022	-	-	-	0.034
NTRU-HRSS	-	-	0.053	-	-
NTS-KEM AVX	0.805	-	1.471	-	2.611
NTS-KEM SSE	1.337	-	2.413	-	4.707
Round5 Ring	0.066	-	0.256	-	0.321
Round5 Ring 5	0.088	-	0.168	-	0.290
Round5 Non-Ring	0.378	-	0.515	-	1.969
Round 5 LongKey	0.061	-	-	-	-
SABER	0.092	-	0.156	-	0.249
SIKE	15.823	22.772	40.642	-	65.121
SIKE Compressed	27.293	37.180	66.586	-	104.814
Three Bears	-	0.192	-	0.316	0.461
Three Bears Eph.	-	0.051	-	0.070	0.076

Table 16: Energy consumption of **`crypto_kem_dec`** function for **Decapsulation** of Round 2 **Key Encapsulation Mechanisms**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Key Decapsulation

- Best Lattice-Based: **CRYSTALS-Kyber 90s &NewHope CPA**
  - *L1: 0.014mJ* L1: 0.022mJ
  - *L3: 0.028mJ* L3: N/A
  - L5: 0.043mJ *L5: 0.034mJ*

- Best Code-Based: **Classic McEliece AVX & SSE**
  - L1: 0.190mJ *L1: 0.160mJ*
  - *L3: 0.179mJ* L3: 0.201mJ
  - L5: 0.264mJ *L5: 0.162mJ*

- Best Other: **SIKE**
  - L1: 15.823mJ
  - L3: 40.642mJ
  - L5: 65.121mJ

Results for Assembly Optimized Implementation

Public-Key Encryption Schemes

Table 17: Energy consumption of `crypto_encrypt_keypair` function for **Keypair Generation** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	1420.300	4751.320	14271.160
LEDAcrypt DFRSL	1961.020	7322.090	21125.400
LAC	0.098	0.311	0.268

Table 18: Energy consumption of `crypto_encrypt` function for **Encryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	1.410	2.520	4.540
LEDAcrypt DFRSL	1.930	4.600	7.280
LAC	0.176	0.296	0.482

Table 19: Energy consumption of `crypto_encrypt_open` function for **Decryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	3.550	6.660	11.740
LEDAcrypt DFRSL	4.890	10.040	18.000
LAC	0.080	0.183	0.208

Table 17: Energy consumption of `crypto_encrypt_keypair` function for **Keypair Generation** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	1420.300	4751.320	14271.160
LEDAcrypt DFRSL	1961.020	7322.090	21125.400
LAC	0.098	0.311	0.268

Table 18: Energy consumption of `crypto_encrypt` function for **Encryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	1.410	2.520	4.540
LEDAcrypt DFRSL	1.930	4.600	7.280
LAC	0.176	0.296	0.482

🟥	Highest energy per level
🟩	Lowest energy per level

Table 19: Energy consumption of `crypto_encrypt_open` function for **Decryption** of Round 2 **Public-key Encryption** schemes. Energy is in milliJoules.

	Level 1	Level 3	Level 5
LEDAcrypt DFR64	3.550	6.660	11.740
LEDAcrypt DFRSL	4.890	10.040	18.000
LAC	0.080	0.183	0.208

Results for Assembly Optimized Implementation

Digital Signature Schemes

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.118	0.167	0.255	0.369	-
CRYSTALS-Dilithium AES	0.100	0.115	0.168	0.233	-
GeMSS	65.017	-	329.908	-	1017.190
BlueGeMSS	65.691	-	327.297	-	997.568
RedGeMSS	76.858	-	339.969	-	1009.862
Luov Small Sig Chacha	-	2.790	-	12.941	21.611
Luov Small Sig Keccak	-	5.171	-	17.652	29.943
MQDSS	-	1.096	-	2.582	-
Picnic UR	0.049	-	0.061	-	0.068
Picnic FS	0.026	-	0.058	-	0.079
Picnic2 FS	0.052	-	0.066	-	0.074
qTESLA	1.464	-	4.376	-	21.869
qTESLA-s	1.524	-	4.124	-	21.532
Rainbow Classic	13.084	-	121.867	-	184.880
Rainbow Compressed/Cyclic	14.087	-	136.343	-	200.194
Rainbow Cyclic	14.176	-	138.416	-	198.908
Rainbow SSE Classic	14.066	-	123.136	-	202.550
Rainbow SSE Compressed/Cyclic	14.680	-	141.406	-	223.691
Rainbow SSE Cyclic	14.904	-	143.365	-	221.944
SPHINCS+ SHA256 s simple	615.820	-	86.960	-	111.380
SPHINCS+ SHA256 s robust	1125.340	-	1650.120	-	445.310
SPHINCS+ SHA256 f simple	19.760	-	29.080	-	7.090
SPHINCS+ SHA256 f robust	39.150	-	54.190	-	28.730
SPHINCS+ SHAKE256 s simple	188.190	-	270.230	-	373.390
SPHINCS+ SHAKE256 s robust	362.230	-	522.330	-	691.150
SPHINCS+ SHAKE256 f simple	6.070	-	9.040	-	23.140
SPHINCS+ SHAKE256 f robust	11.610	-	16.160	-	43.230
SPHINCS+ HARAKA s simple	157.070	263.720	-	-	-
SPHINCS+ HARAKA s robust	252.400	364.310	-	-	-
SPHINCS+ HARAKA f simple	7.010	10.010	-	-	-
SPHINCS+ HARAKA f robust	10.760	13.310	-	-	-

