Optalysys

Optalysys Technology for FHE

Presentation to FHE.org

15/06/23

Intro to Optalysys

Who are we?

We're a deep tech company in the north of England focusing on optical computing.

What do we do?

We're developing a photonic computing system that accelerates Fourier and Number-Theoretic transforms.

What's the goal?

The system we're building is designed to provide massive acceleration (>10,000x) for *fully homomorphic encryption* (FHE).

Where are we now?

In 2023, we'll be making access to photonic accelerators available for end-users.

© Optalysys Ltd 2023

Fully Homomorphic Encryption

Optalysys

The “holy grail” of Privacy Enhancing Technologies:

FHE enables arbitrary computing on encrypted data

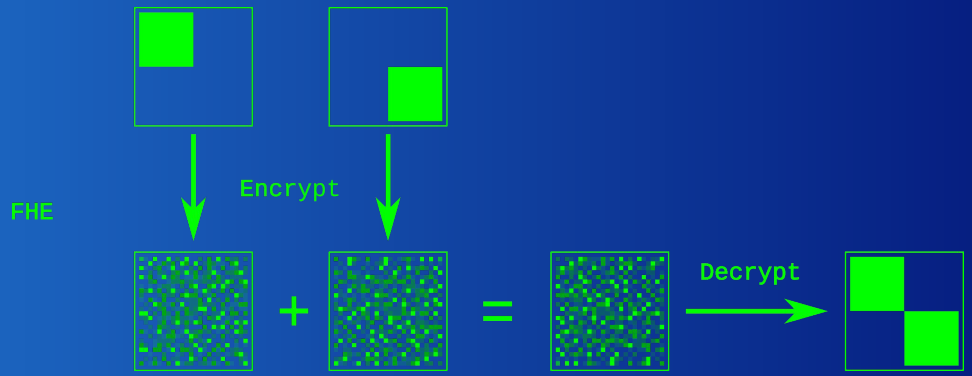
Data is never decrypted. Even the hardware working on it is always blind

The underlying cryptography is post-quantum resistant

Fully Homomorphic Encryption

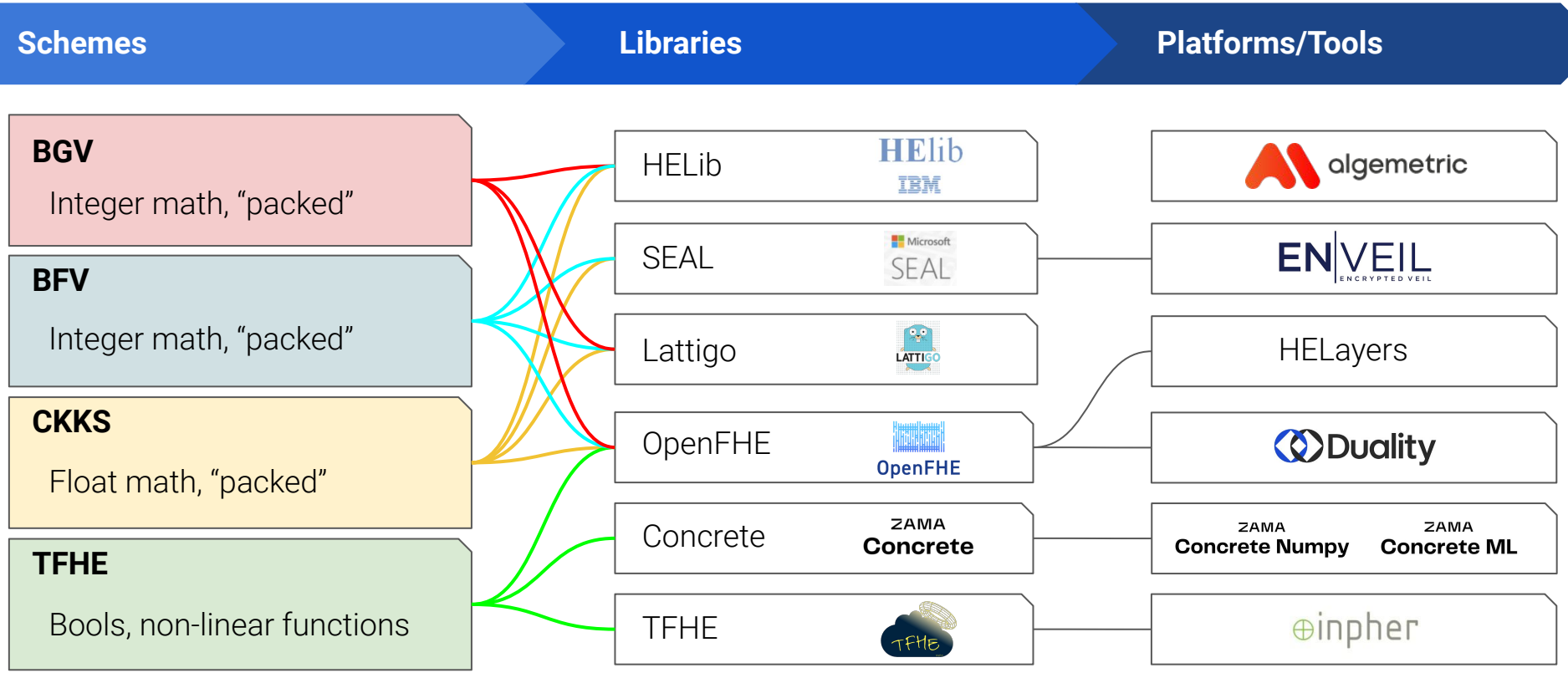
Under FHE, addition and multiplication operations performed on ciphertexts are reflected in the decrypted result.

