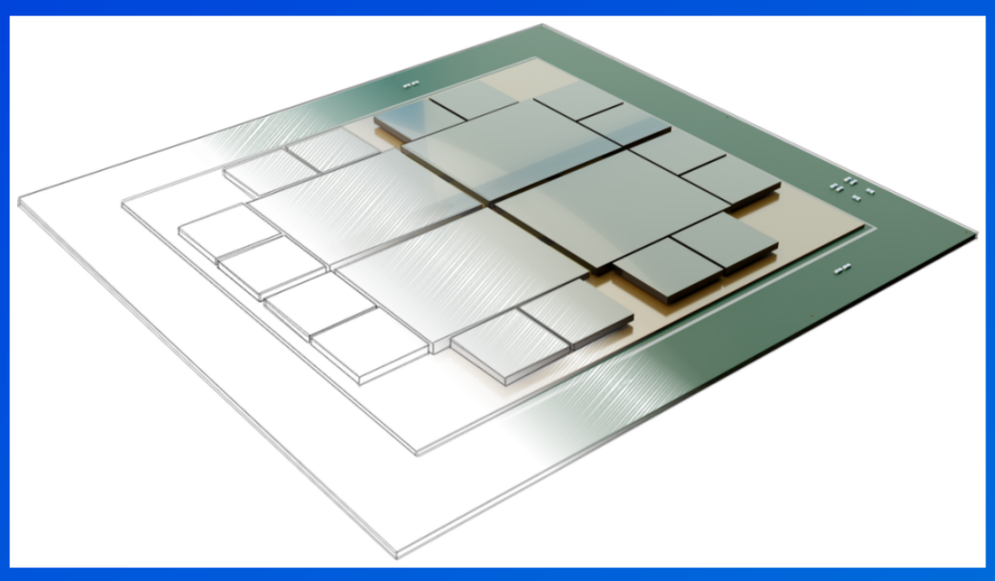
FPGA-accelerated encrypted credit card fraud detection

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 for the dirst ASIC version: 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 the TFHE, BGV, B/FV, and CKKS schemes

Prototype: FPGA-accelerated TFHE for credit card fraud detection

Logistic regression model for flagging fraudulant credit card transactions

Why FHE?

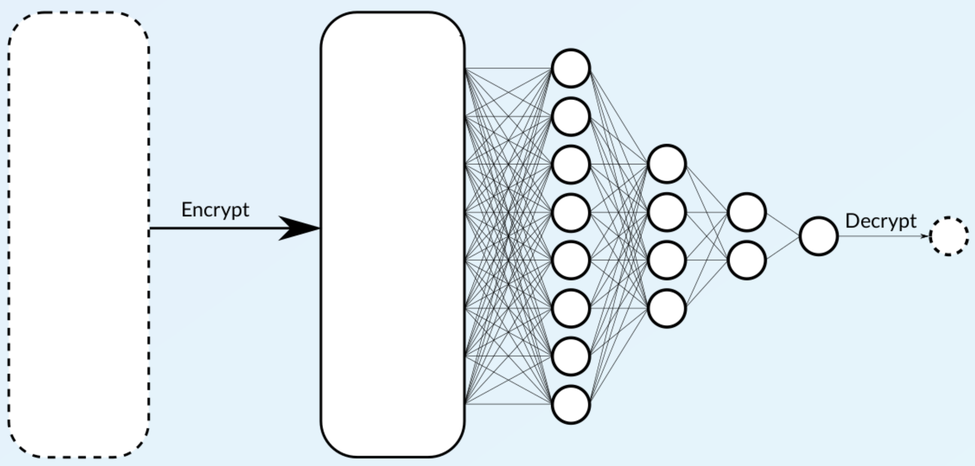
- Card transactions leak ***very*** sensitive information (location, political or religious orientation, health issues, ...)
- Yet close monitoring is required to keep the system (and everyone's bank accounts) secure

⇛ Any acceptable solution formaintaining provacy and security requires transaction data to be collected and processed in encrypted form

A simple model: Logistic regression (optionally augmented with a shallow neural network) to flag possibly fraudulent transactions

⇛ All processing can be done on encrypted data

⇛ Simple enough model to reach acceptable speeds with existing solutions (0.1s to a few s per transaction)



NTT-based TFHE

Current performance: 500 PBS/s/SLR

PBS module fits on one SLR of the Alveo U55C FPGA

Benchmarking parameters: N = 1024, Q = 65537

Work in progress:

- Support for parameters compatible with the TFHE-rs and OpenFHE implementations
- Improve pipelining for faster PBS
- Optical integration

Optical acceleration

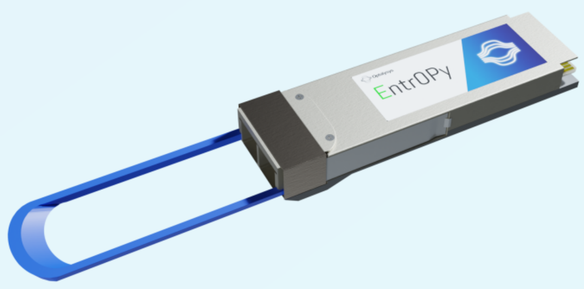
Optical cavity realised and tested in Optalysys lab

Current accuracy 100%
Current operating frequency: 125MHz

Work in progress:

- Link with the FPGA implementation
- Increase the operating frequency to above 1GHz

Upcoming pluggable device with transceiver form-factor



Longer term: ASIC/optical implementation of TFHE and CKKS

Toward real-time FHE

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