Table 20: Energy consumption of `crypto_sign_keypair` function for **Keypair Generation** of Round 2 **Digital Signatures**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.118	0.167	0.255	0.369	-
CRYSTALS-Dilithium AES	0.100	0.115	0.168	0.233	-
GeMSS	65.017	-	329.908	-	1017.190
BlueGeMSS	65.691	-	327.297	-	997.568
RedGeMSS	76.858	-	339.969	-	1009.862
Luov Small Sig Chacha	-	2.790	-	12.941	21.611
Luov Small Sig Keccak	-	5.171	-	17.652	29.943
MQDSS	-	1.096	-	2.582	-
Picnic UR	0.049	-	0.061	-	0.068
Picnic FS	0.026	-	0.058	-	0.079
Picnic2 FS	0.052	-	0.066	-	0.074
qTESLA	1.464	-	4.376	-	21.869
qTESLA-s	1.524	-	4.124	-	21.532
Rainbow Classic	13.084	-	121.867	-	184.880
Rainbow Compressed/Cyclic	14.087	-	136.343	-	200.194
Rainbow Cyclic	14.176	-	138.416	-	198.908
Rainbow SSE Classic	14.066	-	123.136	-	202.550
Rainbow SSE Compressed/Cyclic	14.680	-	141.406	-	223.691
Rainbow SSE Cyclic	14.904	-	143.365	-	221.944
SPHINCS+ SHA256 s simple	615.820	-	86.960	-	111.380
SPHINCS+ SHA256 s robust	1125.340	-	1650.120	-	445.310
SPHINCS+ SHA256 f simple	19.760	-	29.080	-	7.090
SPHINCS+ SHA256 f robust	39.150	-	54.190	-	28.730
SPHINCS+ SHAKE256 s simple	188.190	-	270.230	-	373.390
SPHINCS+ SHAKE256 s robust	362.230	-	522.330	-	691.150
SPHINCS+ SHAKE256 f simple	6.070	-	9.040	-	23.140
SPHINCS+ SHAKE256 f robust	11.610	-	16.160	-	43.230
SPHINCS+ HARAKA s simple	157.070	263.720	-	-	-
SPHINCS+ HARAKA s robust	252.400	364.310	-	-	-
SPHINCS+ HARAKA f simple	7.010	10.010	-	-	-
SPHINCS+ HARAKA f robust	10.760	13.310	-	-	-

Table 20: Energy consumption of `crypto_sign_keypair` function for **Keypair Generation** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

UNIVERSITY OF WATERLOO

Comparison of Results: Keypair Generation

- Best Lattice-Based: **CRYSTALS-Dilithium AES & qTESLA-s**
  - *L1: 0.100mJ* L1: 1.524mJ
  - *L3: 0.168mJ* L3: 4.124mJ
  - L5: N/A *L5: 21.532mJ*

- Best Multivariate-Based: **MQDSS & LUOV S. Signature ChaCha**
  - *L1: 1.096mJ* L1: 2.790mJ
  - *L3: 2.582mJ* L3: 12.941mJ
  - L5: N/A *L5: 21.611mJ*

- Best Other: **Picnic FS & Picnic UR**
  - *L1: 0.026mJ* L1: 0.049mJ
  - *L3: 0.058mJ* L3: 0.061mJ
  - L5: 0.079mJ *L5: 0.068mJ*