This enables arbitrary operations on encrypted data.



FHE Implementations

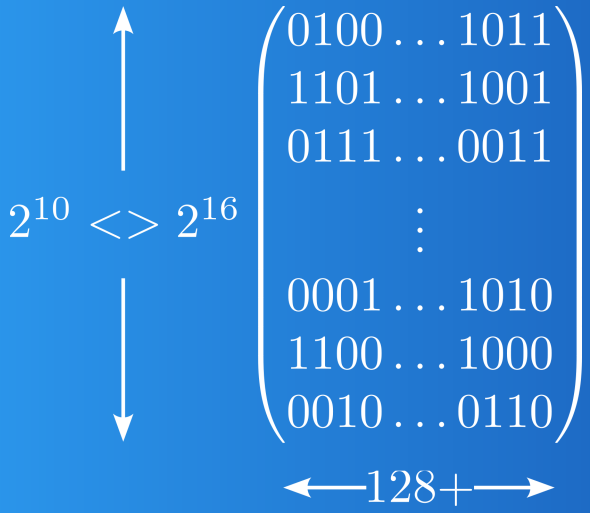
Optalysys



The Challenge

Optalysys

Ciphertexts are *huge* in several respects



Big challenges for hardware developers!

- Efficient multiplication of large polynomials requires *big* transforms at *low* speed
- Arithmetic on large polynomial coefficients
- Data transfer bandwidth and memory

70-90% of compute is in transform (FFT/NTT) operations alone

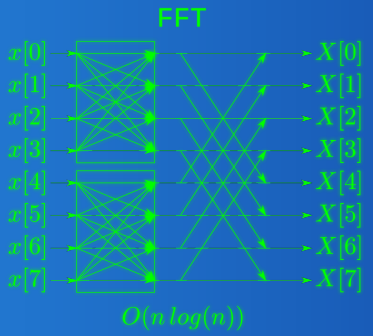
The power of optics

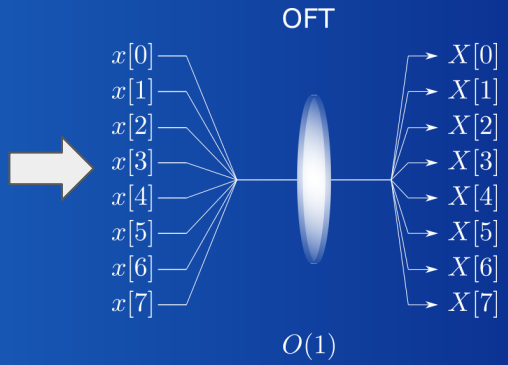
Optalysys

The Optical Fourier Transform

- A near-instantaneous, massively parallel Fourier transform
- Extremely high data processing rates
- Core calculation process is passive

