OSU cryptography research leads to huge efficiency gain in secure computing

August 19 2021, by Steve Lundeberg

Credit: Oregon State University

Oregon State University researchers have developed a secure computation protocol that's 25% more efficient than what had been thought the best possible, meaning future savings in time and energy costs for groups needing to team up on computations while keeping their individual data private.

Mike Rosulek, associate professor of computer science in the OSU College of Engineering, and graduate student Lance Roy presented their findings at this month's virtual 41st annual International Cryptology Conference, or Crytpo 2021. The conference is organized by the International Association for Cryptologic Research.

Roy, a 22-year-old who grew up in Corvallis, entered Oregon State's computer science Ph.D. program at 18, going directly from homeschool high school to the OSU Graduate School. He had begun auditing undergraduate courses at OSU at age 12.

Secure computation is often explained via "Yao's millionaire problem," a hypothetical situation developed by and named after computer scientist and computational theorist Andrew Yao in which two wealthy people want to determine who is richer but neither wants to reveal to the other how much money she/he has.

"In real life, companies and other groups will agree on a computation to run, then they do some cryptographic magic, and at the end they learn only the final result of the computation—the inputs and intermediate results of the computation remain private," Rosulek said. "One of my favorite examples is the city of Boston wanting to answer the question of whether there was a gender-based wage gap in the city's tech sector. The tech companies collectively computed the relevant aggregate statistics on their combined payroll data, but without any company needing to reveal its payroll data."

A standard technique within secure computation protocols is garbled circuits, which can come in multiple constructions. Garbled circuits are one of the few ways to achieve general-purpose secure computation protocols with just a few rounds of communication among the parties involved, Rosulek explains.

"The most efficient construction of garbled circuits is from one of my previous papers, in 2015," said Rosulek, whose Twitter handle is

@GarbledCircus. "In that paper we also gave some good evidence that this was as efficient as you could get. I really believed it was not possible to do better, and since 2015 I have been trying to prove conclusively that it was impossible to do better. This latest result was a big surprise because we showed how to actually do 25% better than that 2015 paper."

Rosulek describes Roy as the "mastermind" behind the more efficient garbled circuits, which involve insights they've named "slicing and dicing."

"I had stopped devoting any thought to trying to do better than what we did in the 2015 paper," Rosulek said. "Lance was familiar with this problem but it wasn't something we were actively working on together. I was very skeptical when Lance came to me with an out-of-the-box idea, but it turns out that his instincts were correct and he soon convinced me that his crazy new idea worked."

A normal computer circuit, Roy explains, contains gates that perform basic computations on data. In a garbled circuit, the gates have been modified—garbled—so the data flowing through them is encrypted.

In trying to prove the 2015 garbled circuit technique could not be improved upon, Roy found his proof idea was valid if a gate used all of the information contained in an input, or none of it, but not if it used some of it. That concept, slicing, shifted his thinking toward trying to improve on the 2015 technique rather than prove it couldn't be made better.

"However, I also had a new problem," Roy said. "The way that slicing works, it'd leak too much information for the garbled circuits to be secure."

A year or so later, in late summer 2020, he came up with a solution:

dicing.

"If the way the garbled circuits were built was randomized—i.e., by rolling the dice—and some other information was kept secret, the slicing idea could be made secure," he said. "Mike was really excited when I showed it to him, and during winter 2021 we refined the technique and wrote up the result."

More information: Mike Rosulek et al, Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits, *Advances in Cryptology – CRYPTO 2021* (2021). DOI: 10.1007/978-3-030-84242-0_5

Provided by Oregon State University

Citation: OSU cryptography research leads to huge efficiency gain in secure computing (2021, August 19) retrieved 24 April 2024 from https://techxplore.com/news/2021-08-osu-cryptography-huge-efficiency-gain.html