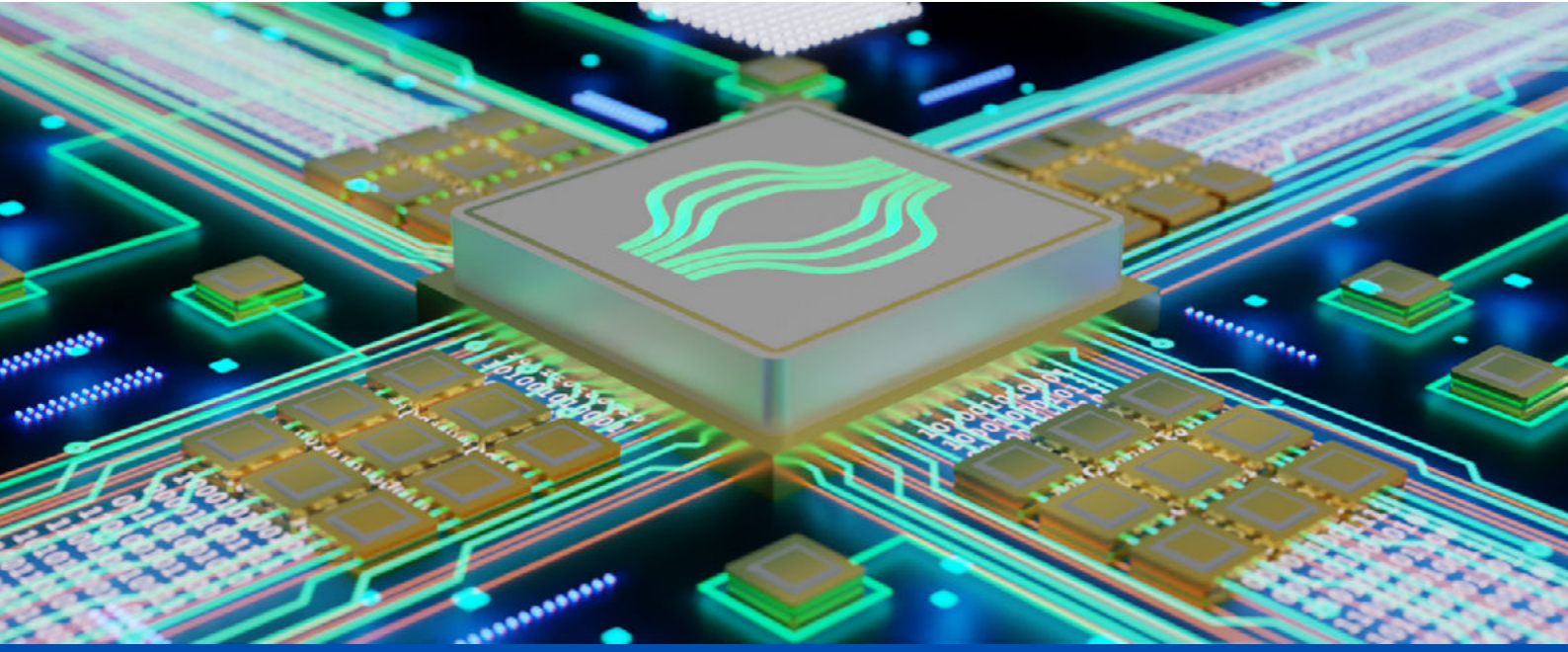
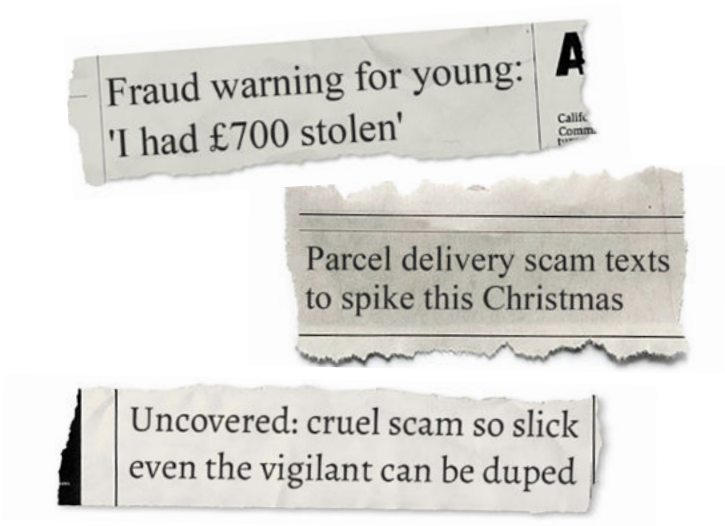


Optalysys

Public introduction to FHE

Cybercrime has always been a major security challenge, but the COVID-19 pandemic saw an explosion in digital fraud. You've probably seen news reports like these, warning of the dangers of unsolicited contacts:



You may even have received scam texts like the one above, which typically start a chain of elaborate events targeted to scam you into handing over money to committed fraudsters.

