Parameter Exploration for Homomorphic Encryption Schemes Analysis.

Cyrielle FERON
Loïc LAGADEC
Vianney LAPOTRE

Plan

I – Introduction

II – PAnTHErS

III – Exploration

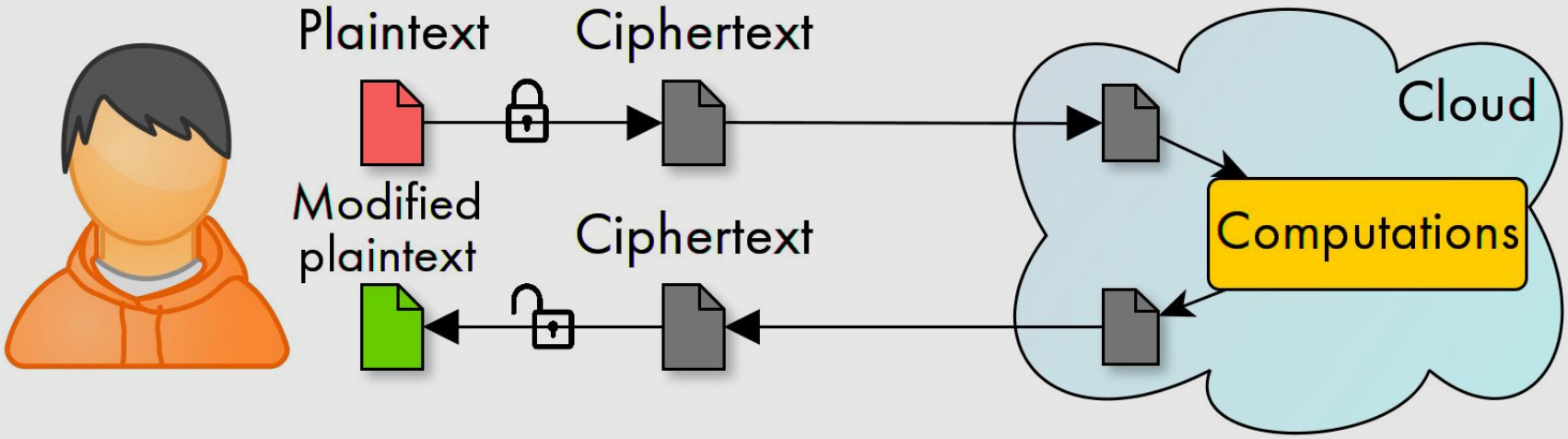
IV – Case study

V – Conclusion & future work

I – Introduction

1. Homomorphic Encryption (HE)
2. Related work
3. Main contribution

Introduction – *Homomorphic Encryption (HE)*



Homomorphic Encryption principle

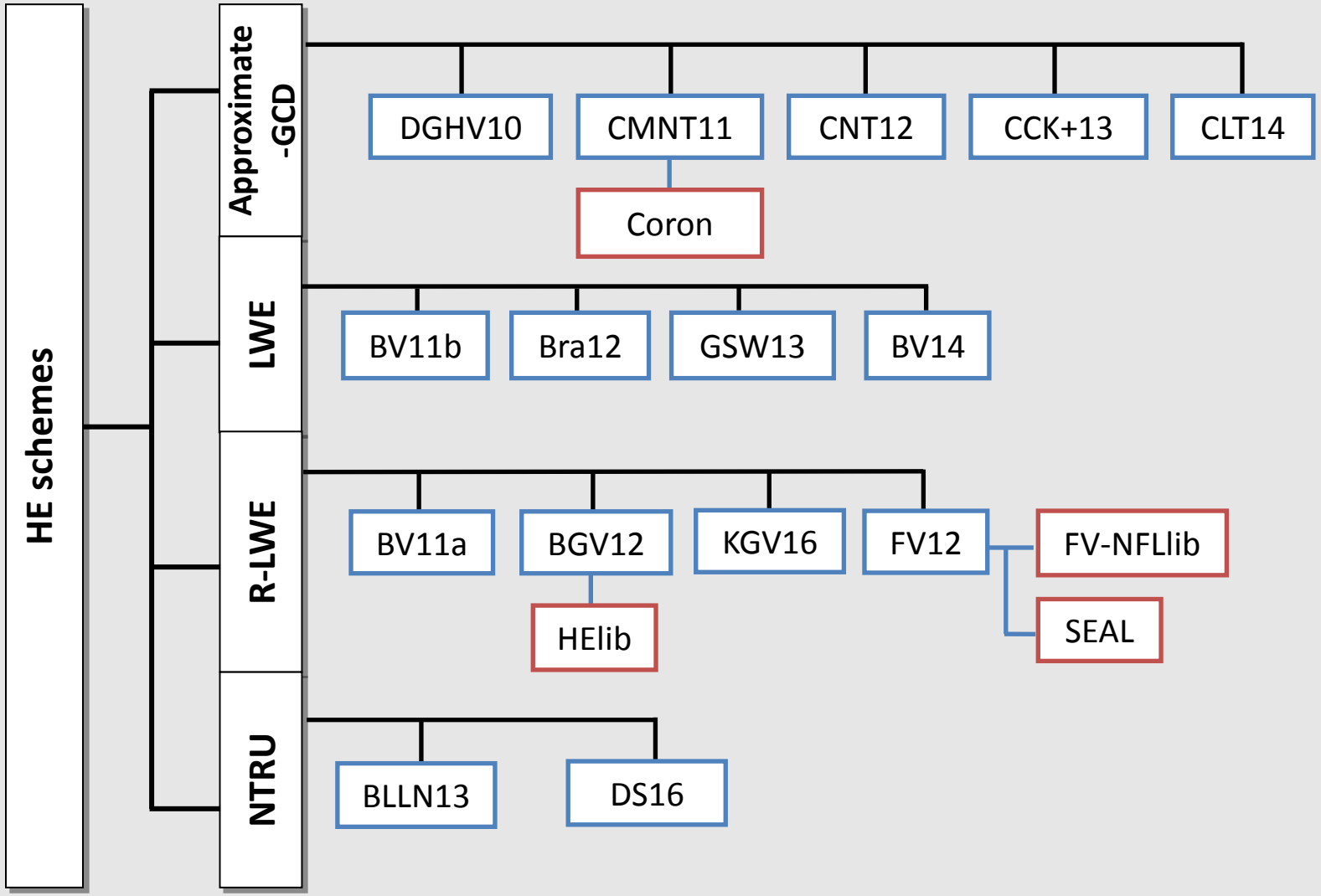
Advantages :

- No decryption in the Cloud.
- Data are secured during the whole process (transfers and computations).