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.392	0.611	0.687	0.729	-
CRYSTALS-Dilithium AES	0.244	0.443	0.588	0.605	-
GeMSS	1244.551	-	3391.091	-	5751.300
BlueGeMSS	196.217	-	502.963	-	791.175
RedGeMSS	7.240	-	18.016	-	27.660
Luov Small Sig Chacha	-	1.258	-	3.238	5.370
Luov Small Sig Keccak	-	3.619	-	8.182	13.645
MQDSS	-	4.543	-	11.769	-
Picnic UR	19.670	-	48.329	-	79.814
Picnic FS	14.801	-	35.907	-	60.796
Picnic2 FS	486.873	-	1388.546	-	2764.521
qTESLA	0.388	-	0.478	-	1.038
qTESLA-s	0.414	-	0.482	-	1.099
Rainbow Classic	0.087	-	0.781	-	1.052
Rainbow Compressed/Cyclic	9.404	-	85.453	-	134.780
Rainbow Cyclic	0.107	-	0.800	-	1.032
Rainbow SSE Classic	0.208	-	0.824	-	1.191
Rainbow SSE Compressed/Cyclic	9.602	-	87.802	-	144.781
Rainbow SSE Cyclic	0.204	-	0.822	-	1.177
SPHINCS+ SHA256 s simple	10883.230	-	2310.780	-	1460.860
SPHINCS+ SHA256 s robust	21286.640	-	40865.710	-	5457.770
SPHINCS+ SHA256 f simple	649.140	-	872.450	-	175.980
SPHINCS+ SHA256 f robust	1269.120	-	1714.890	-	673.160
SPHINCS+ SHAKE256 s simple	3043.750	-	6489.690	-	4596.470
SPHINCS+ SHAKE256 s robust	5473.480	-	11314.230	-	8200.250
SPHINCS+ SHAKE256 f simple	193.970	-	257.790	-	551.490
SPHINCS+ SHAKE256 f robust	351.300	-	475.700	-	1004.150
SPHINCS+ HARAKA s simple	3474.440	7529.410	-	-	-
SPHINCS+ HARAKA s robust	4673.460	11891.060	-	-	-
SPHINCS+ HARAKA f simple	152.790	231.180	-	-	-
SPHINCS+ HARAKA f robust	260.930	329.050	-	-	-

Table 21: Energy consumption of **`crypto_sign`** function for **Signing** of Round 2 **Digital Signatures**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.392	0.611	0.687	0.729	-
CRYSTALS-Dilithium AES	0.244	0.443	0.588	0.605	-
GeMSS	1244.551	-	3391.091	-	5751.300
BlueGeMSS	196.217	-	502.963	-	791.175
RedGeMSS	7.240	-	18.016	-	27.660
Luov Small Sig Chacha	-	1.258	-	3.238	5.370
Luov Small Sig Keccak	-	3.619	-	8.182	13.645
MQDSS	-	4.543	-	11.769	-
Picnic UR	19.670	-	48.329	-	79.814
Picnic FS	14.801	-	35.907	-	60.796
Picnic2 FS	486.873	-	1388.546	-	2764.521
qTESLA	0.388	-	0.478	-	1.038
qTESLA-s	0.414	-	0.482	-	1.099
Rainbow Classic	0.087	-	0.781	-	1.052
Rainbow Compressed/Cyclic	9.404	-	85.453	-	134.780
Rainbow Cyclic	0.107	-	0.800	-	1.032
Rainbow SSE Classic	0.208	-	0.824	-	1.191
Rainbow SSE Compressed/Cyclic	9.602	-	87.802	-	144.781
Rainbow SSE Cyclic	0.204	-	0.822	-	1.177
SPHINCS+ SHA256 s simple	10883.230	-	2310.780	-	1460.860
SPHINCS+ SHA256 s robust	21286.640	-	40865.710	-	5457.770
SPHINCS+ SHA256 f simple	649.140	-	872.450	-	175.980
SPHINCS+ SHA256 f robust	1269.120	-	1714.890	-	673.160
SPHINCS+ SHAKE256 s simple	3043.750	-	6489.690	-	4596.470
SPHINCS+ SHAKE256 s robust	5473.480	-	11314.230	-	8200.250
SPHINCS+ SHAKE256 f simple	193.970	-	257.790	-	551.490
SPHINCS+ SHAKE256 f robust	351.300	-	475.700	-	1004.150
SPHINCS+ HARAKA s simple	3474.440	7529.410	-	-	-
SPHINCS+ HARAKA s robust	4673.460	11891.060	-	-	-
SPHINCS+ HARAKA f simple	152.790	231.180	-	-	-
SPHINCS+ HARAKA f robust	260.930	329.050	-	-	-

Table 21: Energy consumption of `crypto_sign` function for **Signing** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Signing

