Generating zero-knowledge proofs for defense capabilities

July 22 2019

Credit: DARPA

There are times when the highest levels of privacy and security are required to protect a piece of information, but there is still a need to prove the information's existence and accuracy. For the Department of Defense (DoD), the proof could be the verification of a relevant capability. How can one verify this capability without revealing any sensitive details about it? In the commercial world, this struggle manifests itself across banking transactions, cybersecurity threat

disclosure, and beyond. One approach to addressing this challenge in cryptography is with zero-knowledge proofs. A zero-knowledge proof is a method where one party can prove to another party that they know a certain fact without revealing any sensitive information needed to demonstrate that the fact is true.

"A zero-knowledge proof involves a statement of fact and the underlying proof of its accuracy," said Dr. Josh Baron, program manager in DARPA's Information Innovation Office (I2O). "The holder of the fact does not want to reveal the underlying information to convince its audience that the fact is accurate. Take, for example, a bank withdrawal. You may want a system that allows you to make a withdrawal without also having to share your bank balance. The system would need some way of verifying that there are sufficient funds to draw from without having to know the exact amount of money sitting within your account."

In recent years, there has been a marked increase in the efficiency and real-world use of zero-knowledge proofs. Most of these uses have been within the cryptocurrency domain where there is a need to provide certain verifiable data without revealing personal or other sensitive information. While useful in this context, the zero-knowledge proofs created are specialized for this task. They prioritize communication and verification efficiency but do not necessarily scale for transactions that are more complex. For highly complex proof statements like those that the DoD may wish to employ, novel and more efficient approaches are needed.

To help increase the expressivity of problem statements for which zero-knowledge proofs are constructed while also increasing the efficiency of the technology that creates them, DARPA developed the Securing Information for Encrypted Verification and Evaluation (SIEVE) program. SIEVE aims to develop computer science theory and software that can generate mathematically verifiable statements that can be shared

publically without giving sensitive information away. Under the program, researchers will explore the creation of verifiable public statements about software, general computations, as well as social-technical interactions.

More information: www.fbo.gov/index?s=opportunit … 16&tab=core&_cview=1

Provided by DARPA