Optalysys

# The Optalysys Etech

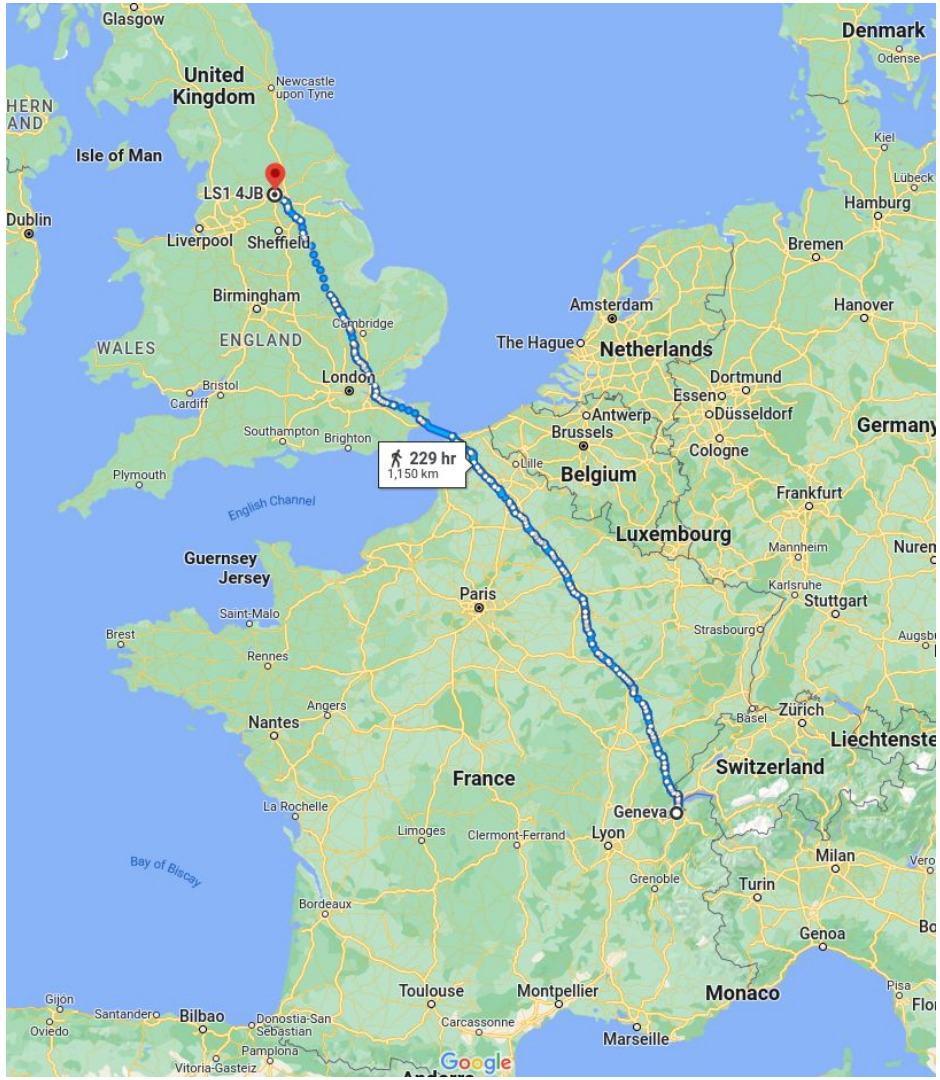
## Accelerating FHE with Silicon Photonics