- Best Lattice-Based: **CRYSTALS-Dilithium AES & qTESLA**
  - *L1: 0.244mJ* L1: 0.388mJ
  - L3: 0.588mJ *L3: 0.478mJ*
  - L5: N/A *L5: 1.038mJ*

- Best Multivariate-Based: **Rainbow Classic & Cyclic**
  - *L1: 0.087mJ* L1: 0.107mJ
  - *L3: 0.781mJ* L3: 0.800mJ
  - L5: 1.052mJ *L5: 1.032mJ*

- Best Other: **Picnic FS**
  - L1: 14.801mJ
  - L3: 35.907mJ
  - L5: 60.796mJ

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.169	0.222	0.294	0.372	-
CRYSTALS-Dilithium AES	0.137	0.167	0.184	0.254	-
GeMSS	0.331	-	0.719	-	2.080
BlueGeMSS	0.321	-	0.758	-	1.575
RedGeMSS	0.585	-	1.241	-	2.410
Luov Small Sig Chacha	-	0.333	-	1.156	1.501
Luov Small Sig Keccak	-	2.697	-	6.070	9.731
MQDSS	-	3.096	-	8.084	-
Picnic UR	15.763	-	39.132	-	65.796
Picnic FS	11.962	-	29.856	-	51.307
Picnic2 FS	261.616	-	603.427	-	1060.452
qTESLA	0.145	-	0.266	-	0.401
qTESLA-s	0.130	-	0.228	-	0.419
Rainbow Classic	0.031	-	0.161	-	0.274
Rainbow Compressed/Cyclic	5.539	-	29.937	-	72.646
Rainbow Cyclic	5.449	-	30.165	-	73.366
Rainbow SSE Classic	0.099	-	0.890	-	0.796
Rainbow SSE Compressed/Cyclic	5.484	-	30.973	-	73.050
Rainbow SSE Cyclic	5.607	-	31.252	-	73.067
SPHINCS+ SHA256 s simple	29.760	-	4.630	-	6.030
SPHINCS+ SHA256 s robust	60.540	-	95.520	-	18.150
SPHINCS+ SHA256 f simple	69.880	-	114.380	-	12.280
SPHINCS+ SHA256 f robust	146.300	-	238.020	-	35.630
SPHINCS+ SHAKE256 s simple	5.190	-	7.490	-	10.000
SPHINCS+ SHAKE256 s robust	9.890	-	14.070	-	19.020
SPHINCS+ SHAKE256 f simple	11.830	-	18.970	-	20.010
SPHINCS+ SHAKE256 f robust	22.480	-	36.420	-	38.920
SPHINCS+ HARAKA s simple	4.130	5.390	-	-	-
SPHINCS+ HARAKA s robust	7.200	11.910	-	-	-
SPHINCS+ HARAKA f simple	8.710	13.440	-	-	-
SPHINCS+ HARAKA f robust	16.340	28.980	-	-	-

Table 22: Energy consumption of `crypto_sign_open` function for **Verification** of Round 2 **Digital Signatures**. Energy is in milliJoules.

Security Level Scheme	Level 1	Level 2	Level 3	Level 4	Level 5
CRYSTALS-Dilithium SHAKE	0.169	0.222	0.294	0.372	-
CRYSTALS-Dilithium AES	0.137	0.167	0.184	0.254	-
GeMSS	0.331	-	0.719	-	2.080
BlueGeMSS	0.321	-	0.758	-	1.575
RedGeMSS	0.585	-	1.241	-	2.410
Luov Small Sig Chacha	-	0.333	-	1.156	1.501
Luov Small Sig Keccak	-	2.697	-	6.070	9.731
MQDSS	-	3.096	-	8.084	-
Picnic UR	15.763	-	39.132	-	65.796
Picnic FS	11.962	-	29.856	-	51.307
Picnic2 FS	261.616	-	603.427	-	1060.452
qTESLA	0.145	-	0.266	-	0.401
qTESLA-s	0.130	-	0.228	-	0.419
Rainbow Classic	0.031	-	0.161	-	0.274
Rainbow Compressed/Cyclic	5.539	-	29.937	-	72.646
Rainbow Cyclic	5.449	-	30.165	-	73.366
Rainbow SSE Classic	0.099	-	0.890	-	0.796
Rainbow SSE Compressed/Cyclic	5.484	-	30.973	-	73.050
Rainbow SSE Cyclic	5.607	-	31.252	-	73.067
SPHINCS+ SHA256 s simple	29.760	-	4.630	-	6.030
SPHINCS+ SHA256 s robust	60.540	-	95.520	-	18.150
SPHINCS+ SHA256 f simple	69.880	-	114.380	-	12.280
SPHINCS+ SHA256 f robust	146.300	-	238.020	-	35.630
SPHINCS+ SHAKE256 s simple	5.190	-	7.490	-	10.000
SPHINCS+ SHAKE256 s robust	9.890	-	14.070	-	19.020
SPHINCS+ SHAKE256 f simple	11.830	-	18.970	-	20.010
SPHINCS+ SHAKE256 f robust	22.480	-	36.420	-	38.920
SPHINCS+ HARAKA s simple	4.130	5.390	-	-	-
SPHINCS+ HARAKA s robust	7.200	11.910	-	-	-
SPHINCS+ HARAKA f simple	8.710	13.440	-	-	-
SPHINCS+ HARAKA f robust	16.340	28.980	-	-	-

