TFHE Functional bootstrapping over multiple inputs

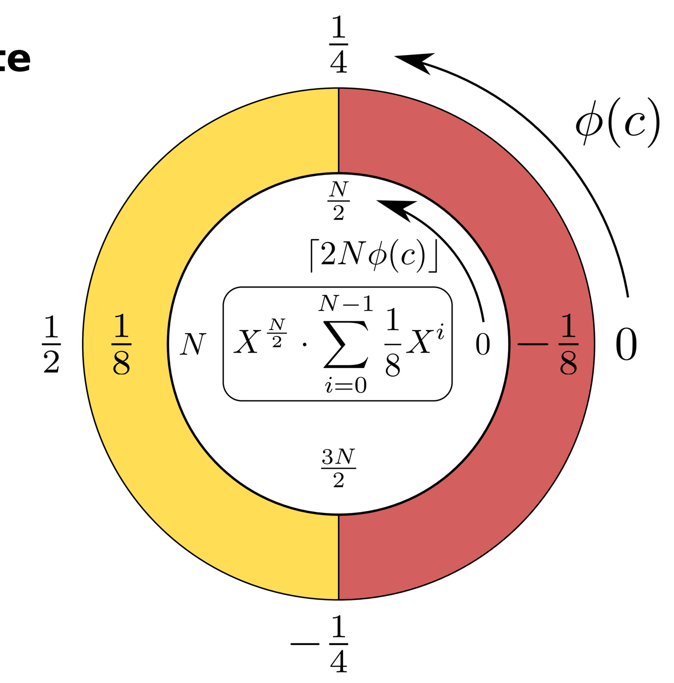
Pierre-Emmanuel Clet, Aymen Boudguiga, Renaud Sirdey

Binary TFHE

Any boolean circuit can be built from a combination of additions and bootstrappings

Example: TFHE AND Gate

Bit	Encoding
0	$-\frac{1}{8}$
1	$\frac{1}{8}$



$[x]$ = Encryption of x

$b_1, b_2 \in \{0,1\}$

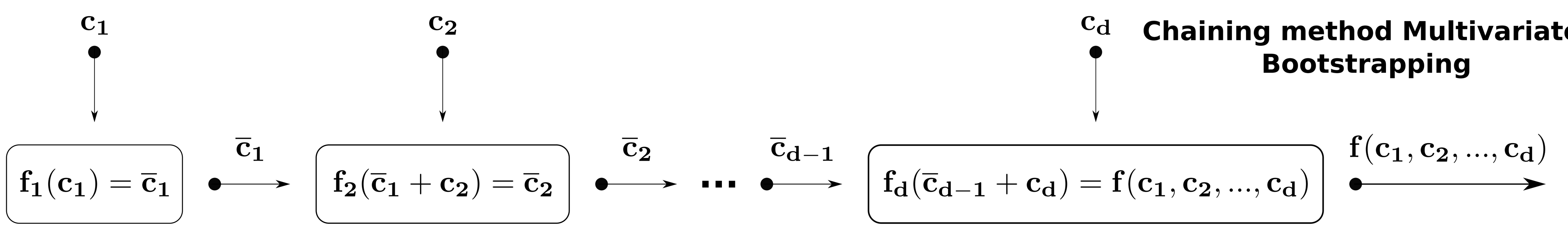
$c = [b_1] + [b_2] + \frac{1}{8}$

Non-binary TFHE (base B>2)

Polynomial functions:
Can be computed with the usual homomorphic additions and multiplications

Univariate functions:
Can be computed with a *functional/programmable* bootstrapping [Cle+22]

Multivariate functions:
- Any function can be computed with the *tree-based method* from [GBA21]
- Specific functions can be computed with the *chaining method* from [GBA21]:



Chaining method Multivariate Bootstrapping

Tree-based method

Tree-based method from [GBA21]:
- Depth grows with number of inputs
- Width grows with basis B and depth of tree

Noise variance: $d \cdot \mathcal{E}_{BR} + (d-1) \cdot \mathcal{E}_{KS}^{TRLWE} + \mathcal{E}_{KS}^{TLWE}$

$$\mathcal{E}_{BR} = n \cdot ((k+1)lN\vartheta_{BK}(\frac{Bg}{2})^2 + (1+kN) \cdot \frac{Bg^{-2l}}{12})$$

$$\mathcal{E}_{KS}^{TRLWE} = N^2 \cdot (t\vartheta_{KS}(\frac{base}{2})^2 + \frac{base^{-2t}}{12})$$