Challenges :

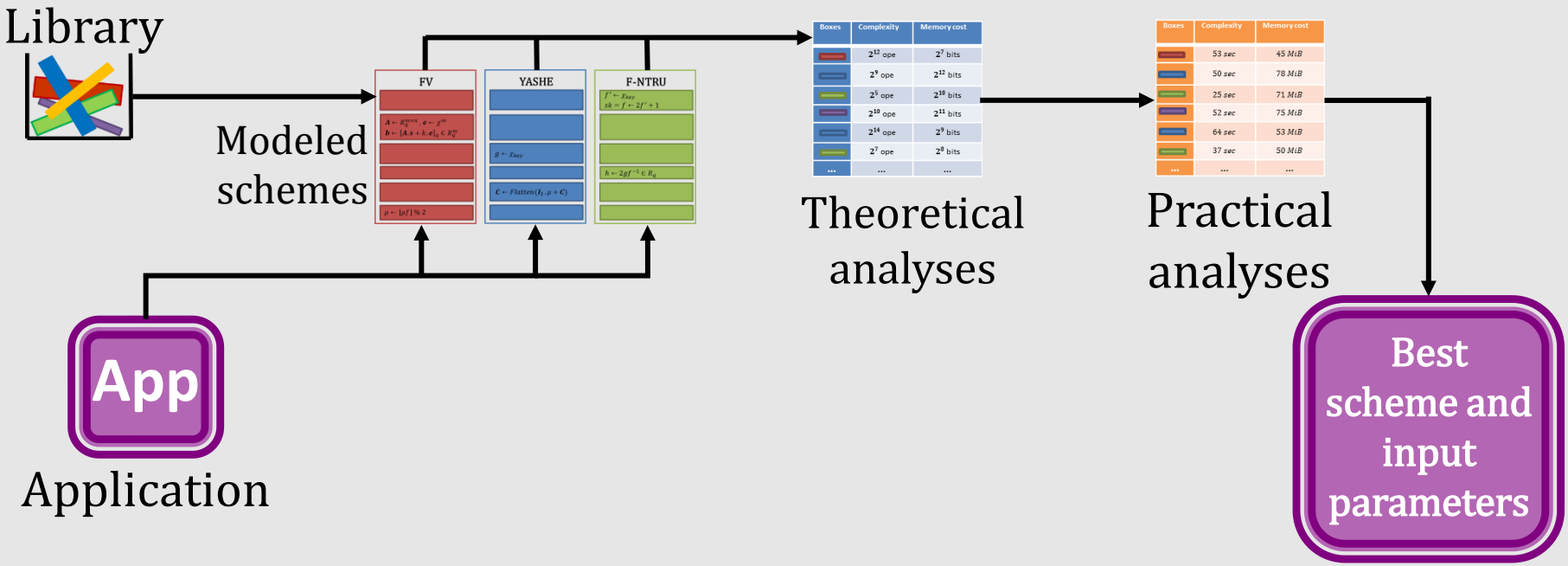
- Active research area
  ⇨ many HE schemes.
- Important complexity and memory consumption.
- Significant expansion factor.

Introduction – *Related work, Taxonomy*



Introduction – *Related work, PAnTHErS*

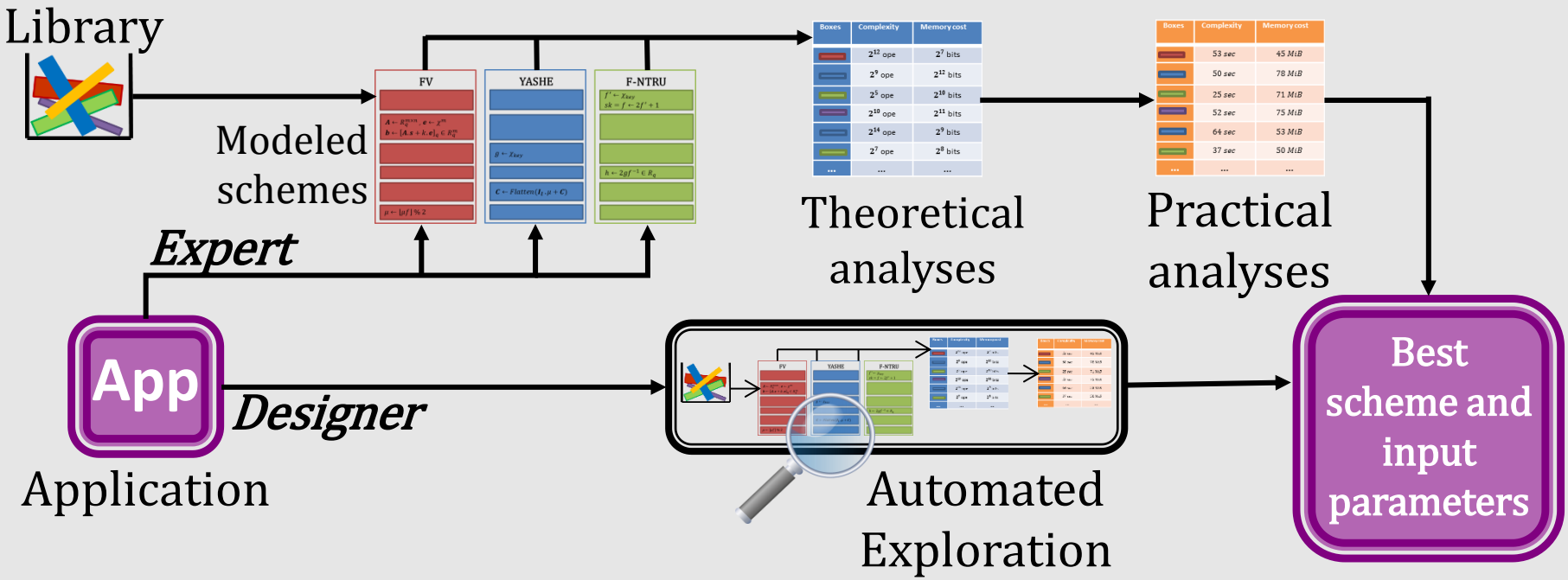
- **PAnTHErS** = Prototyping and Analysis Tool for Homomorphic Encryption Schemes
- Implemented in **Python**, using **Sage**.