Table 22: Energy consumption of `crypto_sign_open` function for **Verification** of Round 2 **Digital Signatures**. Energy is in milliJoules.

🟥	Highest energy per level
🟩	Lowest energy per level

Comparison of Results: Verification

- Best Lattice-Based: **qTESLA, qTESLA-s & CRYSTALS-Dilithium AES**

L1: 0.130mJ	L1: 0.145mJ	L1: 0.137mJ
L3: 0.228mJ	L3: 0.266mJ	*L3: 0.184mJ*
L5: 0.419mJ	*L5: 0.401mJ*	L5: N/A

- Best Multivariate-Based: **Rainbow Classic**
  - L1: 0.031mJ
  - L3: 0.161mJ
  - L5: 0.274mJ

- Best Other: **SHINCS+ HARAKA s simple & SHA256 s simple**

L1: 4.130mJ	L1: 29.760mJ
L3: N/A	*L3: 4.630mJ*
L5: N/A	*L5: 6.030mJ*

UNIVERSITY OF WATERLOO

Discussion of Results

- Using the energy consumption results shown in the previous section, the candidate submissions are ranked
- In this ranking, we do not consider the different variants of each algorithm, but rather the best energy consuming variant in each submission package to best compare each proposed algorithm against each other
- To provide a comprehensive comparison, the results from levels 2 and 4 are consolidated into the results from 1 and 3, respectively
- For rankings of Assembly Optimized Implementation, a reference to its rank in the Optimized C Implementation is provided for ease of comparison

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Round5	Round5	Round5
2	Three Bears	Three Bears	Three Bears
3	LAC	SABER	LAC
4	SABER	LAC	SABER
5	BIKE	ROLLO	ROLLO
Rank	**Encapsulation**		
1	NTS-KEM	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	Round5	Classic McEliece	LAC
4	LAC	LAC	NTS-KEM
5	Classic McEliece	NTS-KEM	Classic McEliece
Rank	**Decapsulation**		
1	Round5	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	NewHope	LAC	NewHope
4	LAC	CRYSTALS-KYBER	LAC
5	NTS-KEM	NTS-KEM	CRYSTALS-Kyber

Table 23: The top five most energy efficient submissions for functions pertaining to **Key Encapsulation Mechanisms**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Round5	Round5	Round5
2	Three Bears	Three Bears	Three Bears
3	LAC	SABER	LAC
4	SABER	LAC	SABER
5	BIKE	ROLLO	ROLLO
Rank	**Encapsulation**		
1	NTS-KEM	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	Round5	Classic McEliece	LAC
4	LAC	LAC	NTS-KEM
5	Classic McEliece	NTS-KEM	Classic McEliece
Rank	**Decapsulation**		
1	Round5	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	NewHope	LAC	NewHope
4	LAC	CRYSTALS-KYBER	LAC
5	NTS-KEM	NTS-KEM	CRYSTALS-Kyber

Table 23: The top five most energy efficient submissions for functions pertaining to **Key Encapsulation Mechanisms**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

🟥	Lattice-based
🟨	Code-based
🟦	Other

UNIVERSITY OF WATERLOO

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	CRYSTALS-Kyber (7)	CRYSTALS-Kyber (6)	CRYSTALS-Kyber (7)
2	LAC (3)	LAC (4)	LAC (3)
3	SABER (4)	SABER (3)	NewHope (6)
4	NewHope (8)	Three Bears (2)	SABER (4)
5	Round5 (1)	Round5 (1)	Three Bears (2)
Rank	**Encapsulation**		
1	CRYSTALS-Kyber (8)	CRYSTALS-Kyber (8)	CRYSTALS-Kyber (9)
2	Classic McEliece (5)	Classic McEliece (3)	Classic McEliece (5)
3	LAC (4)	NTRU (12)	NewHope (8)
4	NewHope (9)	LAC (4)	SABER (11)
5	SABER (14)	SABER (10)	LAC (3)
Rank	**Decapsulation**		
1	CRYSTALS-Kyber (4)	CRYSTALS-Kyber (4)	NewHope (3)
2	NewHope (3)	NTRU (11)	CRYSTALS-Kyber (5)
3	Three Bears (2)	Three Bears (1)	Three Bears (1)
4	Round5 (1)	SABER (8)	Classic McEliece (14)
5	LAC (4)	Round5 (2)	SABER (9)

