Communications of the ACM

News

Computing Applications

Homomorphic Technologies Could Process Still-Encrypted Data

Computer scientists are advancing FHE technology that enables the processing of data while preserving its privacy.

By Mark Halper

Posted Jun 4 2025

Feedback

Imagine a home security safe with a valuable necklace locked up inside. The owner wants to add a diamond to the pendant, but doesn't want to open the door.

That would be impossible.

Yet in a crude analogy, the same general sort of thing is plausible in the digital world of encrypted data. Computer scientists are advancing the technology of "fully homomorphic encryption," which enables the processing—albeit, not the changing—of data while it is under lock and key.

The concept of fully homomorphic encryption is a Holy Grail that has been around for decades. Pursuit of it picked up in 2009 when Craig Gentry, then a Stanford University Ph.D. student and an IBM researcher, and now chief scientist of algorithms at Dallas-based FHE chip developer Cornami, published a paper widely regarded as a proof of concept.

The potential benefits are enormous, especially with AI giving rise to a wave of data which, if protected homomorphically, increases in value and usefulness.

Fully homomorphic encryption (FHE) would allow businesses, governments, research institutions, universities, and other entities to share data that today they cannot share, owing to privacy obligations. With FHE, processors could skim out relevant information that reflects general trends, while not revealing confidential details—and without changing the dataset.

For instance, banks could analyze trends that might reflect money laundering or scams, while keeping individual customer account information secure. Medical researchers, in their quest for cures and ments for cancer, dementia, or just about any illness, could share more information than ever before hospitals and universities, without violating patient confidentiality.

And in a different vein, FHE could also stave off what many believe to be the coming security threat posed by quantum computers, which will likely be able to decrypt much of the world's data as it currently is encrypted. Today's encryption technology, such as the venerable RSA cryptosystem, is based on an "integer" approach, deploying prime number formulas that essentially cannot be hacked with today's computing power. But the heavy artillery of quantum power, once it arrives, could smash through those algorithms.

FHE is not integer-based; it uses a "lattice" structure believed to be far more resilient.

Hold the quantum hacking thought for a moment and simply try to comprehend the logic-defying principle of homomorphic encryption.

"FHE extends that kind of protection that you get from encryption today," said Joseph Wilson, head of strategic innovation for U.K. secure computing company Optalysys, which is developing an optical chip to help usher in FHE. Said Wilson, "For the first time, you get protection for data when it's in transit, when it's at rest, and when it's in use."

On the other hand, "This idea of processing encrypted data without decrypting it, it's nearly an oxymoron," said Rosario Cammerota, senior principal engineer and chief scientist of privacy-enhanced computing research at Intel Labs' Emerging Security Lab in Hillsboro, OR, which is also working on chips to make FHE possible.

This variation of encryption is called "homomorphic" because the data does not change during computation. "Homomorphic" is a mathematical term for that uniformity (the data's morphology remains homogenous). The necklace in the safe noted above is a crude analogy because FHE computations do not alter the encrypted data; they would not add anything to the pendant, but they do extract meaningful data representations without cracking open the analogous steel box.

A Need for Speed

Here's the rub: processing technology as it exists today is too slow to support mainstream, real-time adoption. FHE needs far more speed than is generally available, in order to cut through all of the "noise" that programmers code into homomorphically encrypted data. Noise is a vital ingredient of any encryption scheme, but there is far more of it in FHE compared to other encryption types.

While FHE development has made impressive software strides since Gentry's seminal paper, it needs a hardware kick, he said.

"I have this graph of where we were in terms of performance in 2009," said Gentry. "It's a very steeply improving line for FHE. Performance has been getting much, much better, faster than Moore's Law. But similar to Moore's Law, in terms of algorithms, it's kind of plateaued recently. The way we're going to get better performance is basically through hardware acceleration."

"Speed remains the primary challenge, but the lack of infrastructure is also a deterrent," said Josh Benaloh, senior cryptographer for Microsoft's Microsoft Research division. "If FHE is to be broadly used, it must be both efficient and seamless."

Digressing from speed for a moment to consider the “infrastructure” and “seamless” points, Microsoft is one of several outfits offering an open library of software to help programmers develop applications that can be protected by FHE. So is Duality, a Hoboken, NJ, company that oversees the aptly named OpenFHE library. IBM also has an open library, which it is using to develop FHE into its z/OS mainframe operating system.

The Microsoft version is called Simple Encrypted Arithmetic Library (SEAL). The software giant has used SEAL in combination with open Asymmetric Private Set Intersection (APSI) software to program an FHE feature into its Edge browser called Password Monitor. The product, which is in use today, checks a user’s saved password/username combinations against data breaches and sends alerts to the user when suspicious action is detected.

Password Monitor, like other implementations of FHE, does not operate in real time; it sends alerts after the fact. In a trial example of non-real-time FHE, Brazilian bank Banco Bradesco S.A. in 2019 tapped IBM to homomorphically encrypt accounts in a way that hid account holder identities while the bank extracted account activity information and used machine learning to predict whether an account holder would soon need a loan.

Other trials of FHE, none of them on a real-time basis, have included a South Korean government project with Seoul National University comparing data from different government agencies spanning health, pension, and financial credit information in an effort to improve the country’s credit rating system. Also, in 2022, the government of Singapore ran a trial in partnership with Mastercard to detect money laundering schemes.

While these examples support the notion of FHE’s viability, most FHE developers maintain that the technology’s day has yet to arrive and will not until processing speeds increase so that it can be used in real-time cloud computing operations, rather than being relegated to back-end and batch procedures and long-term data analysis.

“There is promise of greater use of FHE in the future, but efficiency is still not good enough for widespread use,” said Microsoft’s Benaloh.