Workflow of PAnTHErS

Introduction – *Main contribution*

- Extend PAnTHErS with an **automated exploration.**
- Allows **designer** to select the **most interesting HE scheme** and input parameter to use.

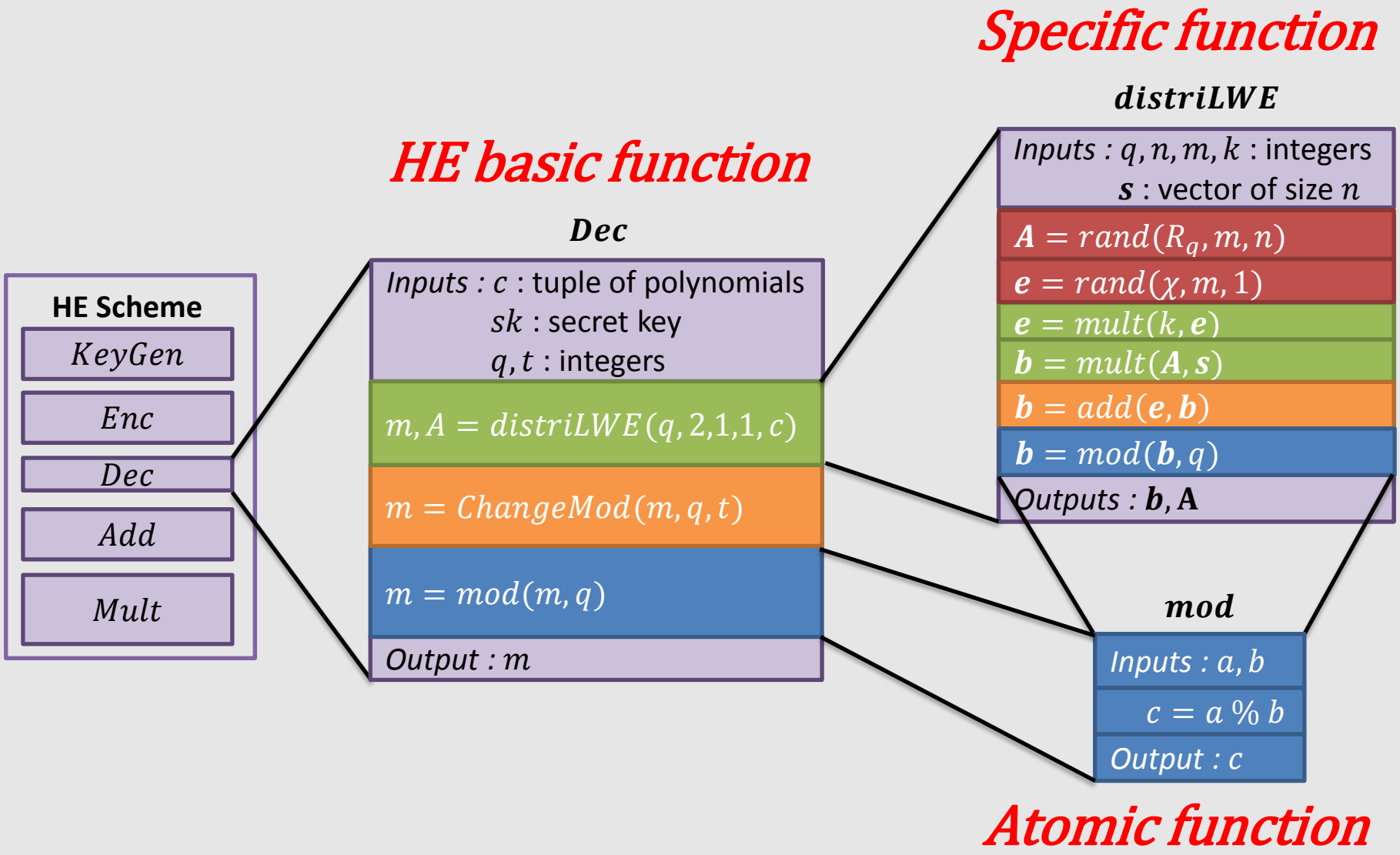


Workflow of PAnTHErS

II – PAnTHErS

1. Modeling
2. Analysis
3. Calibration
4. Interface

PAnTHErS – *Modeling*



PAnTHErS – *Analysis*

Complexity: number of operations performed.