Table 24: The top five most energy efficient submissions for functions pertaining to **Key Encapsulation Mechanisms**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

UNIVERSITY OF WATERLOO

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	CRYSTALS-Kyber (7)	CRYSTALS-Kyber (6)	CRYSTALS-Kyber (7)
2	LAC (3)	LAC (4)	LAC (3)
3	SABER (4)	SABER (3)	NewHope (6)
4	NewHope (8)	Three Bears (2)	SABER (4)
5	Round5 (1)	Round5 (1)	Three Bears (2)
Rank	**Encapsulation**		
1	CRYSTALS-Kyber (8)	CRYSTALS-Kyber (8)	CRYSTALS-Kyber (9)
2	Classic McEliece (5)	Classic McEliece (3)	Classic McEliece (5)
3	LAC (4)	NTRU (12)	NewHope (8)
4	NewHope (9)	LAC (4)	SABER (11)
5	SABER (14)	SABER (10)	LAC (3)
Rank	**Decapsulation**		
1	CRYSTALS-Kyber (4)	CRYSTALS-Kyber (4)	NewHope (3)
2	NewHope (3)	NTRU (11)	CRYSTALS-Kyber (5)
3	Three Bears (2)	Three Bears (1)	Three Bears (1)
4	Round5 (1)	SABER (8)	Classic McEliece (14)
5	LAC (4)	Round5 (2)	SABER (9)

Table 24: The top five most energy efficient submissions for functions pertaining to **Key Encapsulation Mechanisms**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

🟥 Lattice-based

🟨 Code-based

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	Total		
1	Round5	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	LAC	LAC	LAC
4	NewHope	CRYSTALS-Kyber	ROLLO
5	CRYSTALS-Kyber	ROLLO	NewHope

Table 25: The top five most energy efficient submissions for **total** energy consumed of **Key Encapsulation Mechanisms**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Total**		
1	Round5	Three Bears	Three Bears
2	Three Bears	Round5	Round5
3	LAC	LAC	LAC
4	NewHope	CRYSTALS-Kyber	ROLLO
5	CRYSTALS-Kyber	ROLLO	NewHope

Table 25: The top five most energy efficient submissions for **total** energy consumed of **Key Encapsulation Mechanisms**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

🟥 Lattice-based

🟦 Other

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	Total		
1	CRYSTALS-Kyber (5)	CRYSTALS-Kyber (4)	CRYSTALS-Kyber (5)
2	NewHope (4)	SABER (6)	NewHope (4)
3	LAC (3)	Three Bears (1)	SABER (7)
4	SABER (8)	NTRU (14)	LAC (3)
5	Three Bears (2)	LAC (3)	Three Bears (1)

Table 26: The top five most energy efficient submissions for **total** energy consumed of **Key Encapsulation Mechanisms**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

Analysis of Key Encapsulation Mechanisms

	Level 1	Level 3	Level 5
Rank	**Total**		
1	CRYSTALS-Kyber (5)	CRYSTALS-Kyber (4)	CRYSTALS-Kyber (5)
2	NewHope (4)	SABER (6)	NewHope (4)
3	LAC (3)	Three Bears (1)	SABER (7)
4	SABER (8)	NTRU (14)	LAC (3)
5	Three Bears (2)	LAC (3)	Three Bears (1)

Table 26: The top five most energy efficient submissions for **total** energy consumed of **Key Encapsulation Mechanisms**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

🟥 Lattice-based

Analysis of Key Encapsulation Mechanisms

- The average power across all security levels taken with regard to each of the three functions ranges from 24.89-25.73W for Optimized C Implementations whereas it is only 4.58-4.73W for Assembly Optimized Implementations

- Most efficient algorithms are lattice-based; this is even more prominent in the Assembly Optimized Implementations, a testament to lattice-based cryptosystems’ high parallelizability

Analysis of Key Encapsulation Mechanisms

- The average power across all security levels taken with regard to each of the three functions ranges from 24.89-25.73W for Optimized C Implementations whereas it is only 4.58-4.73W for Assembly Optimized Implementations