“The hardware that’s been built up to now has just not been suitable for fully homomorphic encryption,” says Intel’s Cammerota.

“FHE is not good for real-time analytics,” notes Sridhar Muppidi, IBM’s vice president and chief technology officer of software security. “So the adoption has been slow. I see more and more adoption, but it’s not a mainstream technology yet.”

Limited forms of homomorphic encryption (“partial” and “somewhat”) are more common than full homomorphic encryption. Partial encryption, which is what Microsoft uses for its ElectionGuard voting software, can encrypt one mathematical operation at a time.

Forsaking Von Neumann

Exactly how much faster things need to be for "full" homomorphic encryption is a matter of lively discussion. IBM's Muppidi said there is no one answer, that it depends on the use case, each of which will involve its own algorithms. While business-to-consumer financial applications might require response times in fractions of seconds, some business-to-business environments might settle for slower speeds.

Duality co-founder and chief technology officer Kurt Rohloff also suggests some deployments won't require as much speed as others. For example, FHE used to assure compliance with data-sharing regulations might be a comparatively slow version, but could still be much faster and less expensive than deploying teams of lawyers to do likewise.

Either way, acceleration is in order. To that end, any number of companies are developing processors aimed at seriously picking up the pace. Those include Cornami Intelligent Computing (where FHE scientist Gentry now works), as well as Intel, IBM, Optalysys, Niobium, and others.

In a radical approach, Cornami is forsaking the von Neumann architecture that has defined chip design. Cornami co-founder and chief technical officer Paul Master characterizes today's CPUs and GPUs as "sloshing" data back and forth between different sections of the chip such as cache, memory, and registers. Cornami is designing a chip that "streams" rather than "sloshes," and that it claims can support hundreds of thousands of operations at a time.

"Right now, the only tools to run FHE are CPUs and GPUs," said Master. "Do they run it efficiently? No, they do not." Advanced algorithms such as those associated with FHE "don't play nice with existing von Neumann machines," he said, adding that Cornami is designing its chip with flexibility to work different FHE protocols and algorithms.

Cornami has not yet given its chip a name but expects to make it available sometime this year, with first adopters likely to be in the financial industry.

Abandoning von Neumann would be a notable development at chip stalwart Intel. So is it doing something similar in pursuit of a faster, FHE-suitable chip?

"Yes, there is an aspect of this," said Cammerota. "Homomorphic encryption requires a different type of computation. It requires a much larger amount of parallelism." He noted that the communications layout of the chip also departs from tradition designs. "At the end of the day, the design paradigm that we used for the chip is completely opposite compared to what you would use in traditional hardware that exists on the market today. That was a surprise for us, to be honest."

Intel expects to release prototypes of the chip later this year. Cammerota declined to commit to a commercial timeline. "That depends on the pull from the market and from business," he said, while also describing FHE as "one of the top big bets within Intel."

Another company working on the FHE chip challenge is Dayton, OH-based Niobium.

"The computing power required to operate on encrypted data is much higher than on regular data," noted Jorge Myszne, who until recently was chief product officer at Niobium. So Niobium is developing an

accelerator chip leaping well beyond the 64-bit architecture common on today's processors, and deploying somewhere in the thousands of bits (the company declines to state the precise number).

At Leeds, U.K.-based Optalysys, the approach is optical. The company is working on a hybrid electronic/photonic accelerator chip that, Wilson says, will increase speeds around 10,000-fold. The company expects to offer the product by 2028 but plans to release other accelerators before then. Like Niobium, it is widening the bit size beyond 64.

Optalsys plans to start production of an FPGA this year, and of an ASIC next year.

Optalysys is also widening the bit size to several hundred. In an FHE knowledge-sharing move, it formed a consortium last October (announced at the ACM Conference on Computer and Communications Security in Salt Lake City) with Niobium and Israeli company Chain Reaction. The group, called FHETCH (the FHE Technical Consortium for Hardware), is inviting other members to join.

All for One

FHETCH is indicative of what Wilson calls a broader need for an ecosystem that supports development of FHE across hardware and software. He noted that in today's RSA- and integer-oriented environment, "People who develop the software very rarely have to engage with the nuts and bolts of encryption; they use standard encryption libraries, standard protocols."

With that in mind, Wilson asked, "How is FHE going to do the same trick? We don't want people to have to become cryptographers to work with it. How do you get to the point where all of this complexity, all of this expert understanding, is condensed and captured in tooling and the ecosystems that will allow the devs of tomorrow to work with this?"

Noting that FHE poses a whole new programming environment because it "merges computing and encryption," he points out the need for working together. And that is precisely the idea of the open FHE libraries, such as OpenFHE overseen by Duality, a company that while shepherding the library, is itself working on accelerator chips.

Duality's Rohloff said he believes computing is "on the cusp" of more widespread FHE deployment.

"A lot of these hardware solutions are nearly there," he noted, looking forward to the social and economic benefits, which he described as "supercharging and democratizing data access for the good of society, with lower costs and higher protection."

Then there is the other great promise of FHE: keeping data safe from the power of prime number-busting quantum computers.

FHE is not the only security technology that could be up to the task. There are others which, like FHE, abandon the classic integer architecture in favor of a lattice approach. Some FHE enthusiasts claim FHE is the best potential solution suited to protecting large datasets.

Cornami's Master observed that the quantum threat to encryption "is a ticking time bomb." A technology like FHE could serve to defuse that "bomb," while unleashing new revenue streams and social benefits by greatly increasing the value of safely shared data.

Mark Halper *is a freelance journalist based near Bristol, England. He covers everything from media moguls to subatomic particles.*

Join the Discussion (0)