Processing Fourier transforms electronically requires multiple clock cycles





Fully complex Optical Fourier transforms eliminate multiple electronic operations

The Optalysys approach provides a path to real time processing of FHE encrypted data

Optalysys

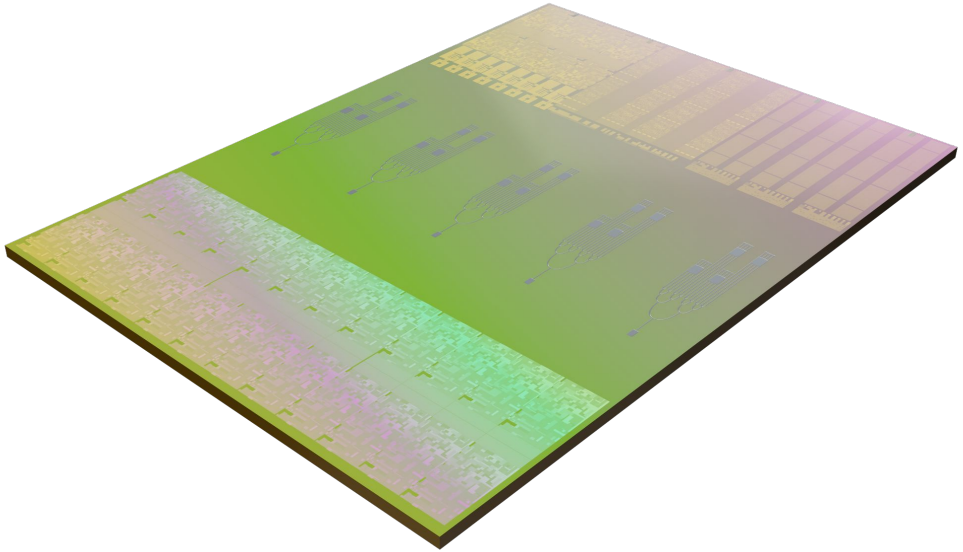
Solution: Optalysys Etile™

Etile is our core technology.

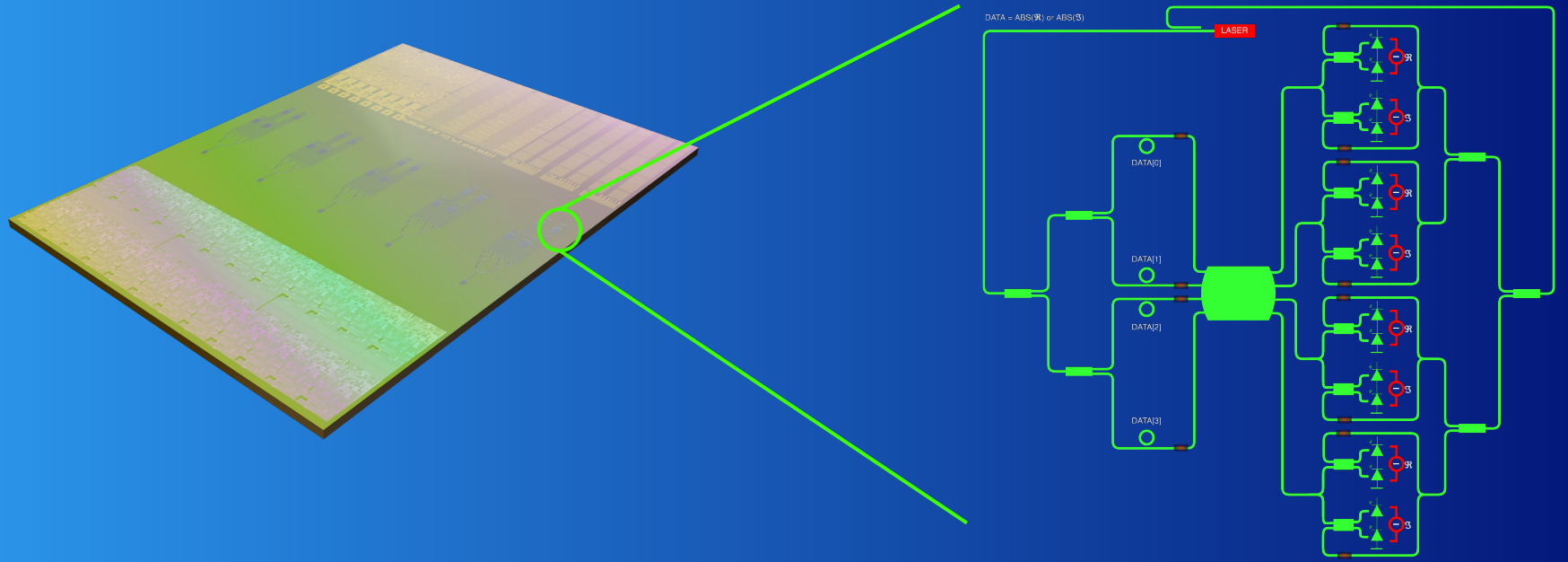
A silicon-photonic optical computing circuit with a digital interface, Etile brings Fourier optics and electronics together at the chiplet level.