Example:

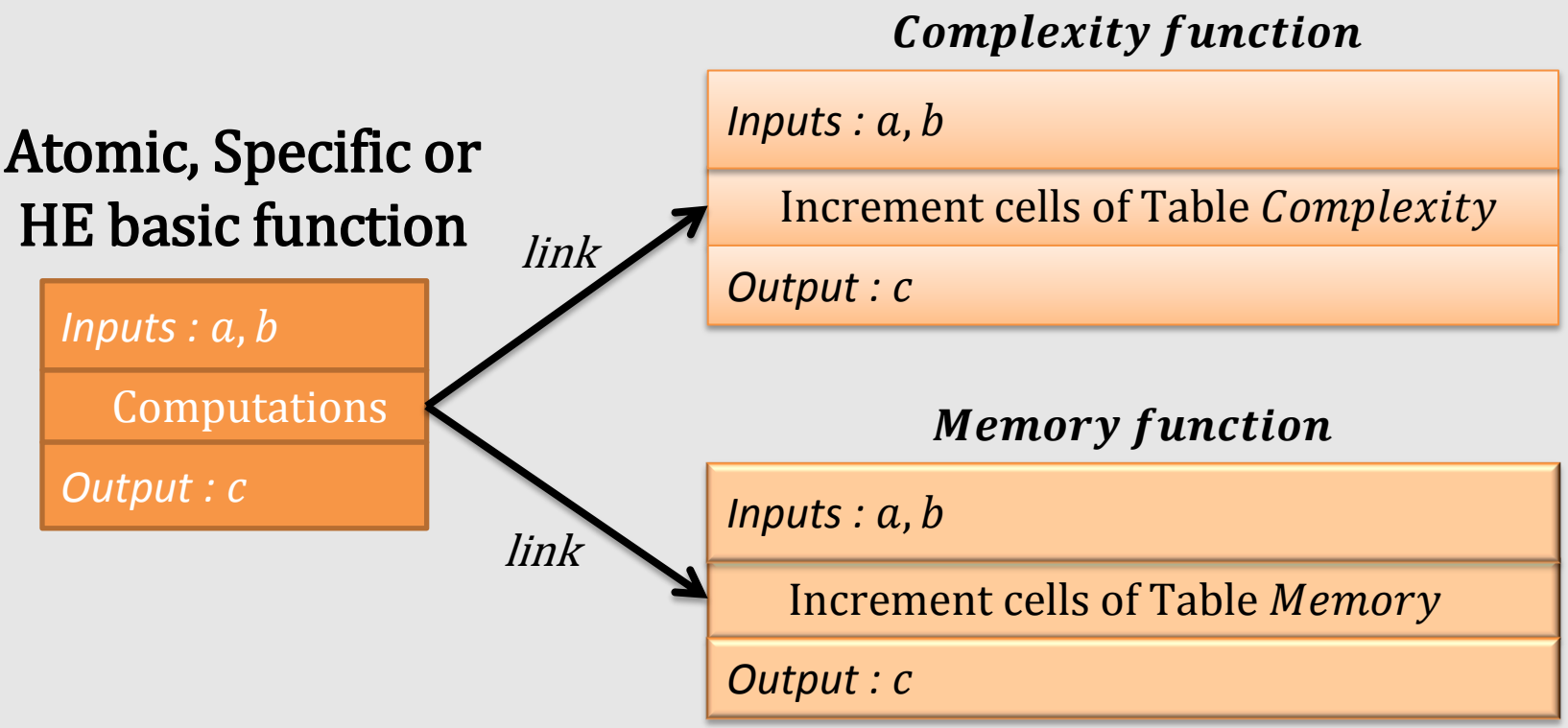
	MULT	ADD	DIV	MOD	RAND	ROUND
INT	$m \times d$	0	0	0	0	0
POLY	$m \times n$	$m \times n$	0	m	$(n+1).m$	0

Memory: characteristics of variables created.

Example:

Name	Rows	Cols	Type	Degree
$\boldsymbol{A}$	n	m	POLY	2048
$\boldsymbol{c}$	m	1	POLY	2048
$\boldsymbol{b}$	m	1	POLY	2048

PAnTHErS – *Analysis*



PAnTHErS – *Analysis*

Executable Scheme

HE Scheme

$p \leftarrow \left[\left[m \times \frac{c}{q}\right]\right] \% q$

$p \leftarrow p \% 2$

$A \leftarrow R_q^{m \times n}, e \leftarrow \chi^m$

$b \leftarrow [A.sk + k.e]_q$

$c \leftarrow \left(((c\%q))\%quotient\right)\%q$

$c \leftarrow Flatten(A, w, q)$

$sk \leftarrow \chi_{key}^{8 \times N}$

Keys: sk, pk, evk
Plaintext: m
Ciphertext: c

Execution time (sec)
Memory_profiler → MiB

Complexity Scheme

HE Scheme

$p \leftarrow \left[\left[m \times \frac{c}{q}\right]\right] \% q$

$p \leftarrow p \% 2$

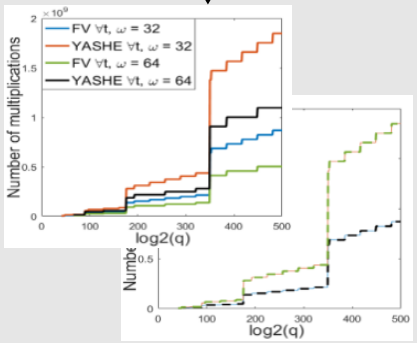
$A \leftarrow R_q^{m \times n}, e \leftarrow \chi^m$

