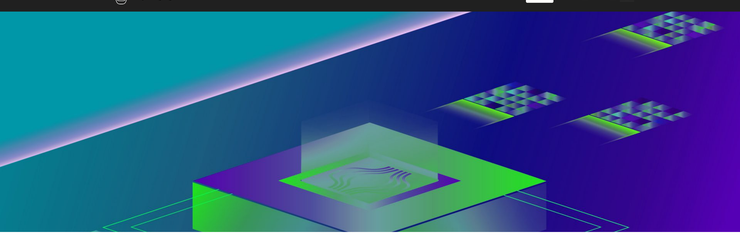


OPTALYSYS: WHAT WE'VE DONE (AND WHY WE DID IT)

An Update

[6 minute read]

When we began writing articles for this website in early 2021, we opened with a description of our technology and our reasons for pursuing this kind of optical computing. Since then, we've gone on to demonstrate the application of Fourier-optical computing across many different technical fields, from artificial intelligence through to wave propagation problems.

The rationale for optical computing that we presented in our original article has not changed. The optical Fourier transform continues to offer an incredibly powerful solution to otherwise intractable computing problems. However, the specifics of how we implement our technology have undergone some slight revisions since our first article.

These revisions are driven by the technical and commercial needs of a very specific application. While many workflows can benefit significantly from the development and deployment of a high-performance Fourier transform co-processor, it is in the field of *encryption* that we have found a significant opportunity to unleash the *full* potential of optics.

As we move forwards with developments in this revolutionary new field of cyber-security, now is a good time to revisit what it is that Optalysys does and consolidate updates on how our technology has been shaped in the context of this development.

The Optical Fourier Transform

The optical Fourier transform (OFT) has always had extremely attractive properties for solving Fourier-based calculations. As things stand, all-digital implementations of the fast Fourier transform (FFT) algorithm run into fundamental limitations to the speed at which they can run.

Modern advances in CMOS electronics simply can't provide the advances in raw transform calculation speed that FHE demands, nor are conventional computers well suited to executing FHE algorithms. By contrast, performing these critical operations using the *Optical* FT benefits from incredibly low execution time.

Under the optical FT, individual sub-elements of a transform calculation are performed at the speed of light. This optical calculation also consumes no direct power, and produces little to no heat.

However, using this remarkable capability as part of *digital* computing requires an efficient way of interfacing electronic and optical computing systems. Solving this problem is by far the most significant aspect of the hardware development work that we do at Optalysys.

Our approach uses the medium of silicon photonics to integrate both the optical processing stages and supporting digital infrastructure on a single chip-scale die. Not only does the use of silicon photonics provide access to extremely high-speed optical modulation technology, but on-die optical-electronic integration allows us to take advantage of contemporary techniques in the design and construction of multi-chip modules.

By designing our photonic processing chips to interface with conventional electronic processing cores over next-generation die-to-die interconnects, we can unify enormous transform processing power with the incredibly high data transfer rates that are needed to transfer the calculation results to electronic processing systems.

In terms of our commercial intentions for this technology, we are now fully focused on developing an a system that provides massive acceleration for fully homomorphic encryption (FHE). This involves an expansion in the scope of our proprietary hardware to incorporate fully-digital technologies that support the unique requirements of FHE computing. However, the core advantages of this solution are as ever provided by the unique capabilities of optics.

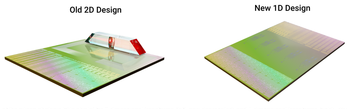
Fully homomorphic encryption and Optalysys technology

The optical Fourier transform gives us a method for calculating mathematical transforms at speeds that cannot be matched by electronics. This is extremely valuable for FHE, as between 70–90% of the total calculation burden is taken up solely in calculating the transforms needed for more efficient polynomial multiplication.

FHE introduces a set of unique challenges in computing, and we've had to find solutions to many of these problems. We won't go into extensive detail on these problems or how we have addressed them (we'll cover some of them in later articles), but here's a quick summary.

- **Given the data type requirements of FHE, we have transitioned from developing a 2-dimensional optical computing process to a 1-dimensional process.**

Rather than ejecting light from the surface of our silicon photonic system into an external free-space optical environment (as described in our early article on free-space optics), we now perform the core optical Fourier transform in a free-space optical environment which is constructed *in the plane* of the silicon die.