Etile is responsible for high-speed generation of FT/NTT components at ultra high speed.

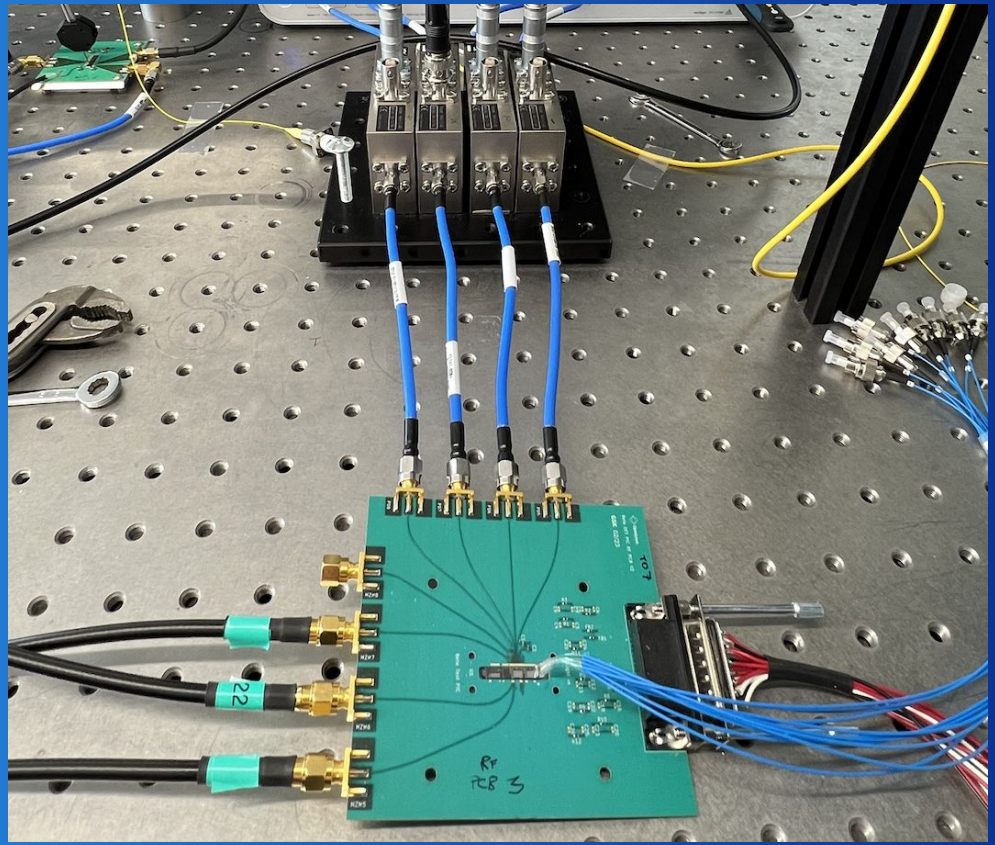
Etile is the key to addressing the main compute and speed challenge of FHE.