www.optalysys.com

Optalysys

# Optalysys

## An optical computing compagny

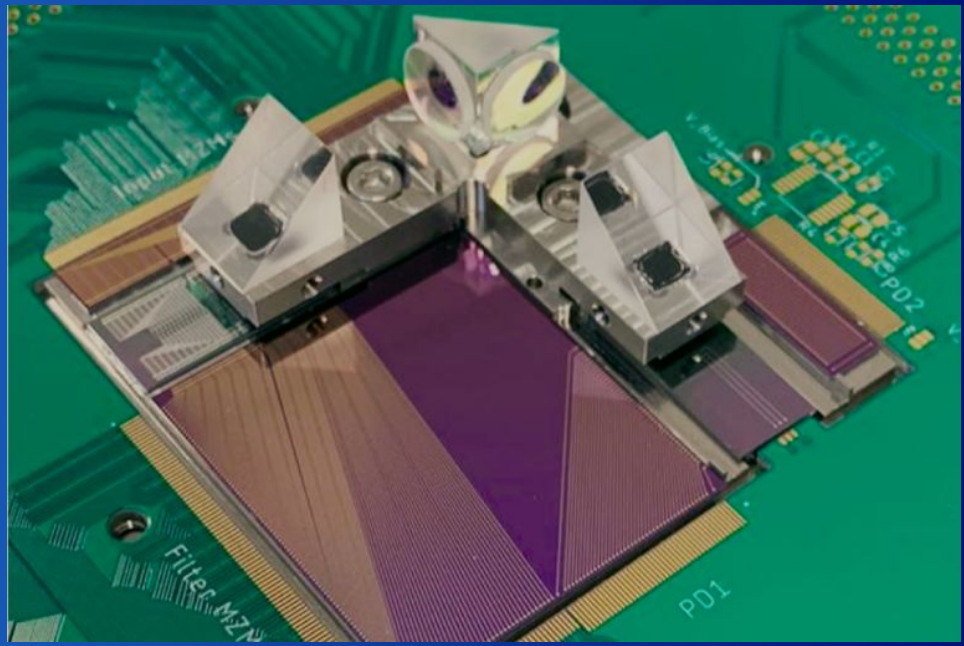


# Optical computing for Fourier transforms and co

Optalysys

Founded in 2013

Optical Fourier transform for pattern matching, correlations, convolutions, and numerical derivative




Now moving to (much) smaller on-chip devices for integration in traditional computing system

# Fully homomorphic encryption is a massive opportunity

Optalysys

## Under existing models of security...


Of enterprise data goes unused

### Why?

Regulation.

Privacy.

Confidentiality.

**Our technology unlocks the value of FHE through unprecedented acceleration and efficiency**

**FHE solves these problems**

**We can realise the full value of data**

**Where we fit: secure data processing hardware**


https://www.frontier-enterprise.com/two-thirds-of-data-available-to-firms-goes-unused/

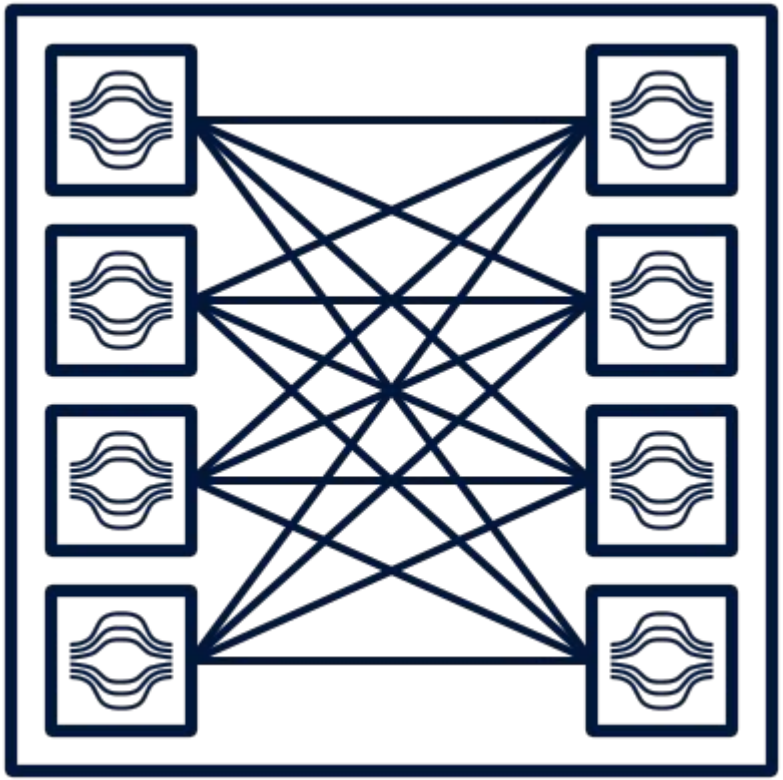
https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

