Fast Parameter Selection for FHE

Elena Kirshanova, CRC, TII, Abu Dhabi, United Arab Emirates
Chiara Marcolla, CRC, TII, Abu Dhabi, United Arab Emirates
Sergi Rovira, WiSeCom, UPF, Barcelona, Spain

Our Contribution

We present a novel method for determining optimal parameters for any FHE scheme, focusing on the *macro* level, namely n, q, σ and λ. (Recall LWE: given A, As + e mod q, find s, where A is uniform from $Z_q^{m \times n}$, e is discrete Gaussian with parameter σ)

- We derive closed and precise formulas of the running times of the lattice attacks as functions of n, q, σ, λ and β (block size of BKZ for a lattice of rank n) for the most relevant parameters in FHE.
- We use them to express λ and n as a function of the other parameters.
- We fine-tune our formulas to make sure that lower-order terms in the derived expressions are of the correct form, and hence, provide accurate estimates for broad parameter sets.
- We provide Python scripts that implement our formulas.

Formula for λ (uSVP)

$$\lambda = A\beta + B \ln \left(\frac{2n \ln(q/\zeta)\beta}{\ln(\beta/(2\pi e))} \right) + C, \tag{1}$$

$\mathrm{A} = 0.28862 \quad \mathrm{B} = 1.33981 \quad \mathrm{C} = 5.61427 \quad$ if $\sigma_s = \mathcal{U}_2$
$\mathrm{A} = 0.296208 \quad \mathrm{B} = 0.800603 \quad \mathrm{C} = 12.09086 \quad$ if $\sigma_s = \mathcal{U}_3$.

Simplified formula for λ (uSVP)

$$\lambda \approx A \ln \left(\frac{Bn}{\ln q} \right) \frac{n}{\ln q} + C \ln n + D \tag{2}$$

$\mathrm{A} = 0.445309 \quad \mathrm{B} = 1.486982 \quad \mathrm{C} = 0.950115 \quad \mathrm{D} = 11.21416$ if $\sigma_s = \mathcal{U}_2$
$\mathrm{A} = 0.833542 \quad \mathrm{B} = 0.154947 \quad \mathrm{C} = 1.469823 \quad \mathrm{D} = 18.09877$ if $\sigma_s = \mathcal{U}_3$.

Simplified Formula for n (uSVP)

$$n \approx \left(\frac{\lambda + A \ln(\ln q)}{B \ln(\lambda) + C} + D \right) \ln q \tag{3}$$

$\mathrm{A} = -1.142080 \ \mathrm{B} = 0.231197 \ \mathrm{C} = 1.106616 \ \mathrm{D} = -0.233138 \quad$ if $\sigma_s = \mathcal{U}_2$
$\mathrm{A} = -1.073049 \ \mathrm{B} = 0.278319 \ \mathrm{C} = 0.931202 \ \mathrm{D} = 0.792882 \quad$ if $\sigma_s = \mathcal{U}_3$.

Simplified Formula for n (BDD)

$$n = \left(A \frac{\lambda}{\ln \lambda} + B \ln(\ln q) + C \right) \ln q + D \tag{4}$$

$\mathrm{A} = 2.463040 \ \mathrm{B} = 3.426581 \quad \mathrm{C} = -24.92487 \ \mathrm{D} = 128.0417 \quad$ if $\sigma_s = \mathcal{U}_2$
$\mathrm{A} = 2.368303 \ \mathrm{B} = -0.676307 \ \mathrm{C} = -4.104371 \ \mathrm{D} = -19.11047 \quad$ if $\sigma_s = \mathcal{U}_3$.

Verification for λ with $\sigma_s = \mathcal{U}_2$ (uSVP)

	$n = 2^{10}$				$n = 2^{11}$		
$\log q$	Estimator	(1)	(2)	$\log q$	Estimator	(1)	(2)
20	172	172	172	37	191	191	188
24	142	142	142	46	151	150	149
25	136	136	136	50	137	137	136
26	130	130	130	53	129	129	128
27	125	125	125	54	126	127	126
28	120	120	120	57	119	119	119
30	112	112	112	62	110	109	109
33	101	101	101	67	100	101	101
37	90	90	90	74	90	91	91
42	79	79	80	84	80	80	80

Table 1: Comparison between the security level provided by our formulas (Equations (1) and (2)) and the Lattice Estimator with with $\sigma_s = \mathcal{U}_2$.

Verification for λ with $\sigma_s = \mathcal{U}_3$ (uSVP)

