The Optalysys Accelerator Program

Your roadmap to developing FHE capabilities

Optalysys

Privacy Enhancing Technologies (PETs) promise to solve longstanding problems in data protection.

How?

PETs are a class of technologies and frameworks that enable data to remain private and confidential, even in scenarios where information would typically be at risk.

This extends from techniques intended to ensure stronger guarantees of anonymity, through to powerful new cryptographic methods that enable secure collaborative computations.

By enhancing confidentiality and security, PETs make previously unexploitable data safe to share and use. In the process, PETs are set to drive a fundamental shift in how businesses and organisations maximise the commercial value of the information they hold.

> ***"By 2030, data marketplaces enabled by PETs, in which individuals, corporates, machines and governments trade data securely, will be the largest ICT market after the cloud"*** [1.]

The opportunities presented by this technology have spurred a wave of innovative solution providers and software libraries which are now reaching maturity.

At the same time, governments and regulatory bodies are increasingly aware of the opportunities and challenges that PETs will present. The core technologies and supporting ecosystems are now primed to deliver meaningful improvements in data security and applicability.

Organisations that can master the transformative opportunities of PETs will be well positioned to re-shape and enhance not only their own operations, but those of entire industries.

At Optalysys, we focus on enabling a particular PET technology known as Fully Homomorphic Encryption (FHE).

Often considered to be the "holy grail" of PETs, FHE is a method of encrypting data such that computations can be performed directly on protected information.

Powerful and flexible, FHE can be applied to enable a diverse range of highly sensitive data analysis tasks.

The steep computational cost of FHE has thus far limited its ability to be deployed at scale. Optalysys hardware is specifically designed to overcome the unique processing challenges inherent to FHE, opening the door for growth and innovation in the field.

We are now pleased to present the Optalysys Accelerator, our framework for companies and organisations seeking to exploit these opportunities.

This program enables both novel hardware access and information transfer to assist businesses in navigating, developing and deploying FHE solutions. In this report, we outline why dedicated hardware acceleration is a much-needed step forwards for FHE, and provide a brief overview of our framework for engagement over 2023.

1. Lawrence Lundy-Bryan in (2021) Privacy Enhancing Technologies: Part 2 - the coming age of collaborative computing. See https://tinyurl.com/wphvv2tj

Why do we need PETs?

The ability to turn data into actionable insight is incredibly important.

In business, a data-driven understanding of customers, competitors and markets is crucial in determining where and how to focus your efforts and capital. In a broader social context, data informs the planning of major projects, the provision of social services, and much more.

However, data can sometimes be a liability.

Whenever you acquire data, you also take on the responsibility for its management. Protecting data, especially sensitive data such as personally identifiable information (PII), is becoming legally critical at a global level. The objectives of a good data strategy are not just to maximise your beneficial outcomes, but to minimise your potential exposure to downsides.

Achieving these objectives is often easier said than done.

Actively malicious external threats to data are only one of the many ways in which a data owner may fail to meet their obligations. Internal threats, inadvertent disclosures or software flaws also represent hazards by which an organisation can fail in its statutory duties.

These risks are products of the shortcomings in current methods for controlling access to sensitive or confidential information, yet the root cause of these failures is the fact that data protection has always ultimately relied on trust.

That might be trust in your own employees, your security management processes, even the statistical safety of a data analysis. Further afield, it might involve trusting a collaborator, a software vendor or a cloud provider.

No matter where that trust is placed or how the risks are offset, the current state of data security demonstrates that these approaches alone will never be sufficient.

At the same time, maintaining a competitive commercial edge and delivering next-generation services is increasingly reliant not only on the ability to use and learn from data, but to collaborate over information shared between organisations.

How then do we overcome the growing tension between protecting and using data? How do we expand access to data when it is already increasingly difficult to protect it?

PETs provide the answer.

While there are a diverse range of PETs, these technologies are unified in terms of their utility in contemporary data management. The principle that drives all PETs is to remove the need for trust in protecting privacy and confidentiality.

Be it through advanced statistics, cryptography or secure hardware, PETs look to create a world in which trust isn't a prerequisite to making the most of the data you hold.

As privacy laws tighten across the globe and the barriers to data movement go up, PETs represent not only a vital tool for satisfying new restrictions, but an opportunity to re-shape the way in which organisations and societies approach data.