Optalysys

# Optics and FHE

## Or how optical computing will solve the polymult bottleneck



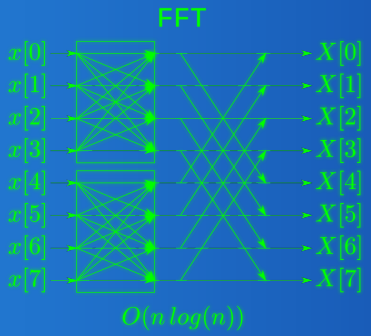
# The power of optics

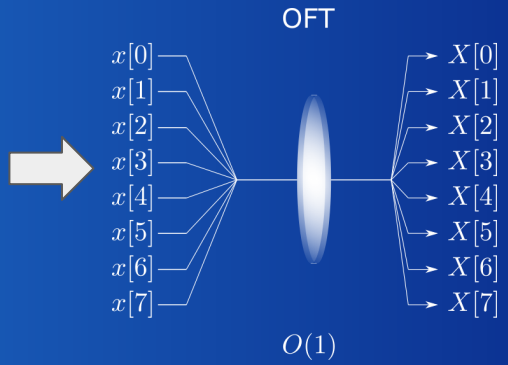
Optalysys

## The Optical Fourier Transform

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

**Processing Fourier transforms electronically requires multiple clock cycles**



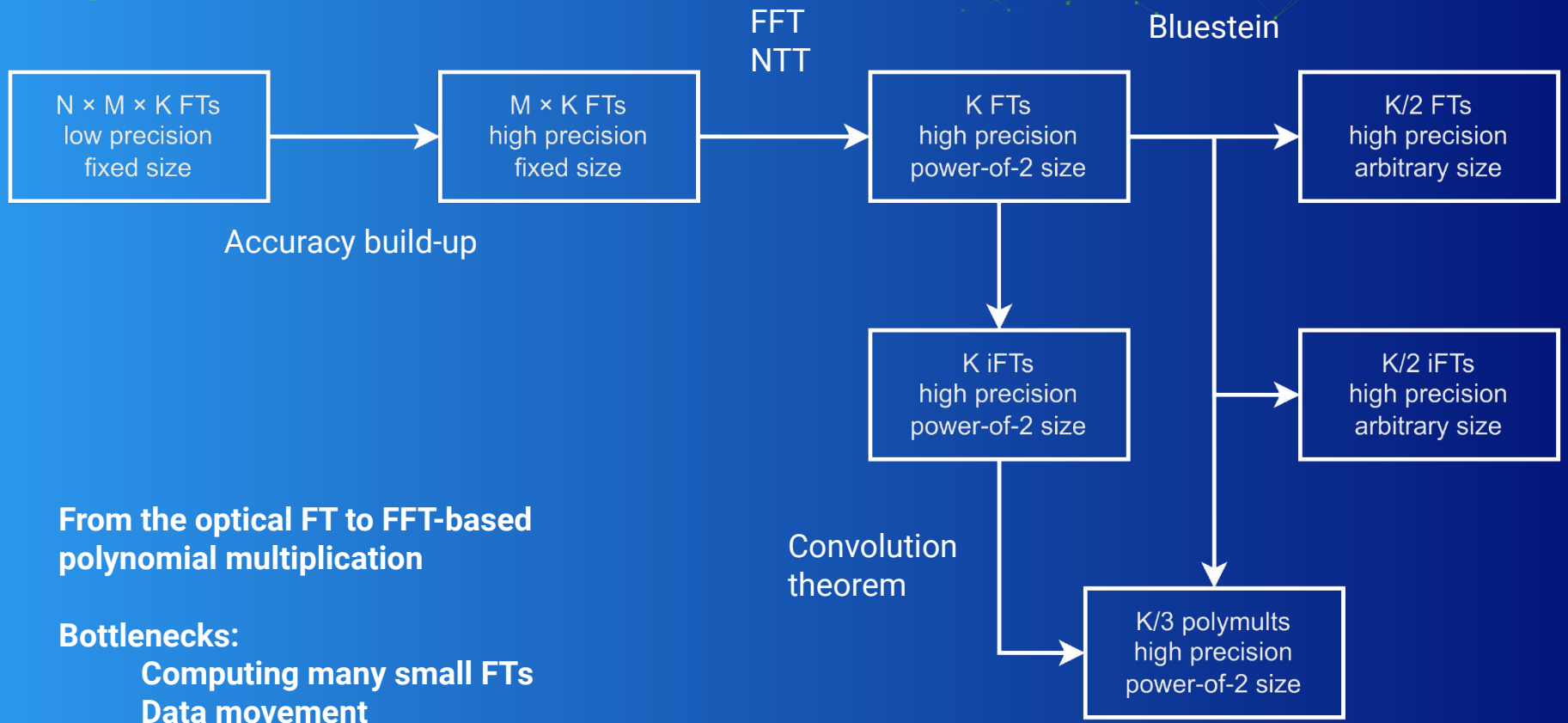




**Fully complex Optical Fourier transforms eliminate multiple electronic operations**

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

# FT Algorithms

Optalysys

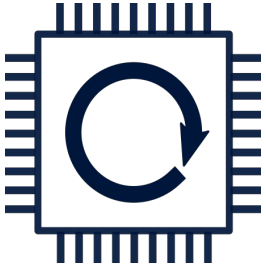



**From the optical FT to FFT-based polynomial multiplication**

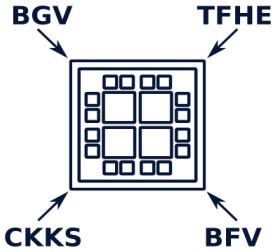
**Bottlenecks:**

- **Computing many small FTs**
- **Data movement**

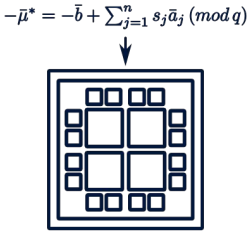
# Our solution: Key points



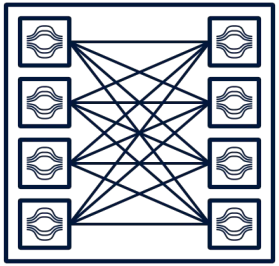
We target all operations on-chip to eliminate interfacing constraints