That scammers can readily find our phone numbers is a concept many of us are familiar with, but some of these scams are extraordinarily complex...

Fraudsters can often gain access to and make use of information that most of us would consider private and confidential, such as our card or banking details, to convince us that they're legitimate. But where does this extra data come from, and how do scammers get their hands on it?

Some scammers find personal details through phishing attacks or by trawling social media, but most sensitive information, like banking records, for example, is sourced or 'stolen' as a consequence of data breaches within the very businesses and organisations that we entrusted our information

to in the first place; we routinely share facts about ourselves regularly. Everything from signing up with your energy provider to transacting with online shopping sites requires that you submit your details.

However, even if the company itself is honest, cybercriminals frequently identify ways of accessing their systems to steal this information. If successful, they then sell this information on to other criminals, who may use this information to convince you to send them money or to acquire products and services online. Other end-users of stolen data might use this information to steal your identity.

The world of scammers and cybercriminals is often murky and hard to understand, but research frequently reveals some shocking statistics. You might think that high-quality stolen information would be quite expensive, but it can be bought for remarkably small sums. Prices vary depending on the nature and quantity of the data, but stolen credit card details alone are sold for an average sum of just $17, while a full package of information (including the cardholder's street address, birth date and more) is worth less than a dollar more.

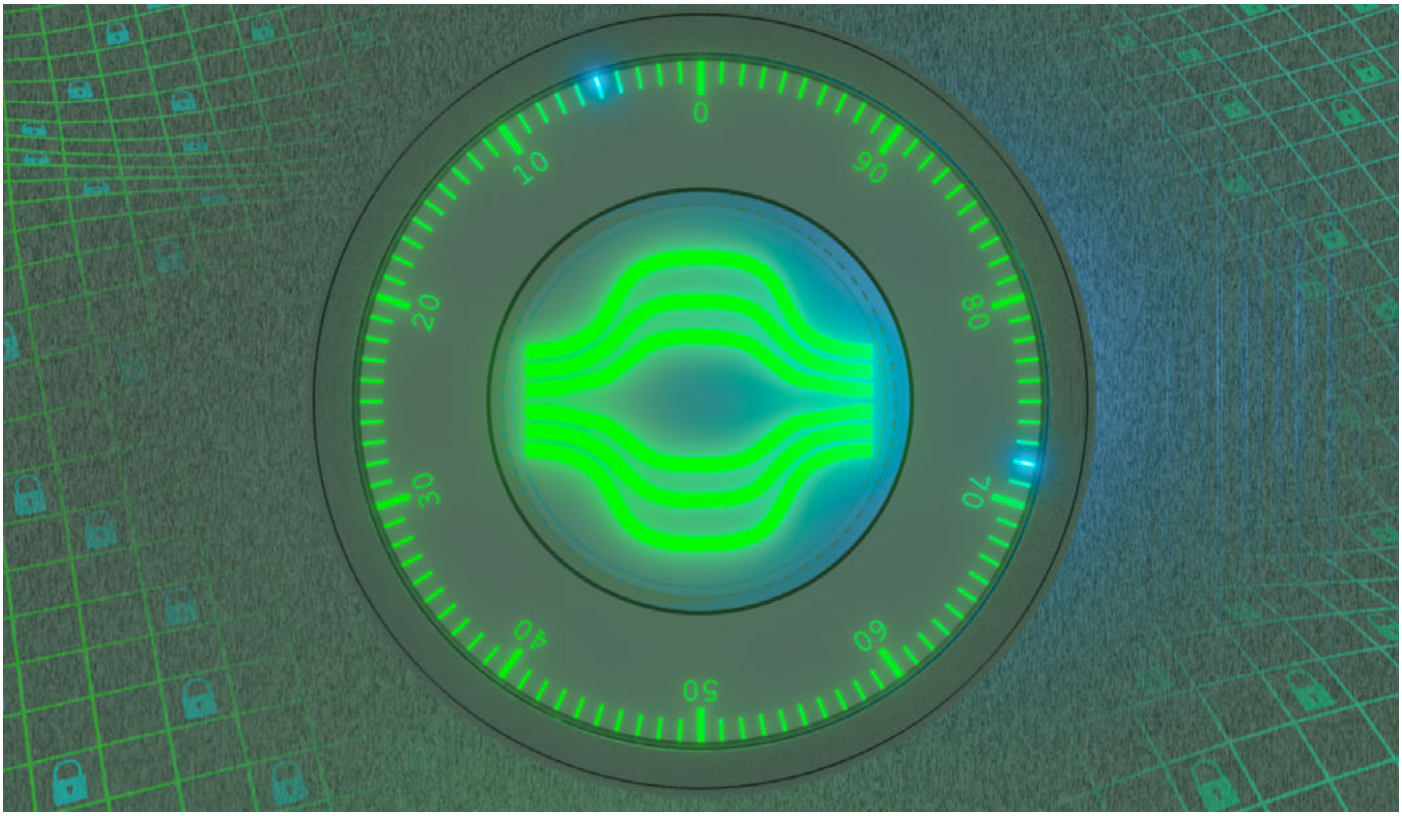
The reason this information sells for so little is that data breaches are hard to prevent, far more frequent than most of us realise, and not always publicised. Keeping this information safe might be challenging, but organisations that collect this kind of data have a legal, moral, and ethical responsibility to do so.

