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

November 27, 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[1] (Commit ID = $a2296b8$). The security expressed in the filename is an approximated value. Estimated security is indicated in the corresponding file.

$$\text{Gaussian\_width} = 2\sqrt{n} \text{ (hardness-reduction compliant [P16, p.11])}$$

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

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

| 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. `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).

[P16] Peikert, Chris How (not) to instantiate ring-LWE International Conference on Security and Cryptography for Networks, 2016


[1] Note that some parameters generated with multiplicative depth 1 are inconsistent (lower-size parameters with bigger estimated security under the same reduction cost model).

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

| Filename | $n$ | $\log_2(q)$ | $\lfloor$std_dev$\rfloor$ | $\lfloor$Gaussian_width$\rfloor$ |
|---|---|---|---|---|
| 1_*q*_*core*_*sieve*_192<br>1_*bkz*_*sieve*_256<br>1_*core*_*sieve*_256 | 4096 | 54 | 51 | 128 |
| 2_*bkz*_*sieve*_192<br>2_*core*_*sieve*_128<br>2_*q*_*core*_*sieve*_128<br>2_*q*_*core*_*sieve*_128<br>2_*q*_*core*_*sieve*_128 | | 76 | | |
| 3_*core*_*sieve*_80<br>3_*bkz*_*enum*_256<br>3_*bkz*_*sieve*_128<br>3_*q*_*core*_*sieve*_80 | | 101 | | |
| 1_*bkz*_*sieve*_80<br>1_*core*_*sieve*_80<br>1_*bkz*_*enum*_192<br>2_*bkz*_*enum*_192<br>2_*bkz*_*sieve*_80<br>2_*core*_*sieve*_80<br>3_*bkz*_*sieve*_80<br>3_*bkz*_*enum*_192 | | 117 | | |
| 4_*bkz*_*enum*_128<br>4_*bkz*_*sieve*_80<br>4_*bkz*_*enum*_80 | | 126 | | |
| 5_*bkz*_*enum*_128<br>5_*bkz*_*sieve*_80 | | 151 | | |
| 6_*bkz*_*enum*_80 | | 176 | | |
| 5_*bkz*_*enum*_80 | | 181 | | |

| Filename | $n$ | $\log_2(q)$ | $\lfloor$std_dev$\rfloor$ | $\lfloor$Gaussian_width$\rfloor$ |
|---|---|---|---|---|
| 3_*q_core_sieve*_192<br>3_*bkz_sieve*_256<br>3_*core_sieve*_256 | 8192 | 108 | 72 | 180 |
| 1_*core_sieve*_192<br>2_*q_core_sieve*_192<br>2_*bkz_sieve*_256<br>2_*core_sieve*_192<br>3_*core_sieve*_192 | | 117 | | |
| 4_*q_core_sieve*_128<br>4_*bkz_sieve*_192<br>4_*core_sieve*_192 | | 135 | | |
| 5_*bkz_sieve*_128<br>5_*core_sieve*_128<br>5_*q_core_sieve*_128 | | 162 | | |
| 4_*q_core_sieve*_80<br>4_*bkz_enum*_256<br>4_*bkz_sieve*_128<br>4_*core_sieve*_128<br>5_*q_core_sieve*_80<br>5_*bkz_enum*_256 | | 181 | | |
| 6_*q_core_sieve*_80<br>6_*core_sieve*_80<br>6_*bkz_enum*_256<br>6_*bkz_sieve*_128 | | 189 | | |
| 7_*core_sieve*_80<br>7_*q_core_sieve*_80<br>7_*bkz_enum*_192<br>7_*bkz_sieve*_128 | | 216 | | |
| 8_*bkz_enum*_128<br>8_*bkz_sieve*_80<br>8_*core_sieve*_80 | | 243 | | |
| 6_*bkz_enum*_128<br>6_*bkz_sieve*_80<br>7_*bkz_enum*_128<br>7_*bkz_sieve*_80 | | 245 | | |
| 9_*bkz_enum*_128<br>9_*bkz_sieve*_80 | | 270 | | |
| 10_*bkz_sieve*_80<br>10_*bkz_enum*_128 | | 297 | | |
| 9_*bkz_enum*_80<br>10_*bkz_enum*_80 | | 309 | | |
| 11_*bkz_enum*_80<br>11_*bkz_sieve*_80 | | 324 | | |
| 12_*bkz_enum*_80 | | 351 | | |
| 13_*bkz_enum*_80 | | 378 | | |