Support for all FHE schemes via unified NTT/FFT photonic architecture




Instruction set designed for low-level integration with FHE libraries and APIs

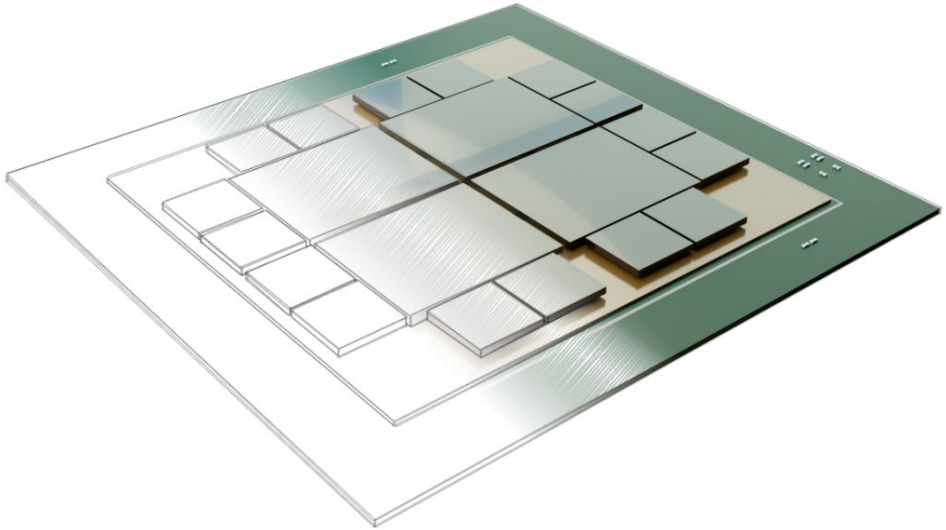


Parallel Etiles for FFT and NTT in a matter of nanoseconds

Optalysys