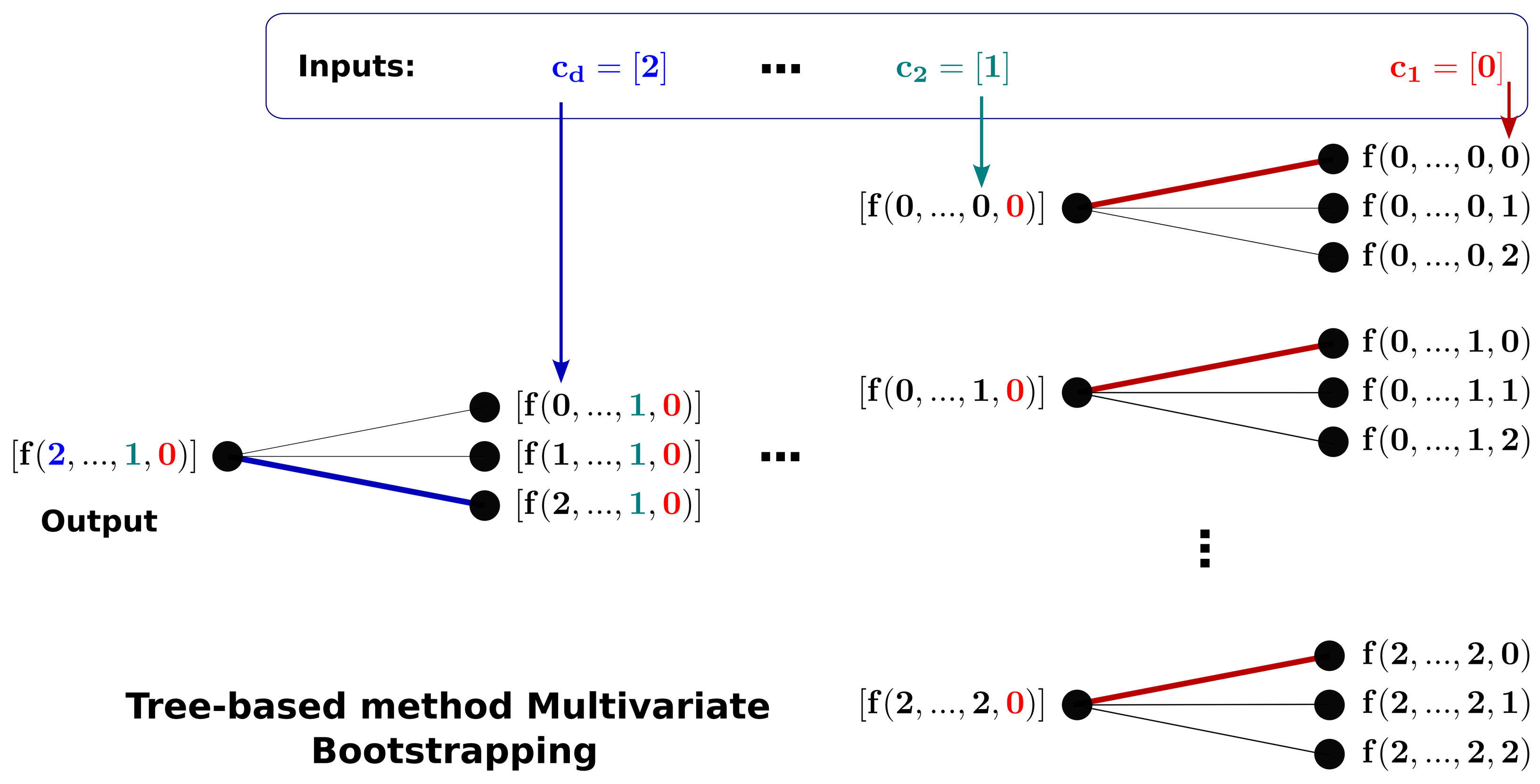
$$\mathcal{E}_{KS}^{TLWE} = N \cdot (t\vartheta_{KS}(\frac{base}{2})^2 + \frac{base^{-2t}}{12})$$