| Filename | $n$ | $\log_2(q)$ | ⌊std_dev⌋ | ⌊Gaussian_width⌋ |
|---|---|---|---|---|
| 5_*q_core_sieve*_256 | 16384 | 174 | 102 | 512 |
| 4_*q_core_sieve*_256 | | 181 | | |
| 6_*core_sieve*_256<br>6_*bkz_sieve*_256<br>6_*q_core_sieve*_256 | | 203 | | |
| 7_*core_sieve*_192<br>7_*q_core_sieve*_192<br>7_*bkz_sieve*_256 | | 232 | | |
| 6_*q_core_sieve*_192<br>6_*core_sieve*_192 | | 245 | | |
| 8_*bkz_sieve*_192<br>8_*core_sieve*_192<br>8_*q_core_sieve*_128 | | 261 | | |
| 9_*bkz_sieve*_192<br>9_*core_sieve*_128<br>9_*q_core_sieve*_128 | | 290 | | |
| 8_*core_sieve*_128 | | 309 | | |
| 10_*q_core_sieve*_128<br>10_*bkz_sieve*_128<br>10_*core_sieve*_128 | | 319 | | |
| 11_*bkz_sieve*_128<br>11_*core_sieve*_128<br>11_*q_core_sieve*_80 | | 348 | | |
| 10_*core_sieve*_80<br>10_*q_core_sieve*_80<br>10_*bkz_enum*_256<br>11_*bkz_enum*_256<br>11_*core_sieve*_80 | | 373 | | |
| 12_*bkz_enum*_256<br>12_*bkz_sieve*_128<br>12_*q_core_sieve*_80<br>12_*core_sieve*_80 | | 377 | | |
| 13_*bkz_enum*_192<br>13_*core_sieve*_80<br>13_*q_core_sieve*_80<br>13_*bkz_sieve*_128 | | 406 | | |
| 14_*bkz_enum*_192<br>14_*core_sieve*_80<br>14_*q_core_sieve*_80<br>14_*bkz_sieve*_128 | | 435 | | |
| 12_*bkz_enum*_192 | | 437 | | |
| 15_*bkz_enum*_192<br>15_*bkz_sieve*_128<br>15_*core_sieve*_80 | | 464 | | |
| 16_*bkz_enum*_128<br>16_*bkz_sieve*_80 | | 493 | | |
| 15_*bkz_sieve*_80<br>15_*bkz_enum*_128 | | 501 | | |
| 17_*bkz_enum*_128<br>17_*bkz_sieve*_80 | | 522 | | |
| 18_*bkz_enum*_128<br>18_*bkz_sieve*_80 | | 551 | | |
| 19_*bkz_enum*_128<br>19_*bkz_sieve*_80 | | 580 | | |
| 20_*bkz_enum*_80<br>20_*bkz_sieve*_80 | | 609 | | |
| 19_*bkz_enum*_80 | | 629 | | |

| Filename | $n$ | $\log_2(q)$ | $\lfloor$std_dev$\rfloor$ | $\lfloor$Gaussian_width$\rfloor$ |
|---|---|---|---|---|
| 11_*q_core_sieve*_256<br>11_*core_sieve*_256 | 32768 | 371 | 144 | 362 |
| 10_*q_core_sieve*_256<br>10_*core_sieve*_256 | | 373 | | |
| 12_*q_core_sieve*_256<br>12_*core_sieve*_256 | | 402 | | |
| 13_*bkz_sieve*_256<br>13_*core_sieve*_256<br>13_*q_core_sieve*_192 | | 433 | | |
| 12_*q_core_sieve*_192<br>12_*bkz_sieve*_256 | | 437 | | |
| 14_*bkz_sieve*_256<br>14_*core_sieve*_192<br>14_*q_core_sieve*_192 | | 464 | | |
| 15_*core_sieve*_192<br>15_*bkz_sieve*_192<br>15_*q_core_sieve*_192 | | 495 | | |
| 14_*bkz_sieve*_192 | | 501 | | |
| 16_*bkz_sieve*_192<br>16_*core_sieve*_192<br>16_*q_core_sieve*_128 | | 526 | | |
| 17_*bkz_sieve*_192<br>17_*core_sieve*_128<br>17_*q_core_sieve*_128 | | 557 | | |
| 16_*core_sieve*_128 | | 565 | | |
| 18_*bkz_sieve*_192<br>18_*core_sieve*_128<br>18_*q_core_sieve*_128 | | 588 | | |
| 19_*bkz_sieve*_192<br>19_*core_sieve*_128<br>19_*q_core_sieve*_128 | | 619 | | |
| 20_*bkz_sieve*_128<br>20_*core_sieve*_128<br>20_*q_core_sieve*_128 | | 650 | | |
| 20_*q_core_sieve*_80 | | 693 | | |
| 20_*q_core_sieve*_256 | 65536 | 692 | 204 | 512 |
| 19_*q_core_sieve*_256 | | 693 | | |