Photonic transform circuit



Benchtop system



Optalysys

Solution: Optalysys Enable™

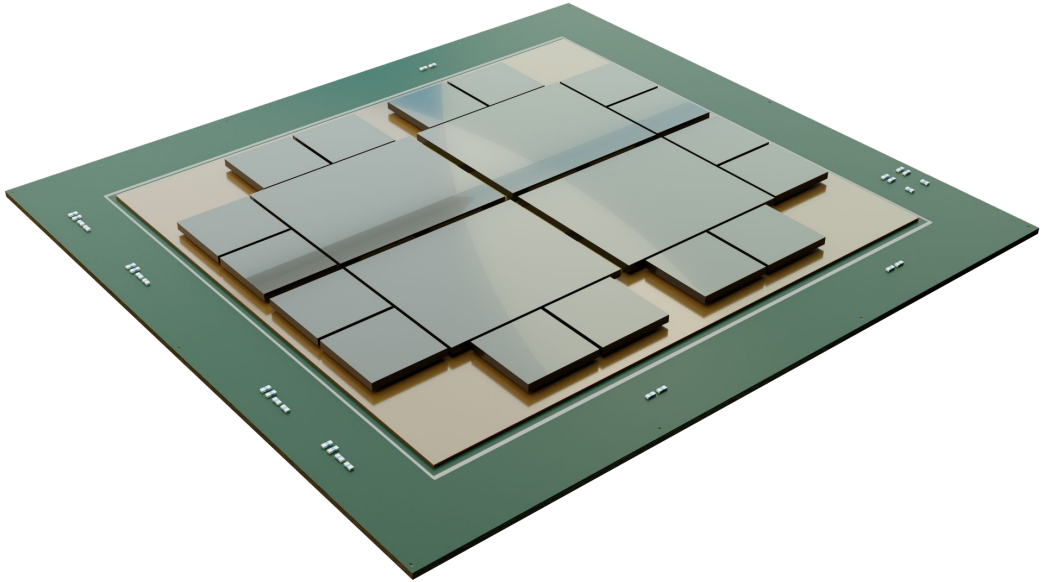
Enable is our complete FHE solution.

Enable leverages the power of Etile to execute high-speed transforms.

Supporting electronics pull the rest of an FHE calculation together.

Enable is projected to be *at minimum* 7x faster than dedicated ASIC solutions for FHE and 10,000x faster than current SOA.

Enable supports *universal* FHE scheme acceleration.

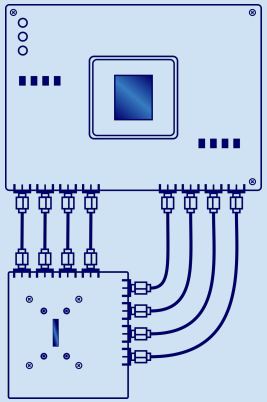


Timeline 2023

Optalysys

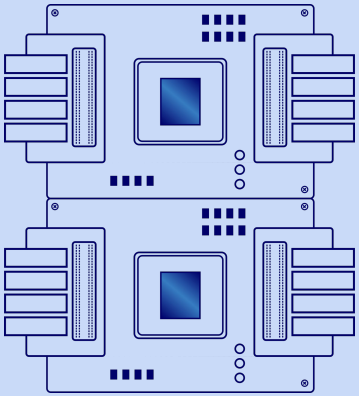
What Optalysys hardware compute solutions are coming for FHE, and when?

Q2 2023 — Q2 2024 — 2025



Benchtop system access -5x

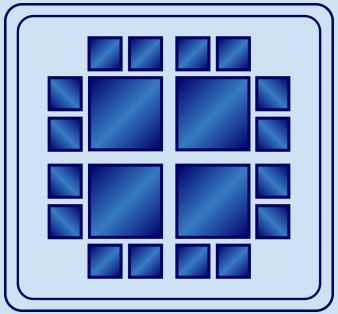
- Remote access to photonic accelerator.
- Full FHE workflows supported.
- Schemes and libraries implemented on Optalysys FPGA and photonic compute capabilities.
- ~5x acceleration vs state of the art CPU.