What do PETs mean for businesses?

Regardless of how you approach PETs, these technologies are set to have an impact on all businesses. Most data privacy laws around the world incorporate language similar to that of Article 25 of the GDPR, which obliges data controllers to ensure their security standards reflect the contemporary state of the art.

Gartner predicts that, by 2025, 60% of large organisations will be using at least one PET technique.

Nations are increasingly alert to the importance of the data they keep and generate, not only on behalf of their populations and industries but as a matter of national security. As PET adoption grows and the barriers to entry fall, some data security methods and frameworks that were once considered acceptable will no longer meet increasingly strict standards.

Engaging with PETs will eventually be essential, and early comprehension of their function in organisations will help users plan this transition effectively.

However, rather than representing a burden on businesses, PETs represent a vital lifeline in navigating a global privacy and confidentiality landscape that is simultaneously becoming stricter and more fragmented.

In this world, PETs will serve as vital channels connecting not only collaborative partners, but even the operations of multinational organisations operating under different legislative regimes.

2/3rds of the data gathered by enterprise goes unused.[2.]

At the same time, the ability to work without trust as a prerequisite will open new possibilities. From breaking down internal data silos through to safely and collaboratively sharing datasets, PETs offer not only greater access to data, but greater ability to automate sensitive data processes.

What's the value of this opportunity? Market research suggests an estimated $53Bn addressable market for FHE services alone by 2030. However, this is contingent on the scalability of FHE processing.

Despite the value of PETs, the question of how to engage with these opportunities is typically less clear. Navigating this space is not just a technical question. It involves awareness of developments in the PET space, the view of regulators, and an ability to connect to end-users.

Expanding access to FHE and assisting in this associated navigation is one of the primary objectives of the Optalysys Accelerator. It is our view that the advantages of PETs should not be restricted solely to those organisations who traditionally work with data privacy. Regardless of your prior engagement or awareness of PETs, the Optalysys Accelerator is designed to assist your business.

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

What is FHE, and why is it a useful PET?

In the modern world, cryptography is essential to data security. Amongst many other things, cryptography is used to protect information passing through the internet, validate user identities, and authenticate messages. Cryptography is a powerful tool, as mathematical secrecy is the only method of information protection that can provide security that extends beyond simple trust.

Encryption is a cryptographic process by which information is concealed. This is done by applying mathematical operations to data in a way that obscures the original content. Crucially, these operations are typically nearly impossible to reverse without knowing a particular piece of information.

By controlling access to this information, the authorisation to view and use encrypted data can easily be delegated to authorised parties.

Proper use of encryption and other forms of cryptography is essential for the operations of every business that receives and manages data. However, for all that contemporary encryption is tremendously powerful, it does have a flaw.

As encryption relies on making information unreadable, most encryption methods have to be reversed (decrypted) before data can be used. This aspect of encryption means that calculations on data have always involved removing the protection of unreadability.

FHE is a method of encryption that still allows computation on encrypted data. Data can now benefit from mathematically strong protection at every stage: in transit, in storage, and in use.

Based on quantum-resistant cryptography, FHE will also remain suitable for use even under the forthcoming changes to the security landscape that will be driven by quantum computing.

FHE is powerful, but slow: Approximately 1 million times slower than regular computing

As a data protection technique, FHE offers exceptional security. As a collaboration tool, FHE is incredibly versatile. By allowing arbitrary computation on encrypted data, it not only allows us to replicate the existing tools and processes that are used to analyse data (including machine learning models), but to apply these tools over shared data-sets.

FHE also allows for a great variety of data access models. For example, multi-key FHE enables many data holders to contribute data to a single computation. This makes FHE suitable for use in safely aggregating and using data held by IoT and mobile devices, amongst many other applications.

However, the abilities of FHE have until now come at a steep cost. On conventional computing systems, FHE requires massively increased processing and runtime.

Current estimates vary depending on task, but calculations performed under FHE are generally accepted to be 1 million times slower than computing on unencrypted data. The cost and speed of FHE has thus far restricted the uptake and development of this technology.

With the arrival of dedicated FHE accelerator hardware powered by Optalysys chip-scale optical processing technology, the final barrier to commercial exploitation of FHE can be removed.