Encryption has proven to be the ultimate method of keeping this kind of information secure, a process that uses complex mathematics to modify information (encode), rendering it unreadable unless you know the secret information (code) that reverses the encryption. Notionally, this means that the problem of protecting large amounts of data can be reduced to protecting only a few pieces of secret information, a far more manageable and affordable task.

The value of encryption

This is why encryption is used everywhere in the modern world. When you communicate with secure websites online, such as your bank or email provider, you do so by exchanging encrypted information. This prevents things like passwords and bank details from being intercepted as it passes through the internet. On a broader scale, encryption is responsible for protecting everything from military communications to medical records.

Encryption is an essential tool in preventing data breaches; even if hackers can gain access to a system and steal the information, good use of encryption would still prevent them or anybody else from being able to read or understand it, making it worthless for criminal purposes.



Such is the role of encryption in preventing breaches that failing to use it is considered negligent. For this reason a major UK telecoms provider was fined £400,000 for a breach in which 4,545 customer records were leaked, a breach that was only possible because the company failed to encrypt some of the data that it stored.

It is tempting to think that breaches can be prevented with proper data management and that the only reason data is stolen is because some companies don't get it right. Whilst that's certainly part of the problem (and it's a huge problem in its own right), there are bigger and more fundamental challenges in keeping your information safe...

Modern software is incredibly complex and usually consists of multiple pieces of software that handle common tasks. Even if a company does everything right, it is still possible for a vulnerability to lurk undetected in one of these smaller building blocks of software. This is exactly what happened with the infamous Log4J vulnerability:

www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

A widely used tool that was a small but important piece of many software packages that turned out to contain a devastating bug that placed millions of systems and devices at risk. While companies can move quickly when vulnerabilities are discovered, that doesn't help if they can be used (possibly for years prior to their "official" discovery) to break into even the most well-designed and managed systems.

Even though the impact of vulnerabilities like Log4J can be mitigated through encryption, it's still not enough to prevent breaches fully. The hardest problem to solve in data protection comes from the nature of encryption itself. Because encryption protects information by making it unreadable, it means that computers also can't understand encrypted data.

When is data vulnerable?

Modern encryption is excellent when you want to protect information at rest in a database or when it travels through the internet, as storage and transmission systems are indifferent about the actual content of data.

However, whenever a computer needs to process data, make changes or run calculations, the content does matter. This seems intuitive; for example, if you were asked to add two numbers together, you would need to know which numbers to add.

Current methods of encryption, therefore, need to be reversed ("decrypted") before the computer can work on the data. This means that there's always a point in even the most secure computer systems where information is necessarily vulnerable.

The conventional picture of a data breach is hackers gaining access to systems that they don't have permission to enter. Encryption, as described above, can help to keep information safe from these threats, but it is far from perfect; if you're utilising data, there is always a point where hackers can strike. This, however, isn't the only threat...

Sometimes, it is people within companies who access, steal and leak information. Trusting companies to keep attackers out is one thing but trusting every single employee in a company is another. When it comes to the most important, sensitive, and confidential secrets, it is nearly impossible to achieve this level of trust, even with encryption.