$b \leftarrow [A.sk + k.e]_q$

$c \leftarrow \left(((c\%q))\%quotient\right)\%q$

$c \leftarrow Flatten(A, w, q)$

$sk \leftarrow \chi_{key}^{8 \times N}$



Memory cost Scheme

HE Scheme

$p \leftarrow \left[\left[m \times \frac{c}{q}\right]\right] \% q$

$p \leftarrow p \% 2$

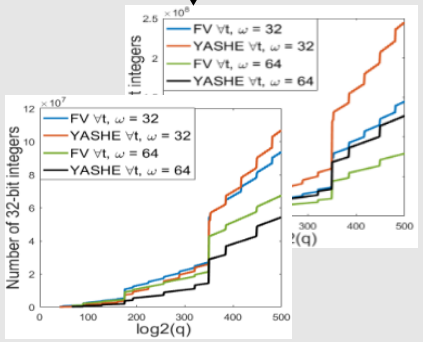
$A \leftarrow R_q^{m \times n}, e \leftarrow \chi^m$

$b \leftarrow [A.sk + k.e]_q$

$c \leftarrow \left(((c\%q))\%quotient\right)\%q$

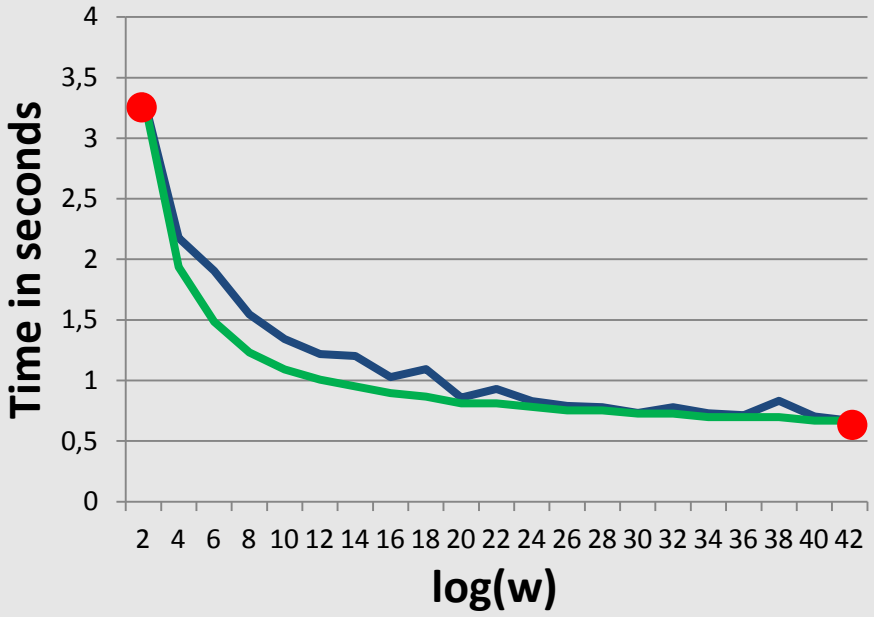
$c \leftarrow Flatten(A, w, q)$

$sk \leftarrow \chi_{key}^{8 \times N}$

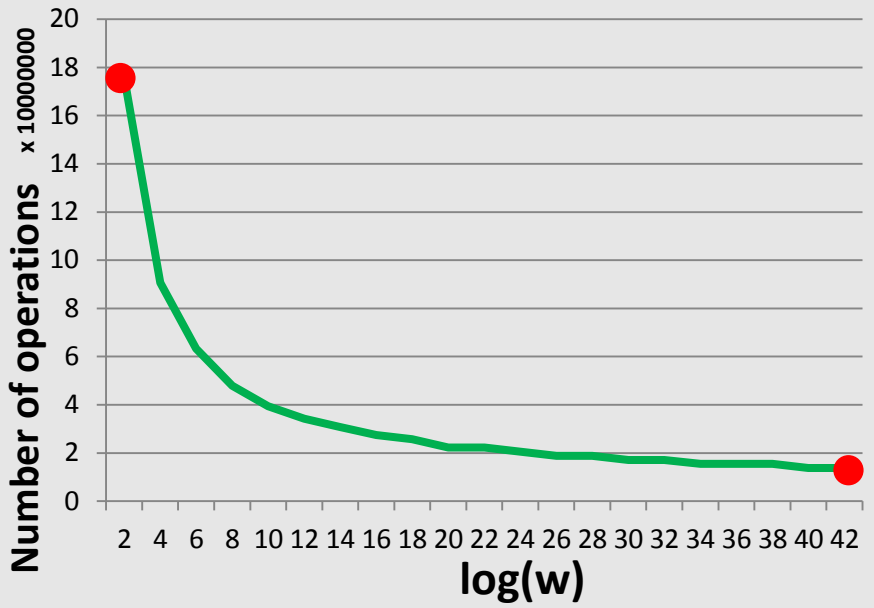


PAnTHErS – *Calibration*

FV execution times



FV complexities estimated by PAnTHErS



$$(2, yTime_2) = (2, yPanthers_2)$$

$$(42, yTime_{42}) = (42, yPanthers_{42})$$

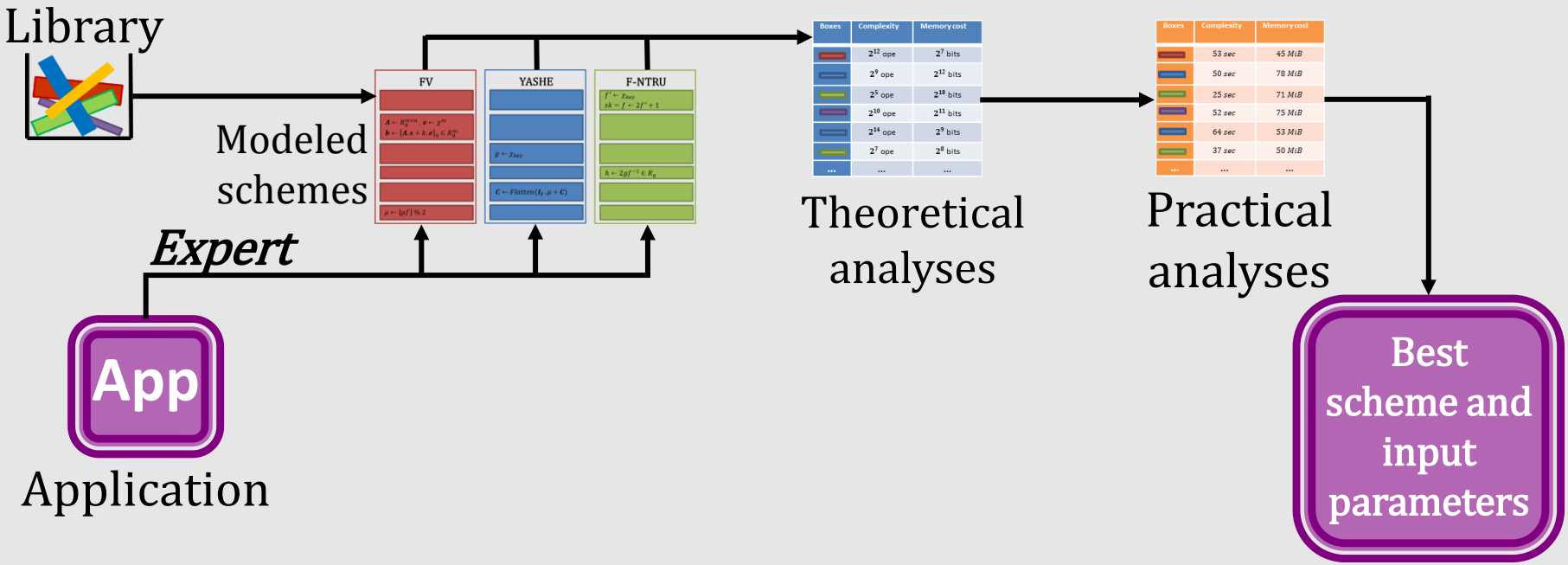
$$\exists a, b \; such \; as \quad \begin{cases} yTime_2 = a.yPanthers_2 + b \\ yTime_{42} = a.yPanthers_{42} + b \end{cases}$$