The Optalysys Accelerator

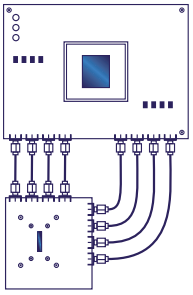
FHE offers significant advantages as a PET, but providing the computing capabilities needed to bring it to scale will require dedicated hardware.

Optalysys' proprietary hardware acceleration for FHE brings the exceptional capabilities of our optical computing technology to bear on the extremely high computational workload of FHE. The photonic components of our system are designed to greatly accelerate the numerical transform operations that are critical to FHE, and to do so with considerably less power draw than conventional electronics.

Throughout 2023, we will be providing access to the first dedicated hardware acceleration capabilities for FHE.

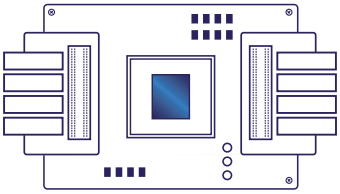
Accelerator resources

Stage 1



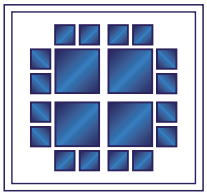
Discrete photonic - electronic solutions

Stage 2



Pluggable optical compute units with electronics

Stage 3



Optalysys Enable™: photonic-electronic integrated system

Access to hardware is provided at the earliest opportunity, and ranges from our first photonic-electronic systems capable of providing an accelerated end-to-end FHE workflow, through to ongoing developments in system integration culminating in our commercial-grade solution for FHE at scale: Optalysys Enable™.

Optalysys hardware is designed for integration with existing FHE libraries and toolchains. No specialist optical computing knowledge is required to exercise the full advantage of our photonic systems in accelerating FHE workflows.

Alongside access to hardware, the Optalysys Accelerator also provides technical support resources including manuals and tutorials for using our core technology to solve the most demanding problems.

Optalysys

Engagement Framework

Optalysys provides hardware designed specifically to address the intensive computation involved in FHE. With the computational restriction on scalability removed, the path forwards is now determined by the goals and objectives of end-users of FHE and other PETs.

We see two distinct routes to success in deploying FHE. Our Accelerator engagement framework is designed to work with you, enabling you to make the right choices for your application sector.

Route 1: Platform solutions

Some organisations will want to work with established solutions providers in the PET space.

This approach not only accelerates your roadmap to FHE adoption, it eliminates the need to bring significant technical and privacy expertise into your business.

This is especially valuable, as such talent is in globally short supply relative to the opportunities posed by FHE.

For organisations where advanced privacy techniques aren't a primary competency, using a dedicated solution can help to manage risk and liability.

Route 2: Development

Other organisations will see opportunities to innovate within their sector and will pursue the creation of bespoke FHE products and applications.

This introduces the dual challenge of cultivating or onboarding talent, and a potentially lengthy development process.

However, the tools for creating and deploying FHE applications have become increasingly user-friendly, and the barrier to access is dropping rapidly.

The Optalysys view on integrating PETs with business

When developing a solution, we take into account not only the technical aspects, but give significant thought to how that solution works within your business.

While no two businesses are the same, for organisations looking to adapt to the PET space we generally recommend the development of a specialist unit dedicated to managing and enhancing your data usage through PETs. This is motivated by the following reasons:

- Firstly, the collaborative opportunities that FHE enables will require inter-organisational agreement on the format for data exchange and protocols. A dedicated team will have the agility to adapt to the evolution of these protocols and any surrounding regulatory activity without impacting upon your core day-to-day operations.
- Secondly, a dedicated unit segregates the need to understand advanced privacy

principles and technologies, reducing the scale of change management and training needed over the whole business.

