March 8, 2021

Intel to Collaborate with Microsoft on DARPA Program

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Intel today announced that it has signed an agreement with Defense Advanced Research Projects Agency (DARPA) to perform in its Data Protection in Virtual Environments (DPRIVE) program. The program aims to develop an accelerator for fully homomorphic encryption (FHE). Microsoft is the key cloud ecosystem and homomorphic encryption partner leading the commercial adoption of the technology once developed by testing it in its cloud offerings, including Microsoft Azure and the Microsoft JEDI cloud, with the U.S. government. The multiyear program represents a cross-team effort across multiple Intel groups, including Intel Labs, the Design Engineering Group and the Data Platforms Group, to tackle "the final frontier" in data privacy, which is computing on fully encrypted data without access to decryption keys.

> *"Fully homomorphic encryption remains the holy grail in the quest to keep data secure while in use. Despite strong advances in trusted execution environments and other confidential computing technologies to protect data while at rest and in transit, data is unencrypted during computation, opening the possibility of potential attacks at this stage. This frequently inhibits our ability to fully share and extract the maximum value out of data. We are pleased to be chosen as a technology partner by DARPA and look forward to working with them as well as Microsoft to advance this next chapter in confidential computing and unlock the promise of fully homomorphic encryption for all."* – Rosario Cammarota, principal engineer, Intel Labs, and principal investigator, DARPA DPRIVE program

Why It Matters: Protecting the confidentiality of critical information — whether personal data or corporate intellectual property — is of strategic importance to businesses. Today, many rely on a variety of data encryption methods to protect information while it is in transit, in use and at rest. However, these techniques require that data be decrypted for processing. It is during this decrypted state that data can become more vulnerable for misuse.

Fully homomorphic encryption enables users to compute on always-encrypted data, or cryptograms. The data never needs to be decrypted, reducing the potential for cyberthreats. FHE, when implemented at scale, would enable organizations to use techniques, such as machine learning, to extract full value from large datasets while protecting data confidentiality across the data's life cycle. Customers across industries such as healthcare, insurance and finance would benefit from new usages made possible by being able to use and extract value from sensitive data to its fullest extent without risk of exposure.

About Democratizing Adoption of Fully Homomorphic Encryption: FHE adoption in the industry has been slow because processing data using fully homomorphic encryption methods on cryptograms is data intensive and incurs a huge "performance tax" even for simple operations.

Under the DARPA DPRIVE program, Intel plans to design an application-specific integrated circuit (ASIC) accelerator to reduce the performance overhead currently associated with fully homomorphic encryption. When fully realized, the accelerator could deliver a massive improvement in executing FHE workloads over existing CPU-driven systems, potentially reducing cryptograms' processing time by five orders of magnitude.

With its expertise in cloud infrastructure, software stacks and fully homomorphic encryption, Microsoft will be a critical partner in accelerating the commercialization of this technology when ready, enabling free data sharing and collaboration while promoting privacy throughout the data life cycle.

"We are pleased to bring our expertise in cloud computing and homomorphic encryption to the DARPA DPRIVE program, collaborating with Intel to advance this transformative technology when ready into commercial usages that will help our customers close the last-mile gap in data confidentiality —– keeping data fully secure and private, whether in storage, transit or use," said Dr. William Chappell, chief technology officer, Azure Global, and vice president, Mission Systems, Microsoft.

What's Next: The multiyear DARPA DPRIVE program will span several phases starting with the design, development and verification of foundational IP blocks that will be integrated into a system-on-chip and a full software stack. Throughout the project, Intel will assess progress against pre-established performance targets on artificial intelligence training and inference workloads using homomorphically encrypted data at scale.[1] Beyond the development of the core technologies needed for the design of the accelerator, Intel and Microsoft will work with international standards bodies to develop international standards for FHE. Intel will also continue to invest in ongoing academic research in the field.

More Context: Intel Labs (Press Kit)

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

[1] Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20210308005131/en/

Supriya Venkat
503-320-8024

supriya.venkat@intel.com

Source: Intel Corporation