In light of these challenges, it has never been possible to keep information entirely safe from criminals. However, a major advance in cryptography looks set to change everything...

Encrypted computing

This advance is a new method of encrypting data in such a way that you cannot actually read it, but you can perform operations with it. The trick lies in finding a mathematical problem that can be used to hide data while also preserving the structure of that data.

Under this model of encryption, you can perform any operation that you can with a regular computer, but without ever exposing the data to vulnerability through decryption. This doesn't just protect information against hackers, it even

protects it against the very machine that is doing the calculation. Even if the company that owns the machine (or individual employees) wanted to snoop on your data, they'd be unable to do so; because the raw data is never decrypted, it's never vulnerable. Only the output of the calculation can be seen.

This technology is known as Fully Homomorphic Encryption or FHE. When information is encrypted using FHE, it is possible to add or multiply the encrypted information together. Even if we perform many additions and multiplications, when we decrypt the output, the result is the same as if the operations had been performed on unencrypted data.

Any computing operation can be constructed using these processes alone; by enabling sequences of addition and multiplication on encrypted values, we can construct complex tasks (such as AI) as encrypted processes. We can even process and search encrypted text!

If all data held by companies was encrypted using FHE, the ability of cybercriminals to steal information would be virtually eliminated. FHE is also based on a method of encryption which is known to be resistant to attacks from next-generation quantum computers (a problem that currently threatens some existing encryption methods), providing the important benefit of security future-proofing.

How fast is encrypted computing?

FHE allows us to perform confidentiality-preserving computation by preventing anybody from being able to see information at any point, including

during processing. Until now, FHE operations have taken place on very large pieces of encrypted data, which are very different to the data that regular computers were designed to work with.

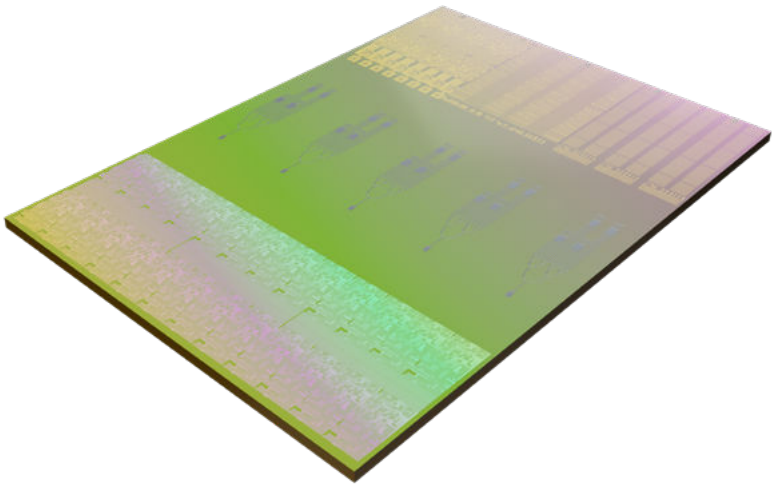
The calculations themselves are also incredibly mathematically intensive. The result? FHE computing has historically been approximately one million times slower than regular computing. When we think about the massive quantities of data that are produced every single day, it's quite clear that established FHE cannot keep all information both safe and usable.

However, one pioneering UK company is set to revolutionise the FHE process...

FHE meets optical computing

At the heart of all FHE calculations is a very specific mathematical function that is used to perform large multiplications. When running on standard computing hardware, this single function accounts for between 70-90% of the enormous processing capacity required for performing FHE calculations. It has hitherto been impossible to make this function run faster on conventional electronic hardware. However, it's also an operation that can be performed using the properties of light...

Optalysys Ltd is a company based in the United Kingdom who have pioneered the merging of optical computing, where information is processed through manipulating light, with next-generation FHE cryptography. Optalysys have been developing optical computing systems dedicated to performing this particular function for nearly a decade, and they've recently set their sights on the enormous benefits to FHE, and in particular, data security.



Optalysys have designed a special kind of computer chip that controls light and uses it to perform the main mathematical operation in FHE, allowing them to speed through calculations that standard electronic computers find so challenging. By designing a specialist accelerator system around this technology, they can massively reduce the runtime of FHE down to near the same speed as unencrypted computing.

By enabling ultra-fast FHE, Optalysys have uniquely developed information security technology that provides a permanent solution to the problem of data breaches and leaks of information.

For more information on what Optalysys are doing, visit www.optalysys.com