How suspicious parties can work together safely

March 19 2019

Credit: CC0 Public Domain

Cryptographer Max Fillinger developed new methods to analyse a group of algorithms called commitments schemes. These schemes are building blocks for cryptographic protocols, which enable multiple parties that do not trust each other to work together safely. His Ph.D. Defence is on 19 March.

Keeping information safe

Fillinger is a Ph.D. candidate at the Centrum Wiskunde & Informatica (CWI) and the Mathematical Institute (MI) in Leiden, supervised by Serge Fehr. With his new analysis methods, Fillinger proved that a previous relativistic commitment scheme, proposed in 2015, has been massively underestimated. "It was previously thought that the information in this scheme was safe for only a few milliseconds, but in fact it remains safe for virtually unlimited time – or until the memory of the devices running it is full," he says. This result shows the usefulness of his newly developed methods for analysing commitment schemes.

What is a commitment scheme?

Imagine the following situation: Alice has made a forecast of the stock market. She wants to convince Bob of her ability to predict, but she doesn't want to give him free advice. Therefore, she wants to keep her prediction a secret at first. However, if she only revealed her prediction after it came true, Bob won't believe she actually predicted the stock market rightfully. So she gives her prediction to Bob in a locked safe. Only after the prediction has come true, she gives him the key. In this way, Bob knows that the prediction was right, and Alice doesn't have to give away free advice. Commitments schemes implement this functionality by means of digital communication and calculations, instead of a safe.

Security guaranteed

Most commitment schemes that are used in practice are computationally secure, such as in the cryptocurrency Zerocoin. This means that with current computers, it would take years or decades of computation to crack the code, in other words to cheat. But theoretically, there also is

the notion of unconditional security, Fillinger says. "Here, the probability of undetected cheating should remain miniscule, no matter how much computational power the cheater has at his disposal." That sounds ideal, but it has already been mathematically proven that unconditionally secure commitment schemes with one computer are impossible.

Faster than light?

However, there is good news: scientists found a different scheme which is unconditional. In 1988, a group of researchers proposed a commitment scheme where Alice (from the example in the box) would use two computers. "One computer creates Alice's commitment, the other opens it," says Fillinger. "If they cannot exchange information, it becomes impossible for Alice to cheat." But if Bob does not trust Alice, how can he be sure that she won't cheat by sending information from one computer to the other? "Because information cannot travel faster than light, there is a short window of time where it is physically impossible for the computers to exchange information," says the cryptographer. "During this extremely short time window, the commitment is unconditionally secure!"

The sum of its parts

Adrian Kent expanded on this idea starting in 1999 and introduced the concept of relativistic commitment schemes: these schemes remain unconditionally secure for a longer time, but Bob's computer must continually exchange messages with Alice's computers at precise times. "Previously, relativistic commitment schemes were analysed as a whole. This makes for some hard-to-read proofs." In his thesis, Fillinger offers a more modular approach by analysing parts of the scheme separately. "To simplify a bit: if the parts of a relativistic commitment scheme are

secure when considered on their own, then the security of the whole follows mathematically. This makes it easier to analyse these schemes."

Provided by Leiden University