Fheanor: a new, modular FHE library for designing and optimising schemes [OPP25]

Hiroki Okada[1,2], Rachel Player[3], and Simon Pohmann[3]

[1]KDDI Research [2]The University of Tokyo [3]Royal Holloway, University of London

Our contribution: Fheanor

- Rust library for FHE
- Open-Source
- Contributions welcome
- Design mirrors mathematical structure of HE schemes
- Modular, configurable
- Good performance

⇒ Perfect for research!

BFV/BGV Library Comparison

Library		BGV	BFV	CLPX	bootstrapping	general m
HElib	C++	✓	✗	✗	✓	✓
OpenFHE	C++	✓	✓	✗	✗	✗
Seal	C++	✓	✓	✗	✗	✗
Lattigo	Go	✓	✓	✗	✗	✗
$\Lambda \circ \lambda$	Haskell	✓	✓	✗	✗	✓
Fheanor	Rust	✓	✓	✓	✓	✓

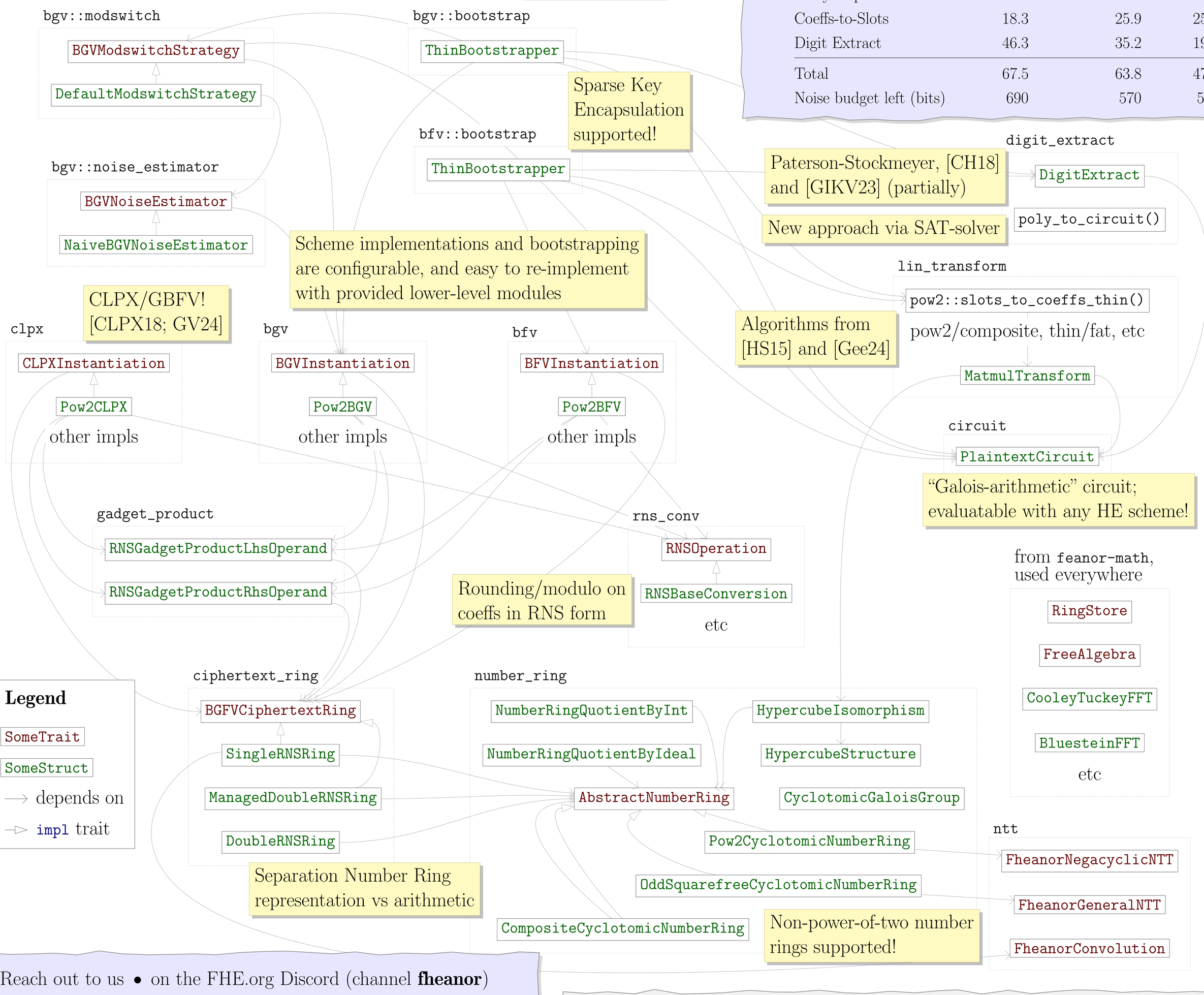
Performance I: SHE

(binary mult. tree, 16 inputs, 15 mults)

$(m, \log_2(q), c)$	SEAL	Lattigo	HElib	Fheanor	
$(21845, 425, 3)$			1.6 s	0.9 s	BGV
$(2^{16}, 855, 3)$			2.3 s	1.8 s	BGV
$(42799, 1115, 3)$			6.7 s	4.6 s	BGV
$(2^{16}, 855, 4)$	1.4 s	0.53 s		1.6 s	BGV
$(2^{17}, 1710, 4)$	9.7 s	3.1 s		9.5 s	BGV
$(2^{16}, 855, 4)$	2.9 s	1.6 s		5.4 s	BFV
$(2^{17}, 858, 4)$	19.1 s	9.5 s		28.0 s	BFV

Performance II: BGV bootstrapping

$(m, t, \log_2(q), c, h(s), v)$ $= (42799, 4, 1120, 10, 128, 8)$	HElib	Fheanor	
		Prior digit extraction	New digit extraction
Slots-to-Coeffs	2.6	1.5	1.5
Noisy Expansion	0.27	1.2	1.2
Coeffs-to-Slots	18.3	25.9	25.9
Digit Extract	46.3	35.2	19.2
Total	67.5	63.8	47.8
Noise budget left (bits)	690	570	591