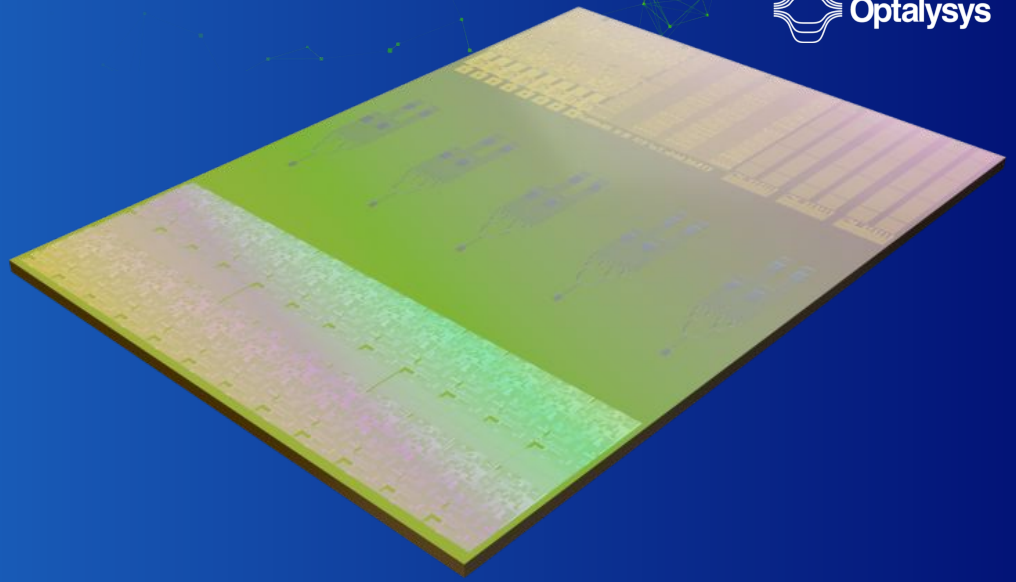
# The Etech

## Our plan to make real-time FHE a reality

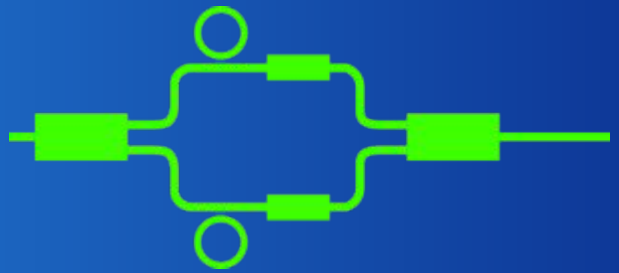


# Etile: The core optical unit

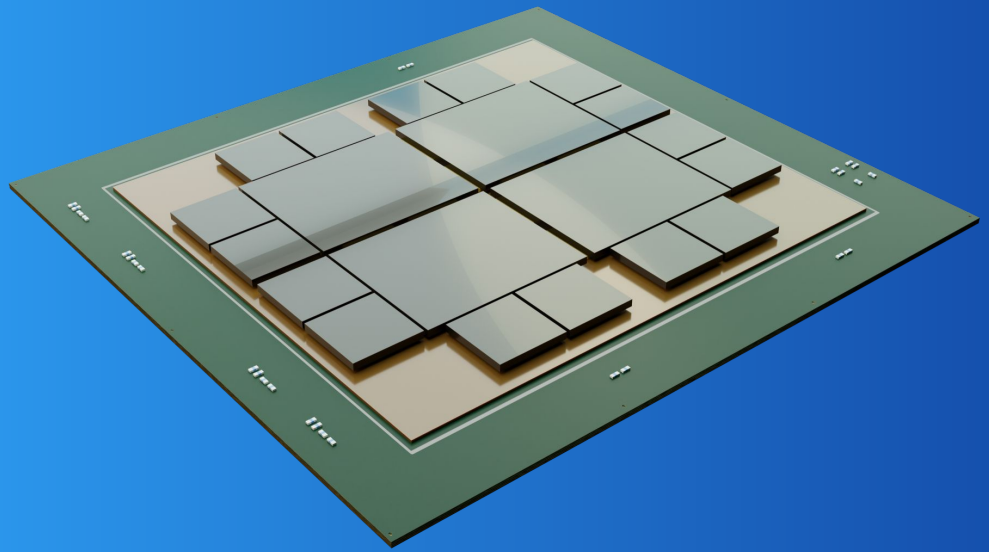
Multiple free-space optical elements for simultaneous computation of fixed-size FTs



