Comparison:
LEDA, BIKE, QC-MDPC, HQC

Carl A. Miller
NIST Computer Security Division
October 19, 2018

NIST PQC Seminar (not for public distribution)

The Basics

- Each one is a code-based scheme for either encryption or key encapsulation.
- Each one takes advantage of low-weight (i.e., sparse) binary vectors or matrices.

Code-based encryption

Suppose Bob creates a generator matrix G for a binary code that he knows how to decode.

He then obfuscates it by multiplying it by a random invertible matrix U, and gives the result to Alice.

G, U

(UG)

Code-based encryption

In these protocols, we assume that all matrices are **quasi-cyclic**. (This allows smaller key size.)

$$\left[\begin{array}{ccccc|ccccc} a_1 & a_2 & a_3 & \cdots & a_n & b_1 & b_2 & b_3 & \cdots & b_n \\ a_2 & a_3 & a_4 & \cdots & a_1 & b_2 & b_3 & b_4 & \cdots & b_1 \\ a_3 & a_4 & a_5 & \cdots & a_2 & b_3 & b_4 & b_5 & \cdots & b_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_2 & a_3 & \cdots & a_{n-1} & b_n & b_1 & b_2 & \cdots & b_{n-1} \end{array}\right]$$

G, U

(UG)

BIKE-1

Alice chooses a random vector e (low-weight) and m (uniform), and sends m(UG) + e.

Bob recovers e and uses it to compute the shared key.

Here, G is taken to be a random low-density (quasi-cyclic) matrix.

BIKE-3, another KEM, is pretty similar.

G, U

(UG)

m(UG) + e

e

BIKE-2

Bob chooses a low-density parity check matrix H and an invertible matrix V.

(Here V is chosen so that the first block of HV is the identity.)

The key is encapsulated by Alice encoding a random low-weight vector e.

H, V

e(HV)

(HV)

e

QC-MDPC

Like BIKE-1, except:

* ~~G is instead a random **moderate-density parity check** code.~~

  (Ignore the above sentence.)

* The information is contained in m (rather than e).

G, U

m(UG) + e

(UG)

e

LEDApkc

The authors first describes an IND-CPA encryption algorithm, roughly the same as QC-MDPC.

Then they describe a more complex algorithm that is claimed to be IND-CCA2.

G, U

(UG)

m(UG) + e

HQC

A complex algorithm, also claimed to be IND-CCA2 secure.

Here the generator matrix G is fixed, but the message is disguised using additional random matrices x, y, h, e, r_1, r_2. (All are all low-weight except h.)

x, y, h

$r_1 + hr_2$, $mG + s\,r_2 + e$

s (= x + yh)

e, r_1, r_2

Security Considerations

Security considerations

Schemes of this type (quasi-cyclic McEliece-style schemes) seem to be well-studied.

All four schemes claim security based on the hardness of decoding quasi-cyclic codes. (The connection is obvious to me for BIKE, and QC-MDPC, and a little less so for the more complex algorithms in HQC and LEDA.)

Security considerations

BIKE and QC-MDPC claim IND-CPA security.

HQC and LEDA claim IND-CCA2 security (although a commenter challenged this in the case of LEDA).

Other commenters raised security issues for HQC, LEDA, and BIKE, but none of them seem fatal to me.
(Comments from Ray?)

Performance

LEDApkc:
(updated)

Category	n_0	KeyGen (ms)	Encrypt (ms)	Decrypt (ms)
1	2	13.07 (± 0.37)	0.75 (± 0.05)	4.77 (± 0.51)
	3	5.75 (± 0.23)	0.75 (± 0.04)	6.04 (± 0.40)
	4	4.63 (± 0.16)	0.94 (± 0.08)	6.54 (± 0.62)
2–3	2	33.99 (± 0.65)	1.60 (± 0.08)	13.42 (± 1.03)
	3	18.46 (± 0.28)	1.94 (± 0.12)	14.90 (± 0.71)
	4	13.01 (± 0.33)	2.15 (± 0.15)	18.22 (± 0.83)
4–5	2	79.36 (± 1.45)	3.34 (± 0.18)	18.51 (± 0.89)
	3	46.72 (± 0.95)	4.20 (± 0.22)	25.20 (± 0.98)
	4	30.62 (± 0.58)	4.35 (± 0.14)	26.46 (± 1.27)

HQC:

Level:	KeyGen (ms)	Encaps (ms)	Decaps (ms)
1	0.17	0.36	0.57
	0.18	0.38	0.61
	0.19	0.40	0.63
3	0.37	0.77	1.13
	0.40	0.83	1.21
	0.43	0.89	1.28
5	0.65	1.38	1.96
	0.76	1.60	2.22
	0.78	1.65	2.35
	0.82	1.76	2.50

BIKE-1:

	Level 1	Level 3	Level 5
KeyGen (cycles)	730,025	1,709,921	2,986,647
Encaps (cycles)	689,193	1,850,425	3,023,816
Decaps (cycles)	2,901,203	7,666,855	17,483,906

QC-MDPC:

Level 3?

KeyGen (cycles)	131,000,000
Encaps (cycles)	20,000,000
Decaps (cycles)	230,000,000

LEDApkc: (updated)

Level:	Private Key Size (B) At rest	Private Key Size (B) In memory	Public Key size (B)	Max Plaintext size (B)	Ciphertext size (B)
1	24	468	1,880	2,001	3,760
	24	604	2,416	2,483	3,624
	24	716	3,192	3,231	4,256
3	32	644	3,072	3,251	6,144
	32	828	4,464	4,565	6,696
	32	924	5,520	5,602	7,360
5	40	764	4,704	4,950	9,408
	40	988	7,120	7,269	10,680
	40	1,092	8,592	8,681	11,456

HQC:

Level:	Pubkey (bytes)	PrivKey (bytes)	Cipher (bytes)
1	5,558	252	5,622
	5,938	252	6,001
	6,170	252	6,234
3	10,150	404	10,214
	10,918	404	10,982
	11,688	404	11,752
5	14,754	532	14,818
	15,898	532	15,962
	16,926	566	16,990
	17,714	566	17,778

BIKE-1:

	Level 1	Level 3	Level 5
Pubkey (bytes)	2,540	5,473	8,187
Privkey (bytes)	266	287	548
Cipher (bytes)	2,540	5,473	8,187

QC-MDPC:

	Level 3?
Pubkey (bytes)	4,097
Privkey (bytes)	548
Cipher (bytes)	8,226

IP Issues

Patents

HQC has a patent.

LEDApkc is "fully patent free."

"BIKE-1 and BIKE-2 are not covered by any patent. BIKE-3 is covered by a patent whose owners are willing to grant a non-exclusive license … without compensation …"

QC-MDPC has a patent. *(Note: HQC and QC- MDPC have also agreed to a non-exclusive license?)*

Comparison:
LEDA, BIKE, QC-MDPC, HQC

Carl A. Miller
NIST Computer Security Division
October 19, 2018

NIST PQC Seminar (not for public distribution)