Scalable cloud system - 250x

- Multi-chiplet solution via pluggable photonics.
- FPGA-based electronics.
- ~250x acceleration vs state of the art CPU.
- Cloud-deployable

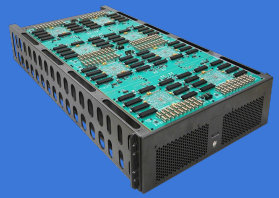
Enable MCM - 10,000x



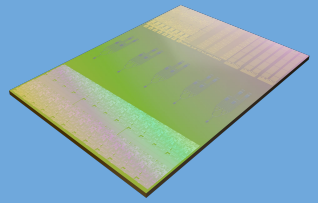
Pathway to Enable

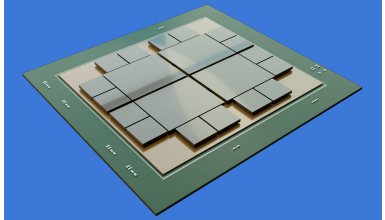
Optalysys

IaaS



IaaS





Beta FPGA System 2 optical cores 5x vs SoA*	EntrOPy Module Pluggable QSFP28 1x4 optical core	Beta Extreme 64 EntrOPy cores 250x vs SOA	Etile Tapeout 64 optical cores	Enable 10,000x vs SoA
Demonstration of High-speed photonics	Enables easy scaling of beta hardware	Deploys EntrOPy at scale. Cloud development.	Full CMOS integration with mass optics	Initial product with massive performance gains

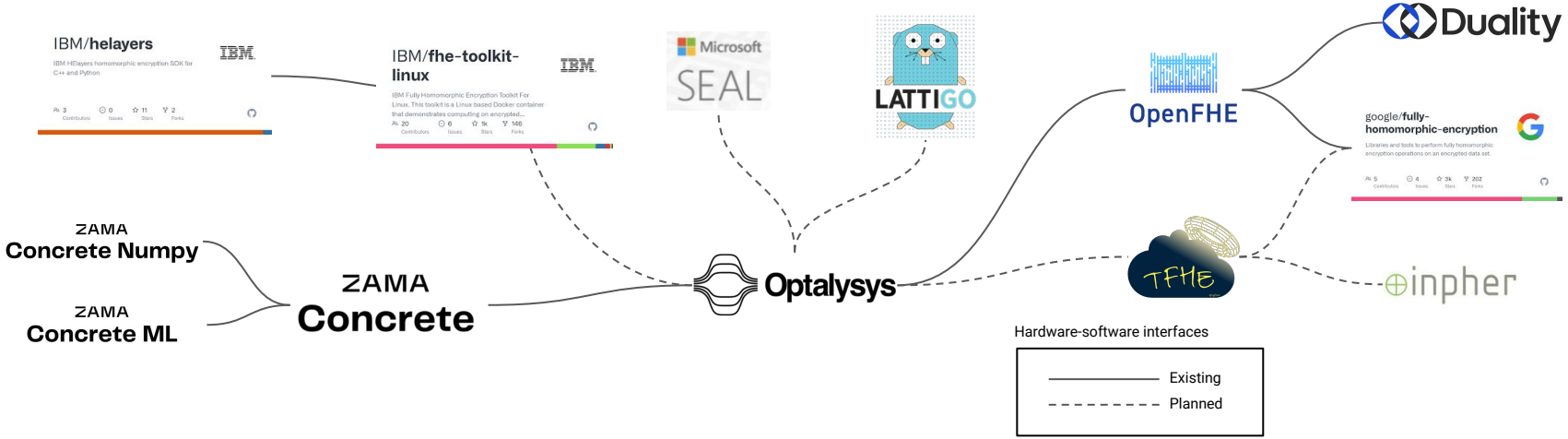
*SOA comparison: Latest generation 12-core Intel i7-12700K CPU @6.3GHz

Hardware Integrations

FHE software libraries and toolchains are rapidly maturing.

You no longer need to be an expert cryptographer to use FHE.

Our accelerator systems integrate with major FHE toolchains.



We are part of the PHOENIX (ferroelectric PHOtonics ENabling neXt generation PICs) project.

Objectives:

- To test novel photonic systems made using new materials; VOx and BTO.
- To provide a BTO/SiN waveguide platform for new photonic ICs and demonstrate the potential to improve their performance and scalability.
- To build up demonstrator systems.
- To advance the realization high-quality oxide thin-films by molecular beam epitaxy (MBE) over large areas.

The demonstration focus of PHOENIX includes FHE, alongside 5G infrastructure and neural network training and inference.

KU LEUVEN

NANOPHOTONICS TECHNOLOGY CENTER

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Lumiphase

UKRI Innovate UK

PNO

IBM

PHOENIX

Questions