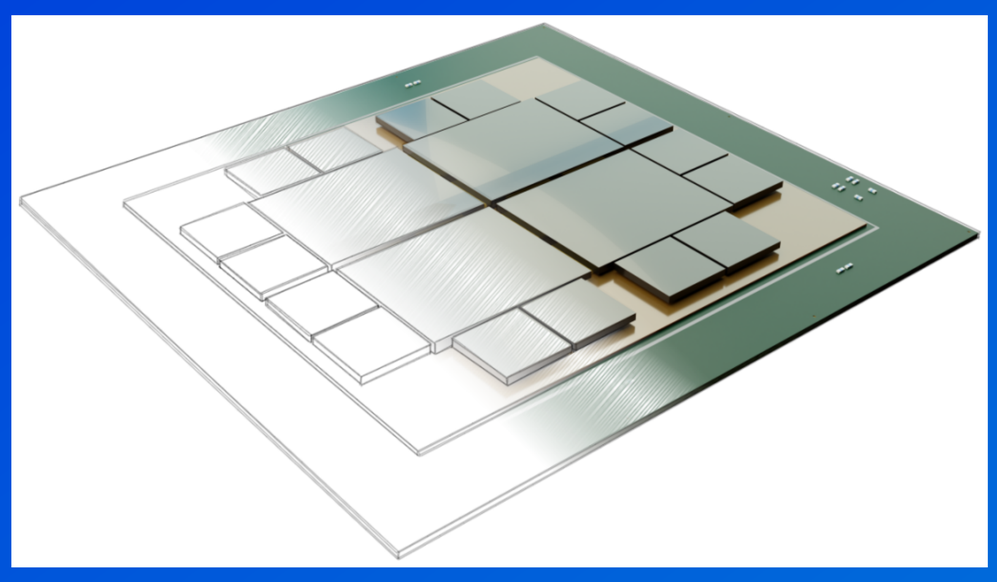
The Optalysys Etech: Optical accelerators for FHE

Optalysys

https://www.optalysys.com



We are developing an optical accelerator for Fourier- and NTT-based computations to bring FHE close to real-time

Optical Fourier transform: Under some conditions, light propagation 'computes' a Fourier transform. (Example: propagation between the two focal planes of an ideal lens.)

Advantages:

* low latency - the calculation happens literally at the speed of light
* low power usage (light propagation is an energy-preserving process)
* fully parallelizable

Target: 10,000× acceleration over state of the art CPU implementations

Planned interfaces with TFHE-rs (https://www.tfhe.com/) and OpenFHE (https://www.openfhe.org/) for acceleration of TFHE, BGV, B/FV, and CKKS schemes

FPGA-based beta systems

March 2023: In-silicon Fourier Transform optical cavity

April 2023 beta system:
1 FPGA + 1 optical core

Aim: Demonstrate the use of the OFT for FHE

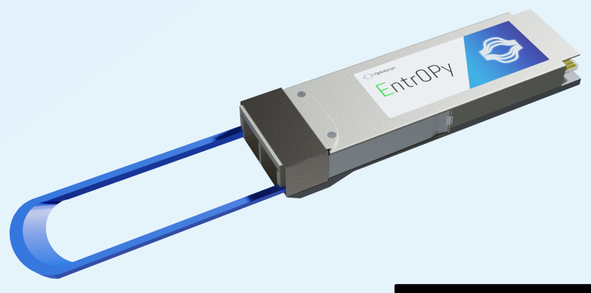
Target acceleration over CPU: 2× to 5×
Limited by number of optical cores and optics / FPGA interface

Operations implemented: TFHE CMUX, some leveled CKKS operations

September 2023: Entropy pluggable: Transceiver form factor

4× Optical cores
+ Silicon Photonics interface
+ Digital / Electronic interface

Accelerate Optical <> Electronic information transfer



End 2023 beta system:
FPGA platform + 64 optical cores

Aim: Optimised accelerator for low- to mid-intensity FHE computation

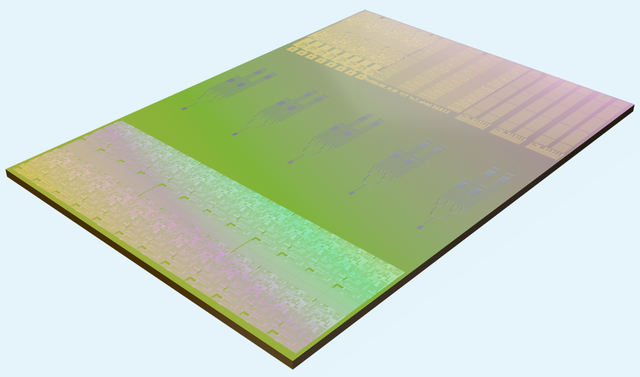
Target acceleration over CPU: 250×

Operations implemented: Full TFHE bootstrapping, full CKKS leveled operations

Interested in our accelerator program?
Contact us for early access to the beta systems!

info@optalysys.com

Beyond FPGAs : towards real-time FHE

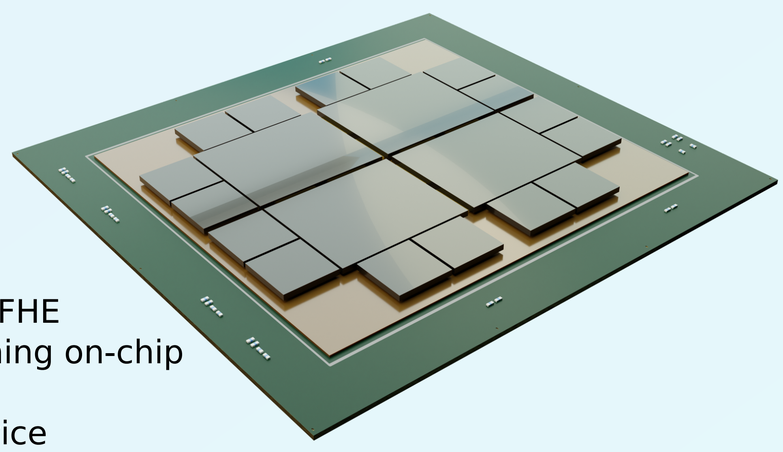


Etile: Integrated optical / SiPh chiplet

Enable: Multi-chip module solution for FHE acceleration

16× Etile chiplets + 4× Exchange ASICs

Target acceleration over CPU: 10,000×
Target release date: 2025



Designed to handle the full TFHE bootstrap or CKKS key switching on-chip

PCIe3 interface for host / device communication

PHOENIX

We are part of the PHOENIX project (ferroelectric PHOtonics ENablIng novel functionalities and enhanced performance of neXt generation PICs), a 3-year collaboration between universities and private companies to unlock next-generation encryption and computing thanks to advances in photonics.

Focus on three high-impact emerging applications:

* Fully Homomorphic Encryption
* 5G infrastructure
* Neural networks training and inference

https://www.heu-phoenix.eu/

Lumiphase · PNO · IBM · Nanophotonics Technology Center · Universitat Politècnica de València · UKRI Innovate UK · KU Leuven