LWE parameters for Brakerski/Fan-Vercauteren scheme implementation in Cingulata

November 26, 2018

This document contains information about parameter sets in the database. They are adapted for the Brakerski/Fan-Vercauteren implementation in Cingulata. Security is estimated using the LWE Estimator (Commit ID = $a2296b8$). The security expressed in the filename is an approximated value. Estimated security is indicated in the corresponding file.

We avoid the notation σ due to different usages in the literature, in the same context.

$$\text{Gaussian\_width} = 2\sqrt{n}$$

$$\text{noise\_rate} = \frac{\text{Gaussian\_width}}{q} = \frac{2\sqrt{n}}{q}$$

$$\text{std\_dev} = \frac{\text{Gaussian\_width}}{\sqrt{2\pi}} = \sqrt{\frac{2n}{\pi}}$$

Remark: Note that some parameters generated with multiplicative depth 1 are inconsistent (lower parameter with bigger estimated security with the same reduction cost model).

Filename	Reference
BKZ Enum	[CheNgu12]
BKZ Sieve	[BDGL16]
Core Sieve	[ADPS16] (mode classical)
Q-Core Sieve	[ADPS16] (mode quantum)

Table 1: Four BKZ reduction cost models considered in CinguParam.

References

[CheNgu12] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates (Full Version). `http://www.di.ens.fr/~ychen/research/Full_BKZ.pdf`

[BDGL16] Becker, A., Ducas, L., Gama, N., Laarhoven, T. New directions in nearest neighbor searching with applications to lattice sieving. SODA 2016

[ADPS16] Edem Alkim, Léo Ducas, Thomas Pöppelmann, & Peter Schwabe Post-quantum key exchange - A New Hope. USENIX Security 16 (pp. 327–343).

Syntax: multiplicative-depth_reduction-cost-model_desired-security-level

Filename	n	$\log_2(q)$	std_dev
1_*q*_*core*_*sieve*_192	4096	54	51
1_*bkz*_*sieve*_256			
1_*core*_*sieve*_256			
2_*bkz*_*sieve*_192		76	
2_*core*_*sieve*_128			
2_*q*_*core*_*sieve*_128			
2_*q*_*core*_*sieve*_128			
2_*q*_*core*_*sieve*_128			
3_*core*_*sieve*_80		101	
3_*bkz*_*enum*_256			
3_*bkz*_*sieve*_128			
3_*q*_*core*_*sieve*_80			
1_*bkz*_*sieve*_80		117	
1_*core*_*sieve*_80			
1_*bkz*_*enum*_192			
2_*bkz*_*enum*_192			
2_*bkz*_*sieve*_80			
2_*core*_*sieve*_80			
3_*bkz*_*sieve*_80			
3_*bkz*_*enum*_192			
4_*bkz*_*enum*_128		126	
4_*bkz*_*sieve*_80			
4_*bkz*_*enum*_80			
5_*bkz*_*enum*_128		151	
5_*bkz*_*sieve*_80			
6_*bkz*_*enum*_80		176	
5_*bkz*_*enum*_80		181	

Filename	n	$\log_2(q)$	std_dev
3_q_core_sieve_192 3_bkz_sieve_256 3_core_sieve_256	8192	108	72
1_core_sieve_192 2_q_core_sieve_192 2_bkz_sieve_256 2_core_sieve_192 3_core_sieve_192		117	
4_q_core_sieve_128 4_bkz_sieve_192 4_core_sieve_192		135	
5_bkz_sieve_128 5_core_sieve_128 5_q_core_sieve_128		162	
4_q_core_sieve_80 4_bkz_enum_256 4_bkz_sieve_128 4_core_sieve_128 5_q_core_sieve_80 5_bkz_enum_256		181	
6_q_core_sieve_80 6_core_sieve_80 6_bkz_enum_256 6_bkz_sieve_128		189	
7_core_sieve_80 7_q_core_sieve_80 7_bkz_enum_192 7_bkz_sieve_128		216	
8_bkz_enum_128 8_bkz_sieve_80 8_core_sieve_80		243	
6_bkz_enum_128 6_bkz_sieve_80 7_bkz_enum_128 7_bkz_sieve_80		245	
9_bkz_enum_128 9_bkz_sieve_80		270	
10_bkz_sieve_80 10_bkz_enum_128		297	
9_bkz_enum_80 10_bkz_enum_80		309	
11_bkz_enum_80 11_bkz_sieve_80		324	
12_bkz_enum_80		351	
13_bkz_enum_80		378	

