December 9, 2022

CKKS Parameters

This file is created to write the encryption paramters of CKKS encryption scheme. The following parameters are used in Openfhe library for 128 bit security. Error sampled from gaussion distribution with standard deviation 3.2 and Secret sampled from uniform ternary distribution with variance $\frac{1}{3}$=.33333.

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=90; RingDimension=65536 RingModulus=645

batchSize = 8; MultiplicativeDepth=10; ScalingModSize=90; RingDimension=65536 RingModulus=1006

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=80; RingDimension=32768 RingModulus=585

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=70 RingDimension=32768 RingModulus=524

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=60; RingDimension=32768 RingModulus=465

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=50; RingDimension=32768 RingModulus=404

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=40 RingDimension=32768 RingModulus=344

batchSize = 8; MultiplicativeDepth=6; ScalingModSize=30; RingDimension=16384 RingModulus=284

Apart form the above mentioned parameters homomorphic encryption standar suggests following paramters as secure parameters. The same parametes have been used in the paper "On the precision loss in approximate homomorphic encryption" as mentioned below.

(Dimension,modulus): (log(N),log(q)) as

(13,109) , (14,220) , (15,443)

Error Distribution: Gaussion with std. deviation 3.2; Secret Distribution: uniform ternary distribution viz. (-1,0,1) with variance $\frac{1}{3}$ = .33333; Delta=2^{40}.

Here is the list of parameter values for varing security levels. Secret and error distribution remains same as that of mentioned above. (Here number corresponding to SVP, dec and dual means bit security provided by the parameter values when attacked using unique svp ,decoding and dual attack)

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 differnt parameter values shown in the table means N represents the ring dimension, security level is the bit security provided by the chosen parameter valuse 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* represnts the bit security against dual attack.