Finding and Evaluating Parameters for FV using the average-case approach

Beatrice Biasioli[1], Chiara Marcolla[1], Marco Calderini[2] and Johannes Mono[3]

1 Technology Innovation Institute, Abu Dhabi, United Arab Emirates, 2 Università degli studi di Trento, Italy; 3 Ruhr University Bochum,Germany

Notations

$\mathcal{R} = \mathbb{Z}[x]/\langle x^n+1\rangle$ $\qquad$ $\mathcal{K} = \mathbb{Q}[x]/\langle x^n+1\rangle$ where $n = 2^\kappa$.

$m \in \mathcal{R}_t$ message $\qquad$ $\mathbf{c} = (c_0, c_1) \in \mathcal{R}_q$ ciphertext

$s \in \chi_s$ secret key, where $\chi_s = \{-1, 0, 1\}$

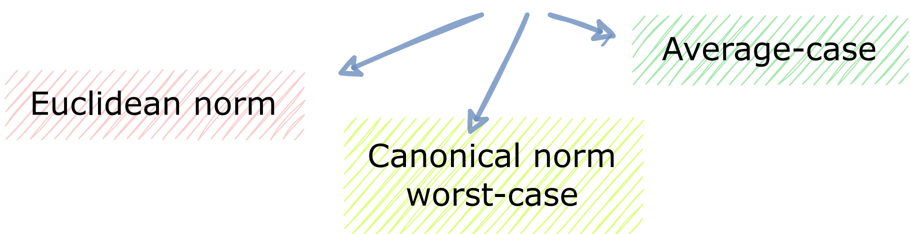
Let $a \in \mathcal{R}$ random, and V_a the variance of the coefficients of a.

The bounds for the error estimation are:

Our max $\leq 6\sqrt{2V_a}$, Our mean $\approx \sqrt{V_a}$, can $||a||^{can} \leq 6\sqrt{nV_a}$

What a complex life!

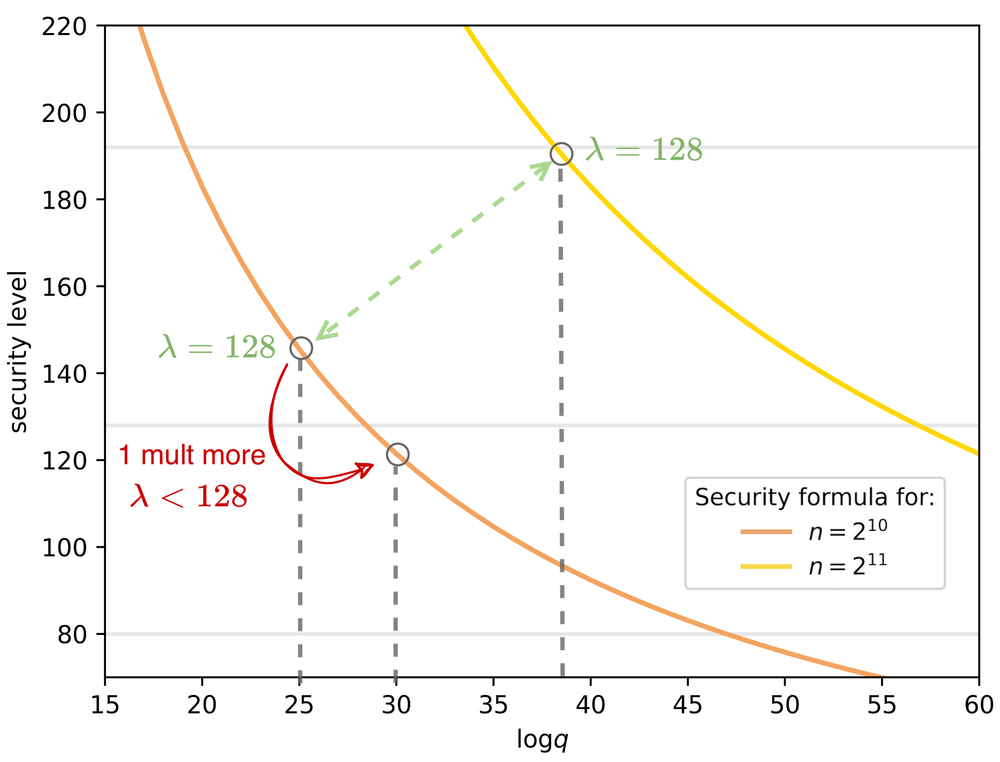
1. Every operation increases the error.
2. Any error must be bounded.



