

## CKKS parameter

**CKKS Error Estimation** The number of error bits in the fresh ciphertext  $c_1$  encrypting message  $m_1$  using error distribution  $N(0, \sigma^2 I_N)$  and secret distribution  $\{-1, 0, 1\}$  is given by (Using Central Limit Theory (CLT))

$$\epsilon_1 = \frac{1}{2} \log N(\rho_{fresh}^2 + \frac{1}{12}) + \log H_c(\alpha, N) \quad (1)$$

where

$$\begin{aligned} \rho_{fresh}^2 &= (\frac{4}{3}N + 1)\sigma^2 \\ H_c(\alpha, N) &= (-\log(1 - (1 - \alpha)^{\frac{2}{N}}))^{\frac{1}{2}} \end{aligned}$$

$\alpha$  = failure probability or error tolerance

Similarly, ciphertext  $c_2$  encrypting message  $m_2$  using the error distribution  $N(0, \sigma'^2 I_N)$  and same secret distribution can be written as

$$\epsilon_2 = \frac{1}{2} \log N(\rho_{fresh}'^2 + \frac{1}{12}) + \log H_c(\alpha, N) \quad (2)$$

where

$$\rho_{fresh}'^2 = (\frac{4}{3}N + 1)\sigma'^2$$

**Addition** Adding these two ciphertext results into ciphertext with error bits

$$\epsilon_1 + \epsilon_2 = \frac{1}{2} \log N(\rho_{fresh}''^2 + \frac{1}{6}) + \log 2H_c(\alpha, N) \quad (3)$$

where

$$\rho_{fresh}''^2 = (\frac{4}{3}N + 1)(\sigma^2 + \sigma'^2)$$

**Multiplication by constant** : Multiplying the ciphertext with a constant results in a ciphertext with error as

$$err = ||\lambda||_2^2 (\frac{4}{3}N + 1)\sigma^2 \quad (4)$$

**Multiplication** : Multiplication of two ciphertext results into ciphertext with error of the following form

$$B_{final\ error} = \Delta^{-1}(B_{mult} + B_{ks}) + B_{round} \quad (5)$$

$$B_{mult} = N(0, N\rho_{fresh}^2\rho_{fresh}'^2 I_N)$$

$$B_{ks} = N(0, \eta_{ks}^2 I_N)$$

$$\rho_{fresh}^2 = (\frac{4}{3}N + 1)\sigma^2$$

where

$$\begin{aligned} \eta_{ks}^2 &= \frac{1}{12}p^{-2}Nq_l^2\sigma^2 + 1_{p \nmid q_l}(\frac{N}{18} + \frac{1}{12}) \\ &= \frac{1}{12}N\sigma^2 \end{aligned}$$

$$[\frac{q_l^2}{p^2}1]$$

N	security level	$\log q$	uSVP	dec	dual
1024	128	25	132.6	165.5	142.3
	192	17	199.9	284.1	222.2
	256	13	262.6	423.1	296.6
2048	128	51	128.6	144.3	133.4
	192	35	193.5	231.9	205.2
	256	27	257.1	327.8	274.4
4096	128	101	129.6	137.4	131.5
	192	70	193.7	213.6	198.8
	256	54	259.7	295.2	270.6
8192	128	202	129.8	130.7	128.0
	192	141	192.9	202.5	196.1
	256	109	258.3	276.6	263.1
16384	128	411	128.2	129.5	129.0
	192	284	192.0	196.8	193.7
	256	220	257.2	265.8	260.7
32768	128	827	128.1	128.7	128.4
	192	571	192.0	194.1	193.1
	256	443	256.1	260.4	260.4

Table 1: The different parameter values shown in the table means following  $N$  is the ring dimension, security level is the bit security provided by the chosen parameter value equivalent to that of AES,  $\log q$  is the number of bits in the modulus  $q$ . *uSVP* represents the bit security against attack using unique shortest vector problem, *dec* represents the bit security against decoding attack and *dual* represents the bit security against dual attack.