Tests on a pedagogic application which has 10 HE Mult and 6 HE Add.

Table : Results *for one parameter variation for 3 HE schemes.*

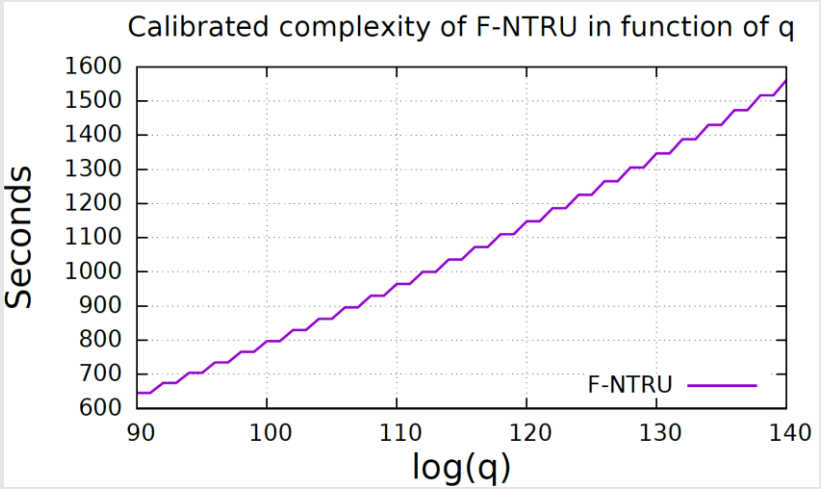
p	2	3
p-calibration time	72 min	111 min
All execution times	2489 min	2489 min
Speedup	34.6	22.4
Mean % of error	5,1 %	4,5 %

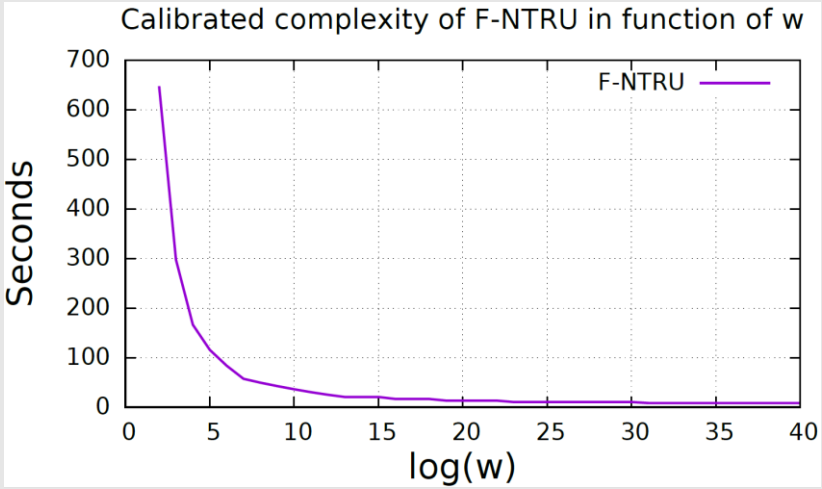
PAnTHErS – *Recap*



PAnTHErS – *Interface*

Choose analysis	Choose one application	Choose one scheme	Fill parameters variation	Analysis
☒ Complexity □ Memory cost	□ App1 ☒ App2 □ App3	□ FV □ YASHE ☒ FNTRU	$\log(q)$ = 90 to 140 by 1 $\log(w)$ = 2 to 40 by 1	Start





Exploration

1. 7 steps of exploration
2. Recap

Exploration – *7 steps of exploration*

1. App 1 / App 2 / App 3

Select one application of depth d

2.

$log(q)$	$log(w)$	t	Depth
100	2	2	10
102	3	5	9
214	3	7	14
110	9	9	12
190	2	3	14
325	5	2	14
200	10	9	8
...	...	...	...