3. Security & Parameters problem:

\# operations $\uparrow$ $\quad q \uparrow \quad \lambda \downarrow$

\# operations $\uparrow$ $\quad q \uparrow \quad \lambda = \quad n \uparrow$



Parameter Generator

Notations

M = # multiplications

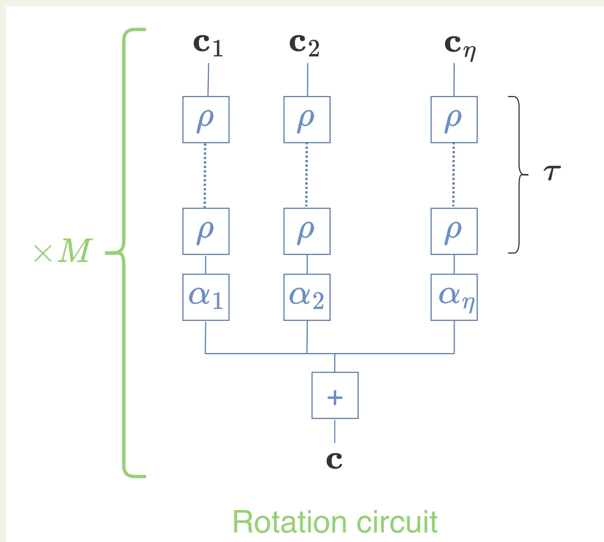
η = # summands

τ = # rotations

Generator Inputs (Selection)

Input	Options
sec *or* n	any integer ≥ 40 or ≥ 4, resp.
M, η	any integer ≥ 1
τ	any integer ≥ 0
Model	$1, 2, 3, 4$
Library	`None`, `'OpenFHE'`, `'PALISADE'`, `'SEAL'`
KeySwitch	`'BV'`, `'GHS'`, `'Hybrid'`

Generator Circuit (Model 3)



Our method: average-case approach analysis

The *invariant noise* associated with a ciphertext $\mathbf{c} = (c_0, c_1)$ is the minimal $\nu \in \mathcal{K}$ such that

$$\frac{t}{q}[c_0 + c_1 s]_q = m + \nu + kt \quad \text{for some } k \in \mathcal{R}.$$

Any coefficient of ν can be well-approximated with a Gaussian centered in 0.

Idea: study the variance of each coefficient.

Problem: coefficients are not independent.

Solution: estimate the behaviour of (powers of) s statistically.

$$\texttt{HomAdd}(\mathbf{c}, \mathbf{c}') \to \nu_{\mathsf{add}} = \nu + \nu' \implies V_{\mathsf{add}} = V + V'$$

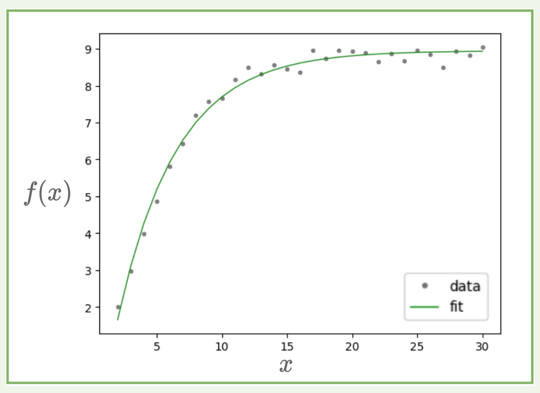
$$\texttt{HomMul}(\mathbf{c}, \mathbf{c}') \to \nu_{\mathsf{mul}} \approx \nu\frac{t}{q'}(c_0' + c_1' s) + \nu'\frac{t}{q}(c_0 + c_1 s)$$

$$\implies V_{\mathsf{mul}} \leq \frac{t^2 n^2 V_s}{12}\Big(V + V'\Big) f(\ell + 1)$$

where

$$f(x) \approx -\frac{1}{e^{ax-b}} + c,$$

where a, b, c depend on n and χ_s.



Comparison

Let ν be the invariant noise associated with $\mathbf{c}$. The *noise budget* captures the correctness in FV. Indeed, it is the number of bits left for correct decryption. Since $||\nu|| < 1/2$, then the noise budget for $\mathbf{c}$ is defined as $-\log_2(2 \cdot ||\nu||)$.

		Encryption					Addition				
			maximum value		mean value			maximum value		mean value	
n	$\log_2(q)$	can	our	exp	our	exp	can	our	exp	our	exp
2^{12}	74	54.9	60.4	61.1	63.5	63.9	53.9	59.9	60.7	63.0	63.4
2^{13}	149	128.9	134.9	135.7	138.0	138.4	127.9	134.4	135.1	137.5	137.86
2^{14}	298	276.9	283.4	284.0	286.5	286.9	275.9	282.9	283.6	286.0	286.4
2^{15}	597	574.9	581.9	582.5	585.0	585.4	573.9	581.4	582.0	584.5	584.9

		Multiplication					Circuit $(M = 3, \eta = 8, \tau = 0, \alpha = 1)$				
			maximum value		mean value			maximum value		mean value	
n	$\log_2(q)$	can	our	exp	our	exp	can	our	exp	our	exp
2^{12}	74	39.9	47.9	48.8	51.0	51.6	0.7	17.7	19.1	20.7	21.4
2^{13}	149	112.9	121.4	122.3	124.5	125.1	71.7	89.7	90.3	92.2	92.8
2^{14}	298	259.9	268.9	269.8	272.0	272.6	216.7	235.2	235.9	237.7	238.4
2^{15}	597	556.9	566.4	567.3	569.5	570.1	511.7	530.2	531.5	533.2	533.9

References

`https://eprint.iacr.org/2023/600`

Contact Information

- B. Biasioli: `beatrice.biasioli@tii.ae`
- C. Marcolla: `chiara.marcolla@tii.ae`