Modulators for data encoding (two branches for the real and imaginary parts)



# Enable: Plug-and-play MCM



16 Etile cores + 4 Ensemble digital cores

**Etile cores:** High-precision Fourier transform / NTT computations of size ≤ 16

**Ensemble cores:** FFT / Fast NTT reconstruction algorithms, convolution, polynomial multiplication, polynomial addition, scalar-polynomial multiplication

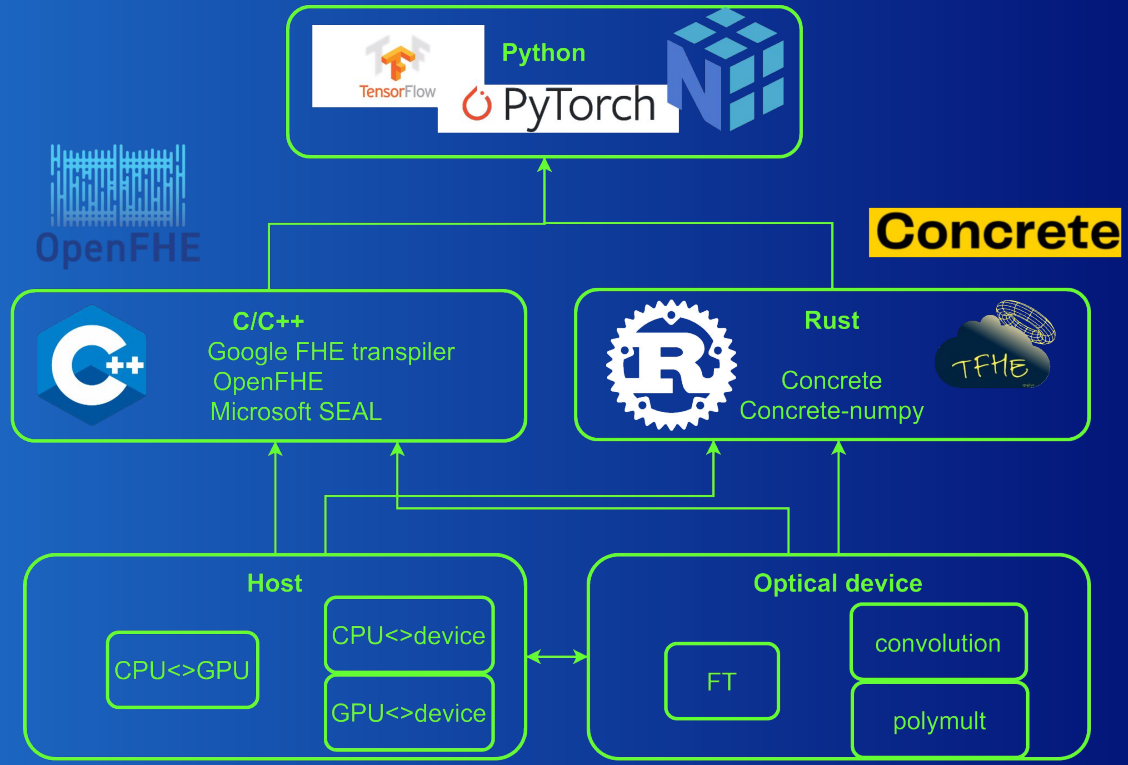
Additional logic and memory to store server keys, relinearization, and bootstrap algorithms

# Software stack

**Firmware:** Direct interaction with the Enable system (send / receive data, send instruction list, FT, NTT, iFT, iNTT, relinearization, bootstrap, …)

