A high-powered processor for cutting-edge encryption

February 27 2023, by Julia Cohen

Credit: CC0 Public Domain

Recent advancements in cryptography have allowed for something exciting: algorithms can now do direct computation on encrypted data thanks to Fully Homomorphic Encryption (FHE).

What does this mean and why is it exciting? Traditionally, sensitive data

is encrypted, and in order for it to be used for any type of analysis or computation, it needs to be unencrypted. While in the unencrypted state, the analysis or computation is performed, and once that's complete, the sensitive data is re-encrypted.

"The problem with those schemes is that, inevitably, there's a breakdown in the process and somebody can snoop and see the unencrypted processing, or somebody forgets to re-encrypt it," said Matthew French, Research Director at USC Viterbi's Information Sciences Institute (ISI), describing some potential vulnerabilities of traditional encryption.

Over the past decade, there have been revolutionary advances in algorithms resulting in FHE, which enables computation directly on encrypted data. "Using FHE, there is no longer any need to decrypt and re-encrypt the data, resulting in a much more secure system," said French.

What's the catch?

Computing power. FHE needs a significantly greater amount of computing power to perform operations equivalent to unencrypted operations. Orders of magnitude greater. FHE requires roughly 100,000 times more computation than traditional approaches so, for it to be useful, FHE must close the computation gap.

French and his team took on the challenge. "Our co-processor, code named TREBUCHET, addresses this by developing custom computer hardware to accelerate FHE processing with the goal of getting within ten times of traditional processing speeds," said French.

Their resulting paper, TREBUCHET: Fully Homomorphic Encryption Accelerator for Deep Computation was recently accepted for oral presentation at the 2023 Government Microcircuit Applications and

Critical Technology Conference (GOMACTech-23) in San Diego, California.

A team effort

TREBUCHET was developed for the Defense Advanced Research Projects Agency (DARPA) DPRIVE Program (Data Protection in Virtual Environments). The team includes both private research facilities and a number of academic institutions. Duality Technologies is the prime, joined by USC Viterbi's ISI and Ming Hsieh Department of Electrical and Computer Engineering, New York University, Carnegie Mellon University, SpiralGen Inc., Drexel University, and Two Six Technologies.

David Bruce Cousins, Duality Labs director and principal investigator for TREBUCHET said, "Duality team members have been supporting DARPA-funded innovation and application of FHE for over a decade. Some members of our team developed the first ever prototype HE hardware accelerators under the DARPA PROCEED program starting in 2010."

He continued, "ISI is an ideal partner in TREBUCHET, bringing with them a great deal of experience in developing custom ASICs for DARPA-hard problems. Such projects always require creative solutions to challenging requirements—which may change during the program."

It comes down to a hardware problem

Traditional computers operate on 64-bit data. FHE requires something much larger than that (128 to 4,096 bits). Furthermore, all math is done using modular arithmetic (where numbers "wrap around" upon reaching a given fixed quantity to leave a remainder). This meant the team would

need to significantly rework the computer architecture. And whatever changes were made, had to be done within the limits of modern chip fabrication.

The team developed a novel tile-based chip design with highly parallel Arithmetic Logic Units (ALUs) to answer the problem. They expanded the ALU to support wider data words; fast modulo arithmetic circuits were added; on-chip networks were widened; and memory architecture and management were redesigned.

The TREBUCHET co-processor provides a highly modular, flexible, and extensible FHE accelerator designed for easy reconfiguration, deployment, integration and application on a wide range of chip sizes. And it provides runtime performance orders of magnitude faster than other solutions.

Privacy, privacy, privacy

Secure computation is critical to the Department of Defense, across financial institutions, healthcare, and anywhere personally identifiable information is accessed. Which means unlocking the computing power to allow for FHE will have major impacts.

French offered an example in the medical field, where patient data could be more readily shared securely to help accelerate research in public health issues, cancer research, etc.

"If you wanted to share the COVID-19 data that the National Institutes of Health has on patients, using FHE you don't have to worry about HIPAA compliance. People can do all their analysis directly on the data while it's encrypted, and not be concerned about people's sensitive data getting out."

Another area of interest has come from the financial crimes investigation sector. French said, "We've seen a lot of interest in the financial crimes area because there's a concern there that once you start searching certain people to see if they're laundering money, they have insiders that are tipping them off and then they move the money." Searching those people using FHE would prevent the tip off.

He continued, "Trebuchet could even support secure monitoring and control of our modern communications and networking systems and power grid."

What's next for TREBUCHET?

The DARPA DPRIVE program recently completed a competitive downselect, and the TREBUCHET team was one of three selected for Phase 2. The first phase of the project concentrated on developing a custom ALU capable of accelerating FHE operations. The second phase will focus on scaling this to the full device level.

"Bringing near-real time computation of FHE applications will have a dramatic impact. I think we're just scratching the surface with the types of applications that would benefit. As TREBUCHET is released, it will enable further R&D on the application side as end users will be able to experiment more broadly. Some of my colleagues in other divisions at ISI are so excited, they knock on my door almost every week asking when the chips will be ready so they can start using them," said French.

Provided by University of Southern California