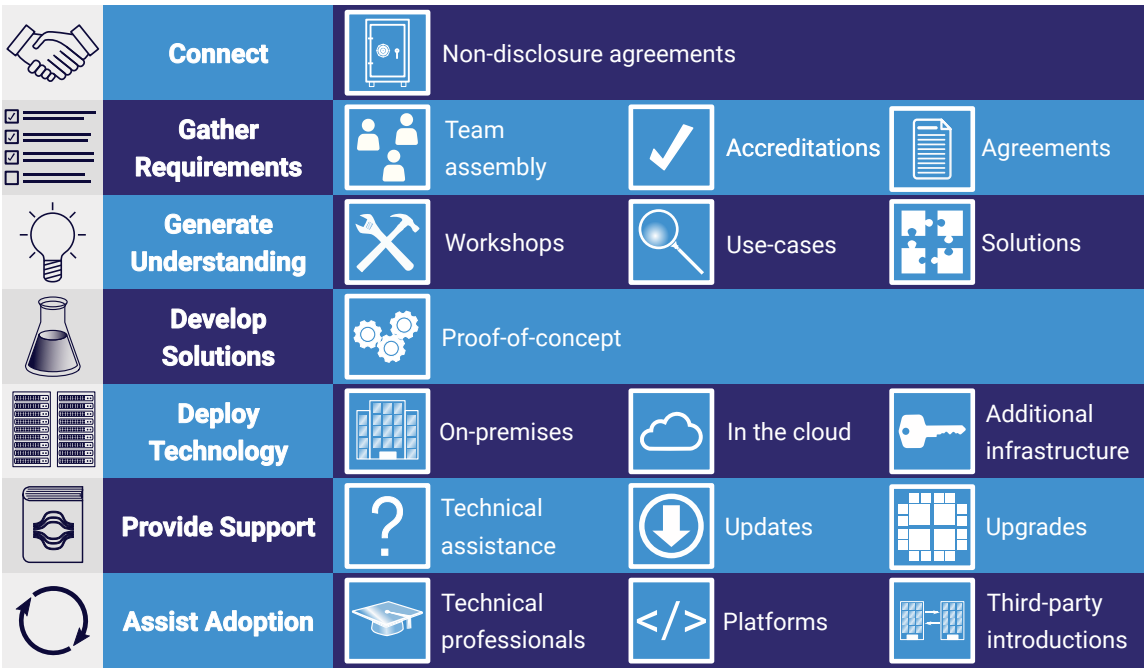
- Thirdly, the technology stack for FHE is novel, and integrating these technologies into existing tools and workflows will pose challenges. Conversely, ground-up design of systems and working practices for privacy will eliminate technical points of friction that might otherwise arise.

Optalysys supports these outcomes by providing ready integration of FHE libraries and services with existing technologies and practices in cloud integration, allowing dedicated business units to work with contemporary methods in information technology and focus on delivering outcomes from day one.

Regardless of your preferred route, hardware acceleration is key to realising the benefits of FHE at scale. The Optalysys Accelerator is designed to provide not just access to the necessary high performance hardware, but to assist in connecting your business to solutions that work.

So how do you engage with us, and what does that look like?

We define 7 distinct stages to the Accelerator program that encompass everything from initial contact through to ongoing support for mature FHE applications. The long-term objective of the accelerator program is to assist you in developing early use-cases and example models, and carrying these through to operational solutions.



In the process, we enable you to navigate the next-generation FHE landscape while delivering the optimal impact for your business. The figure above shows an at-a-glance overview of our Accelerator framework on a stage-by-stage basis, alongside a summary of what each stage entails.

Optalysys

How to engage

Access to the Optalysys Accelerator is open to many different sectors. For further details or to arrange a meeting to explore the Accelerator opportunity further, please contact us at

info@optalysys.com

or via our contact options at www.optalysys.com.

Conclusion

PETs offer a radical opportunity, not only to address major deficiencies in information protection, but to fundamentally alter how we approach the utility of data. Technological advances will be critical for realising one of the most valuable PETs in the form of fully homomorphic encryption, as conventional electronic systems and off-the-shelf accelerators cannot deliver the acceleration or power efficiency needed for FHE deployment at commercial scale.

Optalysys optical computing accelerators are an enabling technology for FHE. By leveraging next-generation techniques in silicon photonics and conventional electronics, a 10,000x acceleration of FHE workloads is now practically realisable.

By providing acceleration for all FHE schemes through interfacing with mature and widely used FHE libraries, Optalysys hardware accelerators offer a solution which is both scalable and user-friendly.

The opportunity to engage with this technology is now open. The Optalysys Accelerator is the first framework of its kind dedicated to placing hardware acceleration for FHE in the hands of end-users. In light of the remarkable capabilities of PETs and the necessity of engaging with these technologies, engagement with this framework offers an exciting opportunity for the future of your business.


Optalysys