(-) Low composability of deep trees due to output noise

(-) Exponential computation time in number of inputs: $\mathcal{O}(B^d)$

(+) Composability can be improved with intermediary bootstrappings

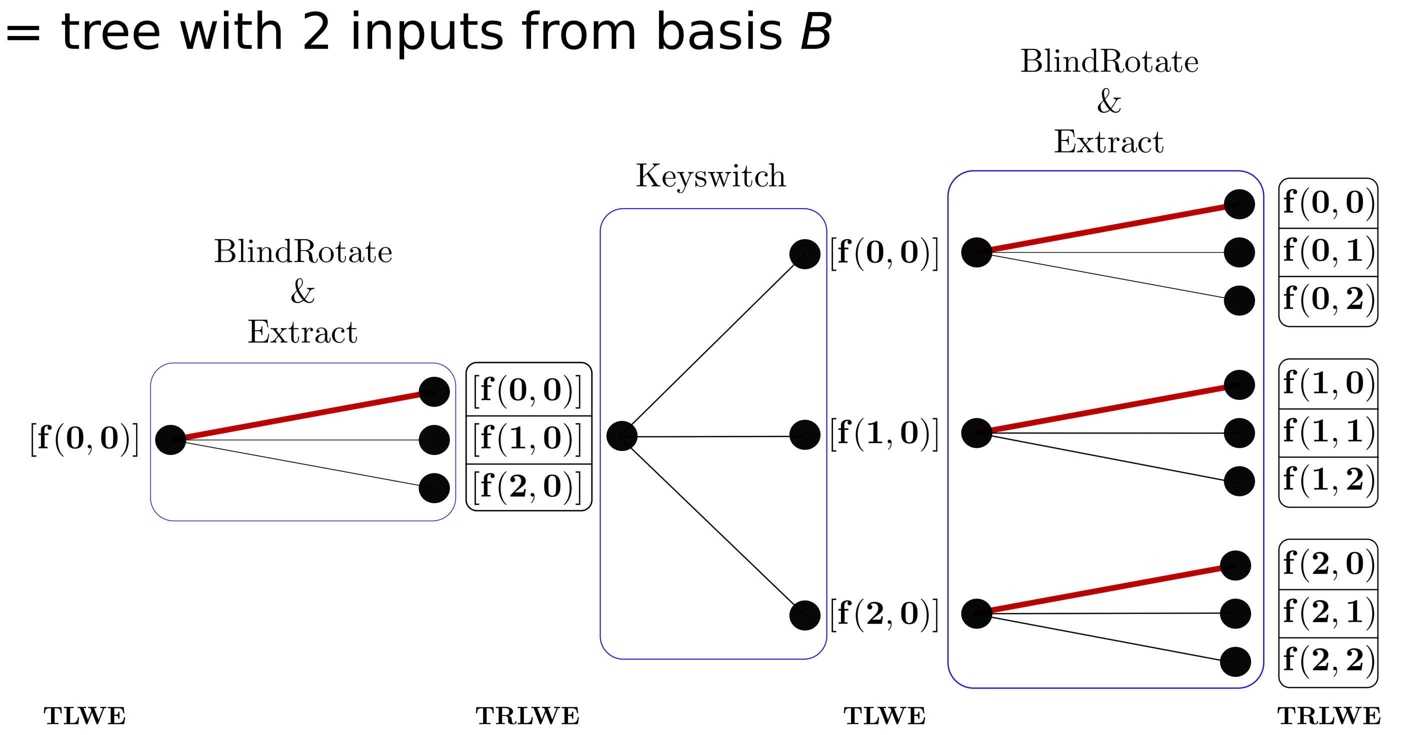
(+) Any function can be implemented with this method



Tree-based method Multivariate Bootstrapping

B-gates

B-gate = tree with 2 inputs from basis *B*



Specific TRLWE Keyswitch

Standard keyswitch keys: $\forall i \in [\![1,n]\!], j \in [\![1,t]\!], \frac{s_i}{base^j}$

Keyswitch noise: $n \cdot \boxed{N} \cdot (t \cdot \vartheta_{KS}(\frac{base}{2})^2 + \frac{base^{-2t}}{12})$

Specific keyswitch key: $\forall i \in [\![1,n]\!], j \in [\![1,t]\!], \sum_{k=0}^{\frac{N}{B}-1} \frac{s_i}{base^j} \cdot X^k$

Keyswitch noise: $n \cdot \boxed{B} \cdot (t \cdot \vartheta_{KS}(\frac{base}{2})^2 + \frac{base^{-2t}}{12})$

Improvement:
Our specific key lowers the output noise by a factor $\frac{N}{B}$

Building circuits

Use *B*-gates to create any logic circuit for any function with inputs in basis *B*

(+) Better efficiency than binary TFHE: less operations thanks to the use of a larger decomposition basis *B*

Circuit generation:

1st approach: Lupanov general circuit [LS11]

(+) Low noise variance

(-) Exponential computation time: $\mathcal{O}(\frac{B^d}{d})$

2nd approach: implement *dedicated* circuits per functions

(+) Flexibility of circuits allows for better performances

(-) Need to craft efficient non binary circuit

Performances

Example: sorting 4 inputs in base B=8
Circuit: bubble sort

n	N	σ	l	Bg_{bit}	t	$base_{bit}$
1250	2048	$4.1 \cdot 10^{-10}$	2	10	1	15

Parameters' set ($\lambda = 128$)

Circuit	Tree-based method
4.8s	94.8s

Time in seconds with 4 inputs and B= 8

References

[LS11] Sergei Lozhkin and Alexander Shiganov. On a Modification of Lupanov's Method with More Uniform Distribution of Fan-out." In: Electronic Colloquium on Computational Complexity (ECCC) 18 (Jan. 2011), p. 130.

[GBA21] Antonio Guimarães, Edson Borin, and Diego F. Aranha. "Revisiting the functional bootstrap in TFHE". In: IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (Feb. 2021), pp. 229–253. doi: 10.46586/tches.v2021.i2.229-253. url: https://tches.iacr.org/index.php/TCHES/article/view/8793.

[Cle+22] Pierre-Emmanuel Clet, Martin Zuber, Aymen Boudguiga, Renaud Sirdey, and Cédric Gouy-Pailler. Putting up the swiss army knife of homomorphic calculations by means of TFHE functional bootstrapping. Cryptology ePrint Archive, Paper 2022/149. https://eprint.iacr.org/2022/149.

[Chi+19] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "TFHE: Fast Fully Homomorphic Encryption Over the Torus". In: Journal of Cryptology 33 (Apr. 2019). doi: 10.1007/s00145-019-09319-x.

Contact:
pierre-emmanuel.clet@cea.fr

cea list