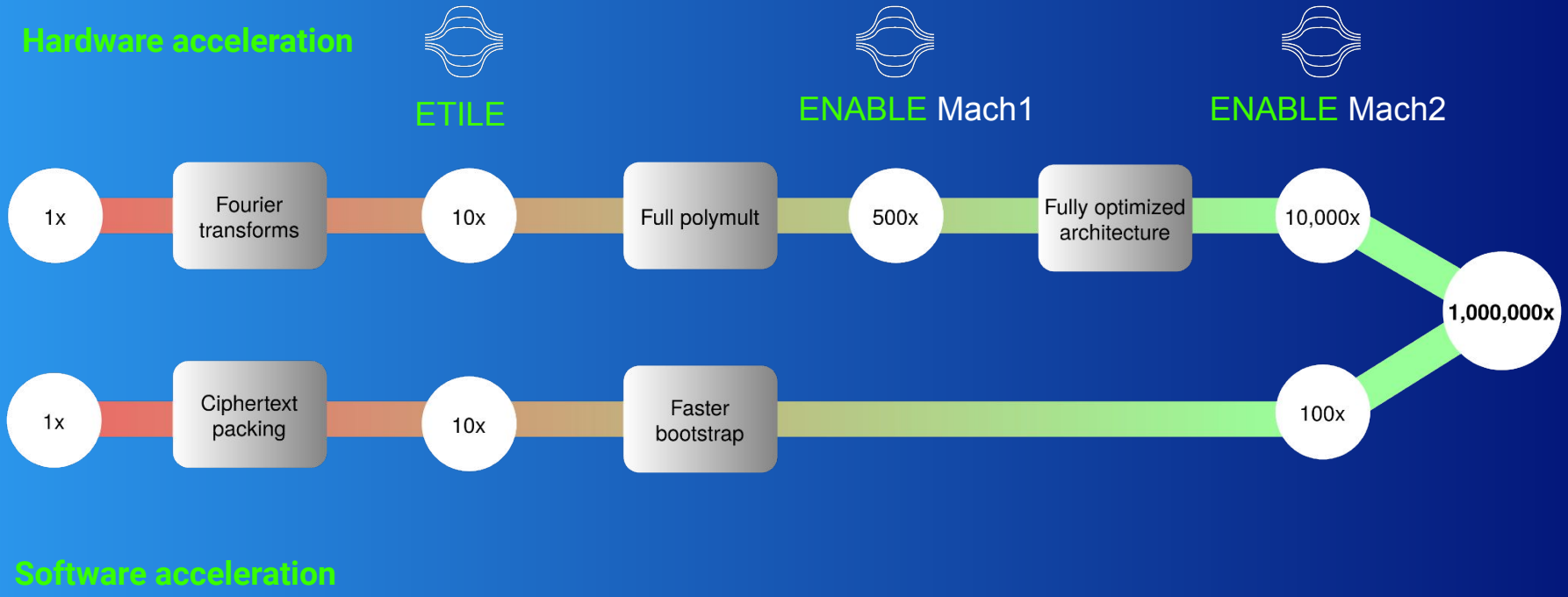
**Low-level:** C/C++ and Rust interfaces for easy integration into existing libraries
WIP custom interfaces for Concrete and OpenFHE

**High level:** Numpy, TensorFlow, and PyTorch interfaces
Custom interface for Concrete-Numpy and Concrete-ML



# Toward real-time FHE

Optalysys



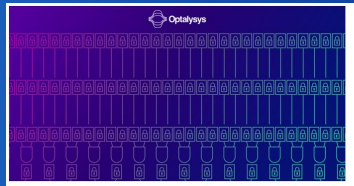

Target all the main FHE schemes: TFHE, DM, BGV, BFV, CKKS

# How to learn more about us?

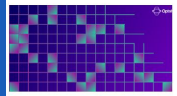
Optalysys

Medium page:
https://medium.com/optalysys

Website: https://optalysys.com

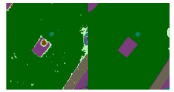




**Encrypted search using fully homomorphic encryption**
With Florent Michel, Joseph Wilson and Edward Cottle
Optalysys · Nov 3 · 16 min read

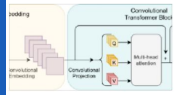


**Fully Homomorphic Encryption and the Game of Life**
Concrete Boolean for efficient FHE meets optical computing
Optalysys · Oct 20 · 20 min read

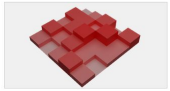
**Attention: Fourier Transforms. A giant leap in transformer efficiency.**
With Joseph Wilson
Edward Cottle · Oct 15 · 7 min read