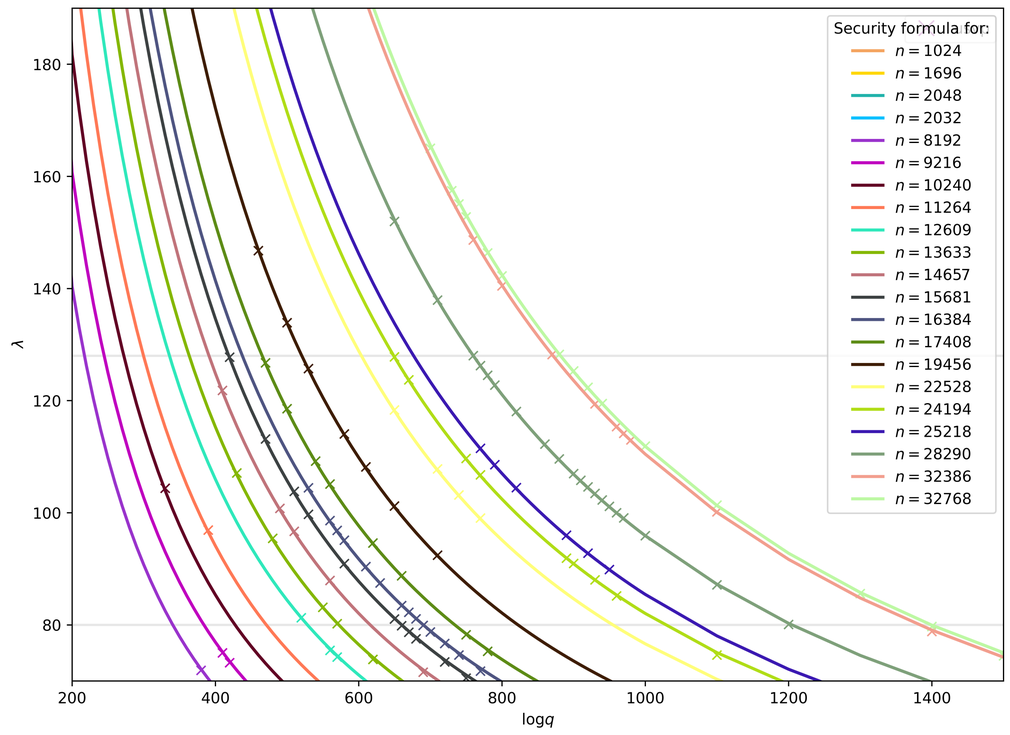

Figure 1: The security formula (Equation (2)) with data points of the Lattice Estimator for $\sigma_s = \mathcal{U}_3$ considering the uSVP attack.

Verification for n with $\sigma_s = \mathcal{U}_2$ (uSVP)

$\log q$	Est_λ	Est_n	(3)	$\log q$	Est_λ	Est_n	(3)
	$\lambda \approx 80$				$\lambda \approx 100$		
42	80	1024	1039	34	100	1024	1041
58	80	1408	1428	46	102	1408	1429
71	80	1728	1743	57	100	1728	1734
84	80	2048	2056	67	100	2048	2034
	$\lambda \approx 110$				$\lambda \approx 120$		
31	110	1024	1038	28	123	1024	1042
42	112	1408	1426	39	121	1408	1424
52	111	1792	1747	48	121	1792	1749
61	112	2048	2063	57	121	2048	2074
	$\lambda \approx 128$				$\lambda \approx 140$		
27	128	1024	1043	24	144	1024	1034
37	128	1408	1425	34	140	1408	1424
45	129	1728	1742	41	143	1728	1748
54	128	2048	2072	49	142	2048	2073

Table 2: Comparison between the LWE dimension provided by our formula Equation (3) and the Lattice Estimator with secret distribution $\mathcal{U}_2$.

Verification for n with $\sigma_s = \mathcal{U}_3$ (BDD)

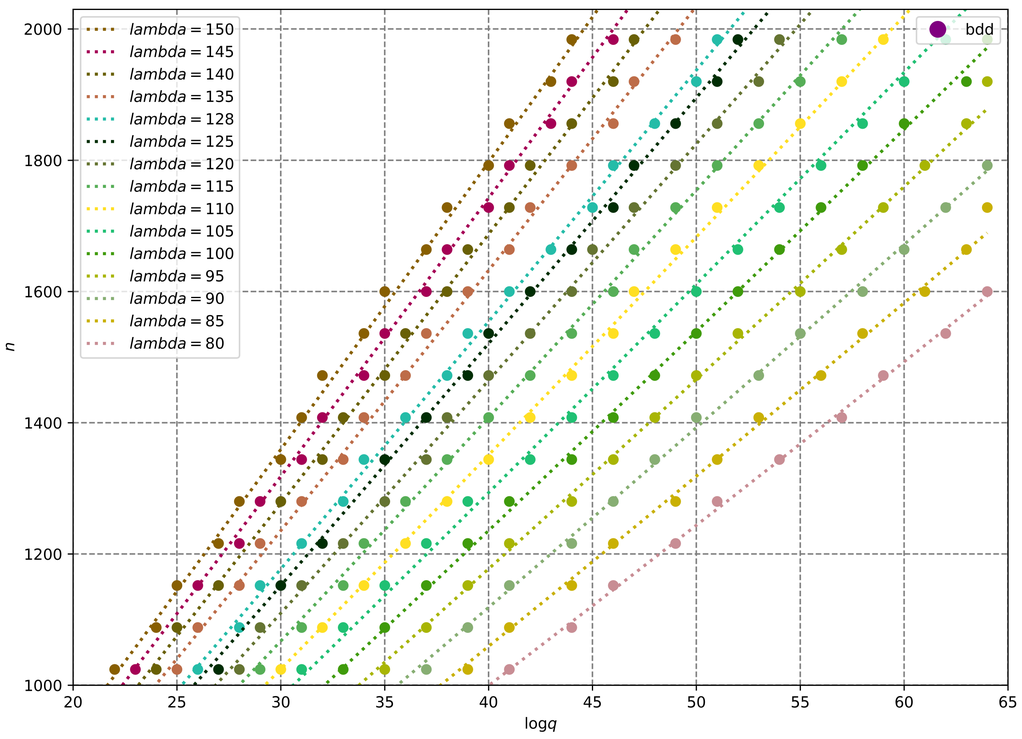

Figure 2: The security formula (Equation (4)) with data points of the Lattice Estimator for $\sigma_s = \mathcal{U}_3$ considering the uSVP attack.

ACKNOWLEDGEMENT

The 3rd listed author is partially supported by the Spanish grant PID2019-110224RB-I00.

CONTACT

- Elena.Kirshanova@tii.ae
- Chiara.Marcolla@tii.ae
- sergi.rovira@upf.edu

TRY IT OUT!

https://github.com/fhe2024/fastselection