- Most efficient algorithms are lattice-based; this is even more prominent in the Assembly Optimized Implementations, a testament to lattice-based cryptosystems' high parallelizability

- Code-based algorithms are competitive with lattice-based implementations for key encapsulation, but their total energy is dominated by the energy required to perform key generation

- Big leap in energy efficiency when hardware-accelerated symmetric primitives are used; candidate submissions can be drastically improved when hardware support for symmetric primitives become available

Analysis of Digital Signatures

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Picnic	Picnic	Picnic
2	CRYSTALS-Dilithium	CRYSTALS-Dilithium	qTESLA
3	qTESLA	qTESLA	SPHINCS+
4	MQDSS	MQDSS	Luov
5	SPHINCS+	SPHINCS+	Falcon
Rank	**Signing**		
1	Rainbow	CRYSTALS-Dilithium	Falcon
2	qTESLA	qTESLA	qTESLA
3	Falcon	Rainbow	Rainbow
4	CRYSTALS-Dilithium	Luov	Luov
5	Luov	GeMSS	Picnic
Rank	**Verification**		
1	qTESLA	qTESLA	Falcon
2	Falcon	CRYSTALS-Dilithium	qTESLA
3	GeMSS	GeMSS	GeMSS
4	Rainbow	Rainbow	Rainbow
5	CRYSTALS-Dilithium	SPHINCS+	SPHINCS+

Table 27: The top five most energy efficient submissions for functions pertaining to **Digital Signatures**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

UNIVERSITY OF WATERLOO

Analysis of Digital Signatures

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Picnic	Picnic	Picnic
2	CRYSTALS-Dilithium	CRYSTALS-Dilithium	qTESLA
3	qTESLA	qTESLA	SPHINCS+
4	MQDSS	MQDSS	Luov
5	SPHINCS+	SPHINCS+	Falcon
Rank	**Signing**		
1	Rainbow	CRYSTALS-Dilithium	Falcon
2	qTESLA	qTESLA	qTESLA
3	Falcon	Rainbow	Rainbow
4	CRYSTALS-Dilithium	Luov	Luov
5	Luov	GeMSS	Picnic
Rank	**Verification**		
1	qTESLA	qTESLA	Falcon
2	Falcon	CRYSTALS-Dilithium	qTESLA
3	GeMSS	GeMSS	GeMSS
4	Rainbow	Rainbow	Rainbow
5	CRYSTALS-Dilithium	SPHINCS+	SPHINCS+

Table 27: The top five most energy efficient submissions for functions pertaining to **Digital Signatures**. Results are from **Optimized C Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3.

🟥 Lattice-based

🟩 Multivariate-based

🟦 Other

Analysis of Digital Signatures

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Picnic (1)	Picnic (1)	Picnic (1)
2	CRYSTALS-Dilithium (2)	CRYSTALS-Dilithium (2)	SPHINCS+ (3)
3	MQDSS (4)	MQDSS (4)	qTESLA (2)
4	qTESLA (3)	qTESLA (3)	Luov (4)
5	Luov (6)	SPHINCS+ (5)	Rainbow (6)
Rank	**Signing**		
1	Rainbow (1)	qTESLA (2)	Rainbow (3)
2	CRYSTALS-Dilithium (4)	CRYSTALS-Dilithium (1)	qTESLA (2)
3	qTESLA (2)	Rainbow (4)	Luov (4)
4	Luov (6)	Luov (4)	GeMSS (6)
5	MQDSS (9)	MQDSS (8)	Picnic (5)
Rank	**Verification**		
1	Rainbow (4)	Rainbow (4)	Rainbow (4)
2	qTESLA (1)	CRYSTALS-Dilithium (2)	qTESLA (2)
3	CRYSTALS-Dilithium (5)	qTESLA (1)	Luov (6)
4	GeMSS (3)	GeMSS (3)	GeMSS (3)
5	Luov (7)	Luov (6)	SPHINCS+ (5)

Table 28: The top five most energy efficient submissions for functions pertaining to **Digital Signatures**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