**Semantic segmentation using an optical computer**
With Edward Cottle
adhts · Sep 17 · 22 min read

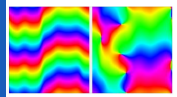



**Accelerating Convolution Vision Transformers**
With Florent Michel and Adhi Saravanan.
Edward Cottle · Aug 31 · 9 min read

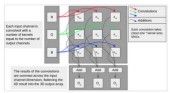


**Higher numerical precision for optical Fourier transforms**
We've described before how our optical computing system has some inherent advantages over electronic methods when it comes to executing the...
Optalysys · Aug 23 · 25 min read

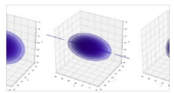

**AI super resolution using an optical computer**
In this article we will discuss super resolution, an AI technique that uses deep neural networks to increase the resolution of images and...
Edward Cottle · Jun 30 · 14 min read



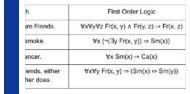
**Optical computing for predicting vortex formation**
with Edward Cottle and Joseph Wilson
Florent Michel · Jun 7 · 13 min read



**Fourier-optical computing: Acceleration squared**
Optical computing is fast, but the way we conventionally think about faster computing can miss the greater point.
Optalysys · May 28 · 8 min read

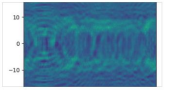


**The Optical Fourier Engine: A Fourier transform accelerator in arbitrary number of...**
We show that the optical Fourier core can be used to compute Fourier transforms in any dimension
Florent Michel · Apr 9 · 17 min read

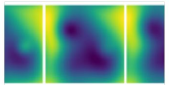


**Neurosymbolic AI: Combining Logic Tensor Networks and Computer Vision**
In our previous article on self-driving vehicles, we explored some of the nuances of the two most common algorithmic approaches...
Edward Cottle · Mar 22 · 17 min read

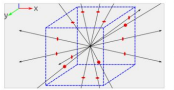
**Self-driving vehicles and Fourier-optical computing: A way forward?**
Over the past half year at Optalysys, we've tested the prototype of our novel Fourier-optical processor technology in a broad range of...
Optalysys · Mar 5 · 9 min read



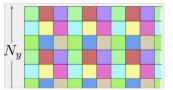
**Simulating wave propagation with the optical Fourier Engine**
We show that the Optalysys Fourier engine can accurately simulate wave propagation, including dispersive and dissipative effects
Florent Michel · Mar 4 · 17 min read



**Deep learning and fluid dynamics: Solving the Navier-Stokes equations with an...**
Using optical computing and deep learning for solving the Navier-Stokes equations
Optalysys · Mar 2 · 20 min read



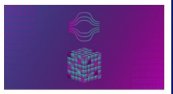
**Optical computing for computational fluid dynamics: An introduction to CFD**
Engineers predict the behaviour of things on a regular basis. "Will this bridge hold under load? Will it hold in high winds? Are there any...
Joseph Wilson · Feb 26 · 21 min read



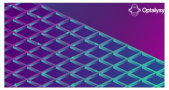
**Scaling up: Using Fourier Optics for Bigger Transforms**
The Fourier transform is a phenomenally useful mathematical tool applied throughout the scientific world. Wherever nature contains a...
Optalysys · Feb 11 · 13 min read

**Optical Computing and Transformer Networks**
We show that optical convolutions can be used to build transformer networks, paving the way for making them more efficient using optics
Optalysys · Feb 10 · 17 min read

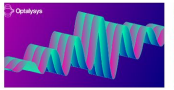
**Model Uncertainty in CNNs**
Industry is becoming increasingly more reliant on computer vision, with large numbers of diverse applications for example robotic surgery...
Edward Cottle · Feb 3 · 6 min read



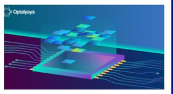
**Optical Computing for Cryptography: Fully Homomorphic Encryption**
Fourier-Optical computing has the capacity to deliver tremendous improvements in artificial intelligence, but that's not the only field to...
Joseph Wilson · Jan 15 · 21 min read



**Optical Computing for Cryptography: Lattice-based Cryptography**



**Optical Computing for Post-Quantum Cryptography: Why we need PQC**



**The MFT System Part 3: Detection**
If you've been reading our previous

Optalysys

# Thank you for your attention!