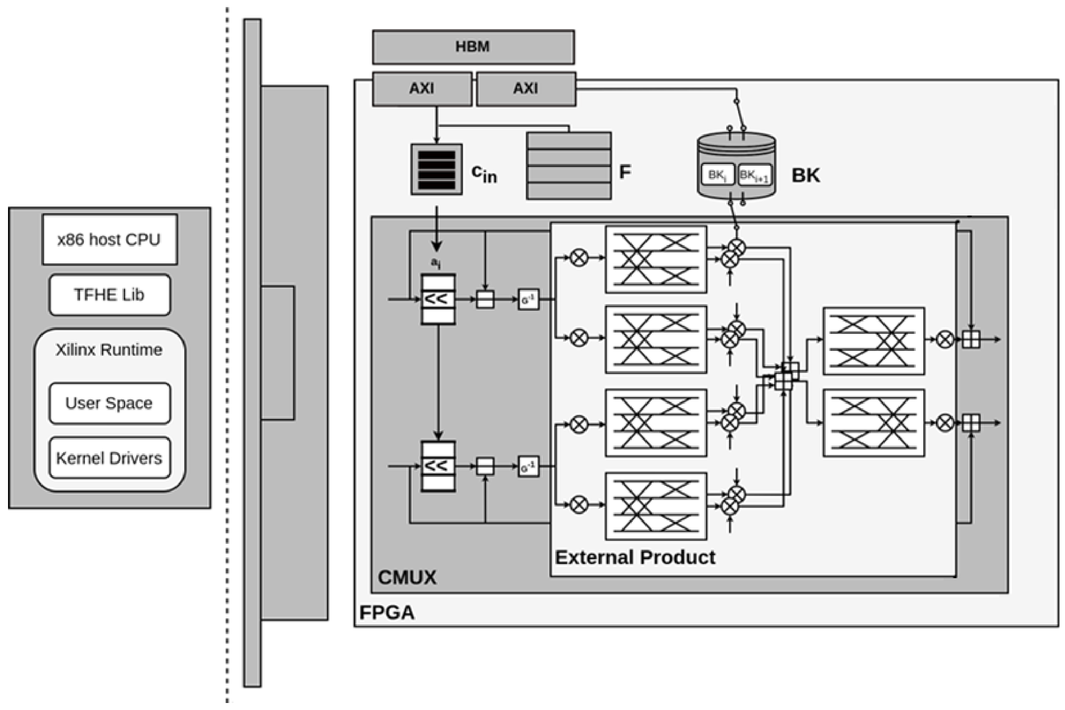
BELFORT

TFHE Acceleration for your Application

FPGA HW Acceleration for TFHE

- Integrated in TFHE-rs and Amazon Cloud
- Based on FPT [FHE.org 2023, ACM CCS 2023]



New features

- Ready for any application
- Support both keyswitch and bootstrap
- Support arbitrary parameter sets
- Improved hardware and interfaces
- Multi-FPGA support

Demonstrator

- Trivium transciphering
- Usecase:
  - Random number generation
  - Convert from symmetric key encryption to FHE
- Ask for a live demonstration!

```
$ ./demo_w_fpga 4-FPGAS
0 F4CD954A717F26A7 44.543053ms
1 D6930830C4E7CF08 44.475535ms
2 19F80E03F25F342C 52.332324ms
3 64ADC66ABA7F8A8E 43.690261ms
4 6EAA49F23632AE3C 44.525798ms
5 D41A7BD290A0132F 44.626038ms
6 81C6D4043B6E397D 44.083890ms
```

```
$ ./demo_wo_fpga 1-THREAD
0 F4CD954A717F26A7 14.595640243s
1 D6930830C4E7CF08 14.5496858885
2 19F80E03F25F342C 14.844905742s
3 64ADC66ABA7F8A8E 15.0278382125
4 6EAA49F23632AE3C 14.080456796s
5 D41A7BD290A0132F 13.9501346585
6 81C6D4043B6E397D 13.9059674745
7 7388F3A03B5FE358 13.964203910s
```

>300×

COSIC KU LEUVEN erc

Speedup . . .

- 123x speedup (one FPGA vs one thread CPU)
- 1.000x speedup early 2025
- Trivium decryption (64 bits):

Target	Execution Time	Relative Time
SW | 1 thread Intel Xeon Silver 4208	14.25 sec	1x
SW | 16 threads Intel Xeon Silver 4208	2.57 sec	5.5x
Our HW (FPGA) | 1 FPGA AMD Alveo U55C	0.116 sec	123x
Our HW (FPGA) | 4 FPGAs AMD Alveo U55C *x4*	0.044 sec	324x
Our HW (FPGA) | 1 FPGA Target next year	0.014 sec	1.000x
Our Dedicated Chip Target 2 years	0.0014 sec	10.000x

… is also a cost reduction

Estimated cost reduction through BELFORT:

- 4.3x now
- 34x early 2025

Target	Cost/ 1M ops	Cost Reduction
CPU AWS hpc7a .96xlarge	$ 0.16	1x
FPGA (our design) AWS f1.2xlarge	$ 0.038	4.3x
Our HW (FPGA) Target next year	$ 0.0047	34x

Future

- Speedup to 10.000x
- Integrate into various FHE libraries
- Integrate into your application

For more information

Ingrid Verbauwhede
info@belfort.eu
https://www.belfort.eu