Reach out to us
- on the FHE.org Discord (channel **fheanor**)
- at **simon@pohmann.de**

Acknowledgements

We thank Seonhong Min, Robin Geelen, Jannik Spiessens, Jiayi Kang and Frederik Vercauteren for fruitful discussions. Simon Pohmann was supported by the EPSRC and the UK Government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/S021817/1). Parts of this research were conducted while Simon Pohmann was an invited researcher at KDDI Research, supported by the International Exchange Program of the National Institute of Information and Communications (NICT).

References

[CH18] H. Chen and K. Han. "Homomorphic Lower Digits Removal and Improved FHE Bootstrapping". 2018, pp. 315–337.

[CLPX18] H. Chen, K. Laine, R. Player, and Y. Xia. "High-Precision Arithmetic in Homomorphic Encryption". 2018, pp. 116–136.

[Gee24] R. Geelen. "Revisiting the Slot-to-Coefficient Transformation for BGV and BFV". In: *Communications in Cryptology* 1.3 (2024), p. 37.

[GIKV23] R. Geelen, I. Iliashenko, J. Kang, and F. Vercauteren. "On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption". 2023, pp. 257–286.

[GV24] R. Geelen and F. Vercauteren. *Fully Homomorphic Encryption for Cyclotomic Prime Moduli*. 2024.

[HS15] S. Halevi and V. Shoup. "Bootstrapping for HElib". 2015, pp. 641–670.

[OPP25] H. Okada, R. Player, and S. Pohmann. *Fheanor: a new, modular FHE library for designing and optimising schemes*. 2025.