UNIVERSITY OF WATERLOO

Analysis of Digital Signatures

	Level 1	Level 3	Level 5
Rank	**Keypair Generation**		
1	Picnic (1)	Picnic (1)	Picnic (1)
2	CRYSTALS-Dilithium (2)	CRYSTALS-Dilithium (2)	SPHINCS+ (3)
3	MQDSS (4)	MQDSS (4)	qTESLA (2)
4	qTESLA (3)	qTESLA (3)	Luov (4)
5	Luov (6)	SPHINCS+ (5)	Rainbow (6)
Rank	**Signing**		
1	Rainbow (1)	qTESLA (2)	Rainbow (3)
2	CRYSTALS-Dilithium (4)	CRYSTALS-Dilithium (1)	qTESLA (2)
3	qTESLA (2)	Rainbow (4)	Luov (4)
4	Luov (6)	Luov (4)	GeMSS (6)
5	MQDSS (9)	MQDSS (8)	Picnic (5)
Rank	**Verification**		
1	Rainbow (4)	Rainbow (4)	Rainbow (4)
2	qTESLA (1)	CRYSTALS-Dilithium (2)	qTESLA (2)
3	CRYSTALS-Dilithium (5)	qTESLA (1)	Luov (6)
4	GeMSS (3)	GeMSS (3)	GeMSS (3)
5	Luov (7)	Luov (6)	SPHINCS+ (5)

Table 28: The top five most energy efficient submissions for functions pertaining to **Digital Signatures**. Results are from **Assembly Optimized Implementations.** Schemes targeting Level 2 and 4 are included in Level 1 and 3. Brackets indicate rank in portable C implementation.

🟥 Lattice-based

🟩 Multivariate-based

🟦 Other

UNIVERSITY OF WATERLOO

Analysis of Digital Signatures

- The average power across all security levels ranges from 25.60-26.65W for Optimized C Implementations whereas it is only 4.75-5.03W for Assembly Optimized Implementations

- Except for Rainbow, all submissions are more energy-efficient when performing signature verification than signature generation

Analysis of Digital Signatures

- The average power across all security levels ranges from 25.60-26.65W for Optimized C Implementations whereas it is only 4.75-5.03W for Assembly Optimized Implementations

- Except for Rainbow, all submissions are more energy-efficient when performing signature verification than signature generation

- When considering the Optimized C Implementation, lattice-based techniques like CRYSTALs-Dilithium, qTESLA, and Falcon are among the most energy-efficient for both signing and verification procedures.

- Multivariate-based scheme GeMSS and its BlueGeMSS variant perform comparatively to their closest ranked lattice-based scheme, having only between 12-64% difference in energy consumption across the different security levels studied

Analysis of Digital Signatures

- The assembly optimizations applied have not shifted the rankings drastically compared to their portable C counterparts
- Multivariate-based scheme tops the rankings for both signing and verification when considering the Assembly Optimized Implementation

Summary and Future Work

- In this work, we measured the energy of the PQC Round 2 candidates, including the required portable C implementation as well as assembly optimized implementations
- Results were categorized by cryptographic function and proposed security level

Summary and Future Work

- In this work, we measured the energy of the PQC Round 2 candidates, including the required portable C implementation as well as assembly optimized implementations

- Results were categorized by cryptographic function and proposed security level

- Candidates were ranked based on their energy consumption to demonstrate which schemes are most energy efficient

- Lattice-based schemes tend to be very efficient in practice and are highly parallelizable; this is reflected in our results, especially when considering implementations with assembly optimizations

Summary and Future Work

- We do not provide a total energy consumption metric for Digital Signatures due to the nature of their use

- Optimization efforts will shift based on the application for which the digital signature scheme is deployed

Summary and Future Work

- We do not provide a total energy consumption metric for Digital Signatures due to the nature of their use
- Optimization efforts will shift based on the application for which the digital signature scheme is deployed
- Efficient signing is generally preferred in settings where resource-constrained devices must have a means to transmit authentic data measurements to a base station
- Applications like public-key certification where a single message is signed once and verified by the masses ideally have an efficient verification procedure

Summary and Future Work

- Of the top five most energy efficient schemes, the energy consumed is mostly attributed to hashing subroutines (ex. Keccak Permutation associated functions), modular reduction routines (ex. Barrett and Montgomery reduction), and multiplication (polynomial, vector multiplication, ring multiplication, etc.)

Summary and Future Work

- Of the top five most energy efficient schemes, the energy consumed is mostly attributed to hashing subroutines (ex. Keccak Permutation associated functions), modular reduction routines (ex. Barrett and Montgomery reduction), and multiplication (polynomial, vector multiplication, ring multiplication, etc.)

- Our ranking only provides one metric of evaluation; a holistic approach should be used when determining which algorithm best suites one's application

- We hope to use our findings in the future to pinpoint which subroutines of the candidate submissions expend the most energy to provide direction for further optimizations

» Full technical report can be found at
http://cacr.uwaterloo.ca/techreports/2019/cacr2019-03.pdf

Acknowledgements

This research was supported in part through a grant provided by the Natural Sciences and Engineering Research Council of Canada. The authors would also like to thank Tanushree Banerjee for her guidance and support in the preliminary stages of this project.