Filename	n	$\log_2(q)$	std_dev
5_q_core_sieve_256	16384	174	102
4_q_core_sieve_256		181	
6_core_sieve_256		203	
6_bkz_sieve_256			
6_q_core_sieve_256			
7_core_sieve_192		232	
7_q_core_sieve_192			
7_bkz_sieve_256			
6_q_core_sieve_192		245	
6_core_sieve_192			
8_bkz_sieve_192		261	
8_core_sieve_192			
8_q_core_sieve_128			
9_bkz_sieve_192		290	
9_core_sieve_128			
9_q_core_sieve_128			
8_core_sieve_128		309	
10_q_core_sieve_128		319	
10_bkz_sieve_128			
10_core_sieve_128			
11_bkz_sieve_128		348	
11_core_sieve_128			
11_q_core_sieve_80			
10_core_sieve_80		373	
10_q_core_sieve_80			
10_bkz_enum_256			
11_bkz_enum_256			
11_core_sieve_80			
12_bkz_enum_256		377	
12_bkz_sieve_128			
12_q_core_sieve_80			
12_core_sieve_80			
13_bkz_enum_192		406	
13_core_sieve_80			
13_q_core_sieve_80			
13_bkz_sieve_128			
14_bkz_enum_192		435	
14_core_sieve_80			
14_q_core_sieve_80			
14_bkz_sieve_128			
12_bkz_enum_192		437	
15_bkz_enum_192		464	
15_bkz_sieve_128			
15_core_sieve_80			
16_bkz_enum_128		493	
16_bkz_sieve_80			
15_bkz_sieve_80		501	
15_bkz_enum_128			
17_bkz_enum_128		522	
17_bkz_sieve_80			
18_bkz_enum_128		551	
18_bkz_sieve_80			
19_bkz_enum_128		580	
19_bkz_sieve_80			
20_bkz_enum_80		609	
20_bkz_sieve_80			
19_bkz_enum_80		629	

Filename	n	$\log_2(q)$	std_dev
11_*q*_*core*_*sieve*_256 11_*core*_*sieve*_256	32768	371	144
10_*q*_*core*_*sieve*_256 10_*core*_*sieve*_256		373	
12_*q*_*core*_*sieve*_256 12_*core*_*sieve*_256		402	
13_*bkz*_*sieve*_256 13_*core*_*sieve*_256 13_*q*_*core*_*sieve*_192		433	
12_*q*_*core*_*sieve*_192 12_*bkz*_*sieve*_256		437	
14_*bkz*_*sieve*_256 14_*core*_*sieve*_192 14_*q*_*core*_*sieve*_192		464	
15_*core*_*sieve*_192 15_*bkz*_*sieve*_192 15_*q*_*core*_*sieve*_192		495	
14_*bkz*_*sieve*_192		501	
16_*bkz*_*sieve*_192 16_*core*_*sieve*_192 16_*q*_*core*_*sieve*_128		526	
17_*bkz*_*sieve*_192 17_*core*_*sieve*_128 17_*q*_*core*_*sieve*_128		557	
16_*core*_*sieve*_128		565	
18_*bkz*_*sieve*_192 18_*core*_*sieve*_128 18_*q*_*core*_*sieve*_128		588	
19_*bkz*_*sieve*_192 19_*core*_*sieve*_128 19_*q*_*core*_*sieve*_128		619	
20_*bkz*_*sieve*_128 20_*core*_*sieve*_128 20_*q*_*core*_*sieve*_128		650	
20_*q*_*core*_*sieve*_80		693	
20_*q*_*core*_*sieve*_256	65536	692	204
19_*q*_*core*_*sieve*_256		693	