Find every sets of parameters implying a depth of d

3. 

Analyze the sets with PAnTHErS

4. 

Execute application with some sets

5. 

Calibrate the others sets

6. 

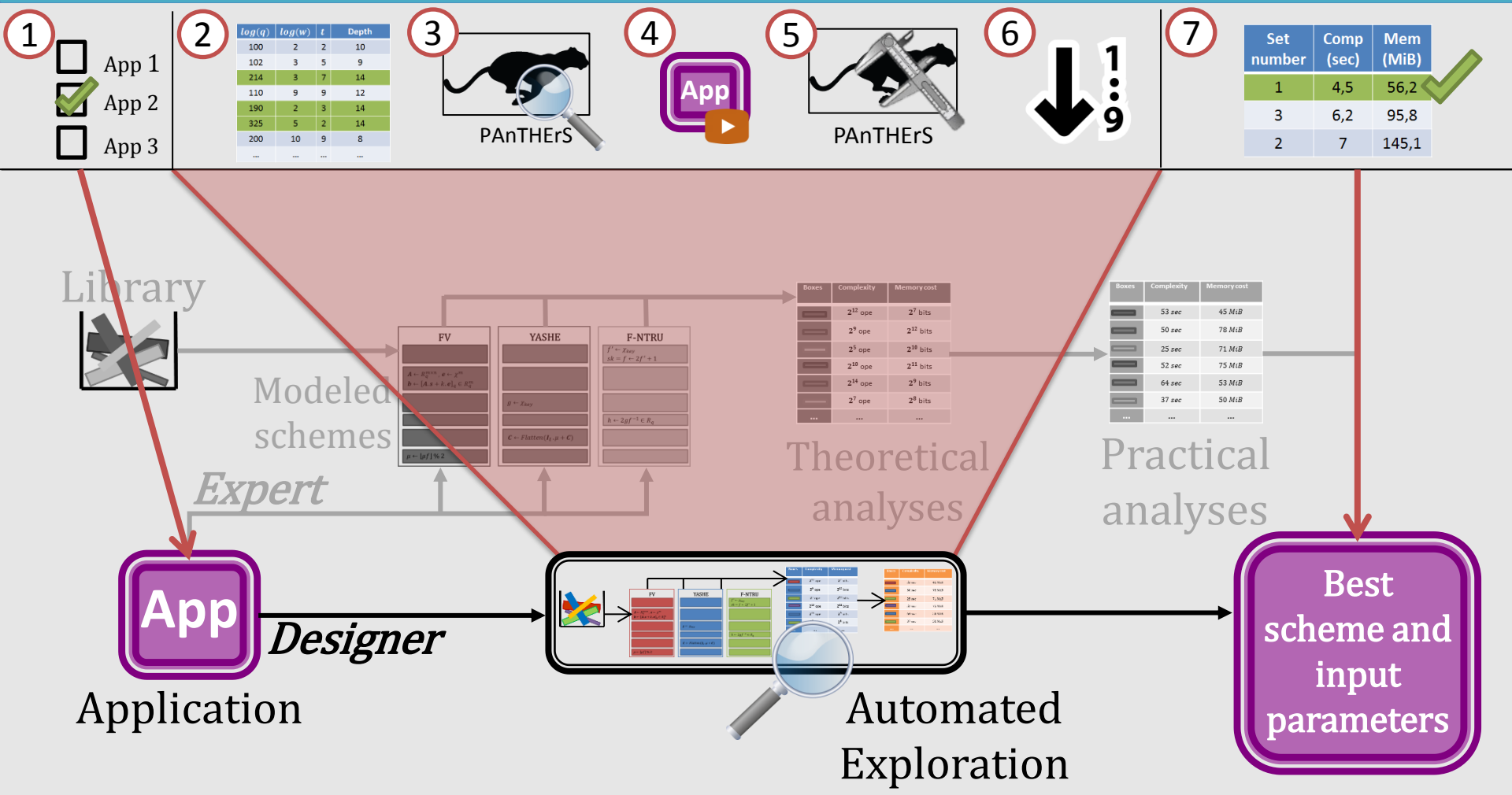
Sort the sets depending on calibration results using Pareto efficiency

7.

Set number	Comp (sec)	Mem (MiB)
1	4,5	56,2
3	6,2	95,8
2	7	145,1

Find the most interesting sets

Exploration – *Recap*



IV – Case study

1. Pedagogic application
2. Expert path
3. Designer path

Case study – *Pedagogic application*

Plaintexts: m_1, m_2, m_3

Encryption:

$$c_1 = Enc(m_1), c_2 = Enc(m_2), c_3 = Enc(m_3)$$

Computations:

$$c = c_1^3 \cdot c_2^2 \cdot c_3^2 \cdot S \cdot T \cdot (S + c_3)(S + c_2 + c_3)$$

with $S = c_1 \cdot T + c_1 + c_2$ and $T = c_1 \cdot c_2 + c_3$

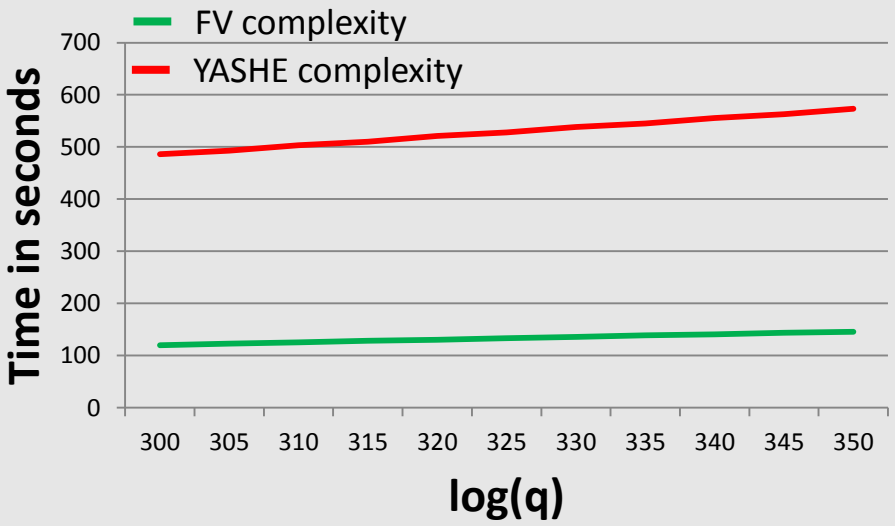
Decryption:

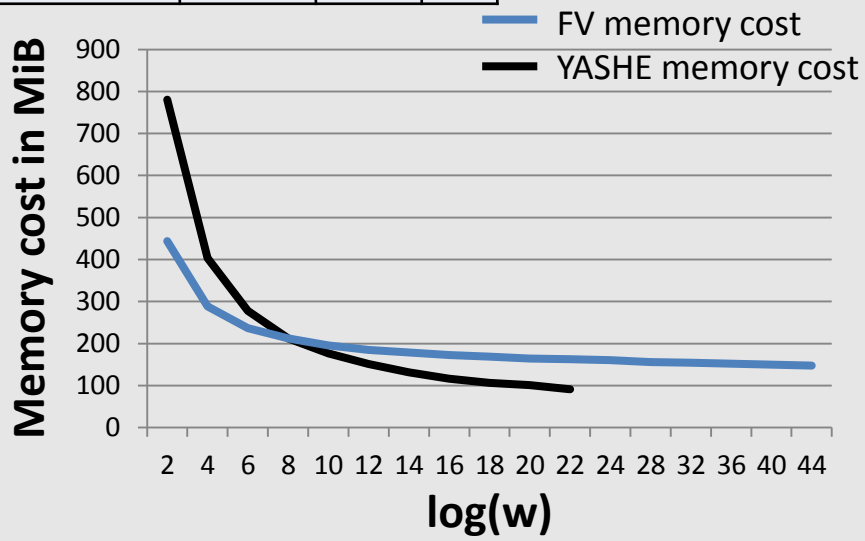
$$m = Dec(c)$$

Which **scheme** is the **most appropriate** for the application ? And which **input parameters** ?

Case study – *Expert path*

Scheme (Comp)	$\log_2(q)$			w	t
	Min	Max	Step		
FV and YASHE	300	350	1	2^2	2
Scheme (Mem)	$\log_2(w)$			q	t
	Min	Max	Step		
FV	2	44	4	300	2
YASHE	2	22	2	300	2





Most interesting : **FV** with $q = 2^{300}, w = 2^{28}, t = 2$

Case study – *Designer path*

Choose analysis	Choose one application	Choose one scheme	Fill parameters variation	Analysis
□ Complexity □ Memory cost ☒ Exploration	□ App1 ☒ App2 □ App3	☒ FV ☒ YASHE ☒ FNTRU	Every sets of parameters for each scheme	Start

Most interesting : **FV** with $q = 2^{339}, w = 2^{68}, t = 2$

	Designer's parameters $q = 2^{339}, w = 2^{68}, t = 2$	**Expert's parameters** $q = 2^{300}, w = 2^{28}, t = 2$
Estimation	12,03 sec and 74,65 MiB	12,27 sec and 90,22 MiB
Execution	10,26 sec and 75,80 MiB	10,77 sec and 84,40 MiB

V – Conclusion & future work

Conclusion

- **HE expert** can use PAnTHErS to **analyze HE schemes** and thus applications.
- **Interface** makes easier PAnTHErS **usage**.
- **Designer path** allows non experts to **select one scheme** and input parameters for one chosen application.

Future work

- Actual **application** analysis (e.g. medical).
- **Fast comparison** of available HE scheme implementation using the proposed calibration method.
- Analysis of **hardware** acceleration.

Thanks

Cyrielle FERON

Loïc LAGADEC

Vianney LAPOTRE

ENSTA Bretagne

Université Bretagne Sud

ubs

References:

[1] Feron, C., Lapotre, V. and Lagadec, L. (2017). PAnTHErS: A Prototyping and Analysis Tool for Homomorphic Encryption Schemes. *14th International Joint Conference on e-Business and Telecommunications* (ICETE 2017), Volume 4: SECRYPT, p. 359-366.

[2] Doröz, Y. and Sunar, B. (2016). Flattening NTRU for evaluation key free homomorphic encryption. *IACR Cryptology ePrint Archive*, 2016:315.

[3] Fan, J. and Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*, 2012:144.

[4] Gentry, C., Sahai, A., and Waters, B. (2013). Homomorphic Encryption from Learning with Errors: Concep-tually-Simpler, Asymptotically-Faster, Attribute-Based. In *Proc. CRYPTO*, pages 75–92, Santa Barbara, CA, USA.

[5] Khedr, A., Gulak, P. G., and Vaikuntanathan, V. (2016). SHIELD: Scalable Homomorphic Implementation of Encrypted Data-classifiers. *IEEE Trans. Computers*, 65(9):2848–2858.

[6] Bos, J.W., Lauter, K. E., Loftus, J., and Naehrig, M. (2013). Improved Security for a Ring-Based FHE Scheme. In *Proc. Cryptography and Coding IMA*, pages 45–64, Oxford, UK.

[7] Carpov, S., Nguyen, T. H., Sirdey, R., Constantino, G., & Martinelli, F. (2016, June). Practical Privacy-Preserving Medical Diagnosis Using Homomorphic Encryption. In *Cloud Computing (CLOUD), 2016 IEEE 9th International Conference on* (pp. 593-599). IEEE.