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 usage in the literature for 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).

Name	n	$\log_2(q)$	std_dev
1_q_core_sieve_192 1_bkz_sieve_256 1_core_sieve_256		54	
2_bkz_sieve_192 2_core_sieve_128 2_q_core_sieve_128 2_q_core_sieve_128 2_q_core_sieve_128		76	
3_core_sieve_80 3_bkz_enum_256 3_bkz_sieve_128 3_q_core_sieve_80		101	
1_bkz_sieve_80 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	4096	117	51
4_bkz_enum_128 4_bkz_sieve_80 4_bkz_enum_80		126	
5_bkz_enum_128 5_bkz_sieve_80		151	
6_bkz_enum_80		176	
5_bkz_enum_80		181	

Name	n	$\log_2(q)$	std_dev
3_*q_core_sieve*_192 3_*bkz_sieve*_256 3_*core_sieve*_256		108	
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	8192	181	72
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	

Name	n	$\log_2(q)$	std_dev
5_q_core_sieve_256		174	
4_q_core_sieve_256		181	
6_core_sieve_256			
6_bkz_sieve_256		203	
6_q_core_sieve_256			
7_core_sieve_192			
7_q_core_sieve_192		232	
7_bkz_sieve_256			
6_q_core_sieve_192		245	
6_core_sieve_192			
8_bkz_sieve_192			
8_core_sieve_192		261	
8_q_core_sieve_128			
9_bkz_sieve_192			
9_core_sieve_128		290	
9_q_core_sieve_128			
8_core_sieve_128		309	
10_q_core_sieve_128			
10_bkz_sieve_128		319	
10_core_sieve_128			
11_bkz_sieve_128			
11_core_sieve_128	16384	348	102
11_q_core_sieve_80			
10_core_sieve_80			
10_q_core_sieve_80			
10_bkz_enum_256		373	
11_bkz_enum_256			
11_core_sieve_80			
12_bkz_enum_256			
12_bkz_sieve_128		377	
12_q_core_sieve_80			
12_core_sieve_80			
13_bkz_enum_192			
13_core_sieve_80		406	
13_q_core_sieve_80			
13_bkz_sieve_128			
14_bkz_enum_192			
14_core_sieve_80		435	
14_q_core_sieve_80			
14_bkz_sieve_128			
12_bkz_enum_192		437	
15_bkz_enum_192			
15_bkz_sieve_128		464	
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	

Name	n	$\log_2(q)$	std_dev
11_q_core_sieve_256 11_core_sieve_256		371	
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	32768	464	144
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	