Visualisation of the silicon photonic Eagle chiplet for 2-dimensional transforms (left, now deprecated) and 1-dimensional transforms (right). The 1D free-space transform stages are now structures integrated into the silicon photonics itself.

- **FHE requires large, high-precision transform operations.**

In past articles, we have previously described how we can use small, low-precision optical transforms to reconstruct larger transforms at higher precision.

While these articles were written in the context of a 2-dimensional system, the same principles hold for the 1-dimensional approach. To support efficient reconstruction of transforms of sizes that are powers of 2 (as is typical in FHE), we have adjusted the design of our free-space optical transform stages to process 4 data points at extremely high speed.

We can construct multiple such transform stages on a single die. The speed at which these photonic cores work, coupled with the ability to leverage parallelism, makes exceptionally short work of the transforms needed for FHE.

- **Supporting the full range of fully homomorphic schemes requires that we support two distinct yet related transform operations; the fast Fourier transform (FFT) and the number-theoretic transform (NTT).**

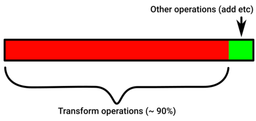
While designing an electronic system that is efficient for both of these tasks is difficult, the design and function of of the 4-input optical transform stages described above actively supports the easy calculation of elements of both the FFT and NTT, allowing us to switch between the two without incurring a runtime penalty.

- **FHE features a relatively simple set of mathematical operations that can be performed on encrypted data.**

From these simple operations, we can construct arbitrary computing capabilities. However, conventional processing hardware is designed to work on plaintext data structures such as floats and integers and to a degree of precision (64-bits in modern architecture) which is often not suitable for FHE, introducing additional limitations and bottlenecks. This requires dedicated logic designed around FHE ciphertext data structures.

The Optalysys Enable FHE accelerator

Accelerating transform operations for fully homomorphic encryption is hugely valuable and is fundamental to our plans for bringing FHE to mass scale and adoption. However, while the speed-ups that can be provided solely from photonics are significant, FHE still presents an extreme challenge. Right now, depending on scheme and application, FHE is approximately a million times slower than unencrypted computing. If we're going to bring FHE to scale, we need to be even faster.



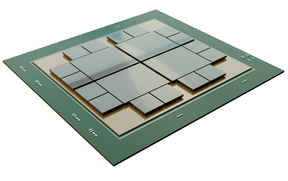
FHE runtime by approximate proportion of calculations using contemporary all-digital methods

Of course, if we reduce *only* the runtime of the transform operations, the other operations become (proportionally) a much larger part of the processing, so the overall acceleration that can be achieved solely by accelerating transforms is limited by these other operations.

Accelerating only the transform operations will eventually yield diminishing returns relative to the total computational load. While the major benefits of Optalysys technology come from our optical approach to transform operations, we realise the need for effective supporting hardware to tackle the non-transform operations. This includes very large vector operations such as addition and modular reduction. Combining these two solutions will yield a highly effective FHE acceleration platform.

Providing a *solution* for fully homomorphic encryption that addresses the enormous runtime disparity between encrypted and unencrypted computing thus requires more than a single technology. It requires that we tackle both the transform processing *and* provide an efficient solution for the other operations.

This is the objective of the FHE solution now under development at Optalysys. This system is called *Enable*, and it pairs Optalysys photonic computing chiplets with logic dedicated to both the management of transform data and the supplementary operations that are required for greater levels of FHE acceleration.



Visualisation of an Enable Multi-Chip Module (MCM). The smaller chiplets towards the edge of the MCM are Optalysys Eagle units that provide high-performance FFT and NTT transforms, while the large central chips feature custom logic for handling the enormous data flow from the Eagles and other FHE operations such as addition and modular reduction.

Optalysys Enable brings mass acceleration to FHE. By targeting both transforms and other operations, the objective of the Enable system is to ultimately bring a factor of 10,000x acceleration to *all* FHE schemes in a highly scalable form factor.

To learn more our Eagle and Enable systems , you can visit our site for an in-depth overview of the advantages of Optalysys technology in FHE. Meanwhile, in subsequent articles, we will be demonstrating world-first demonstrations of FHE applications and techniques that make use of the core optical principles of our systems.