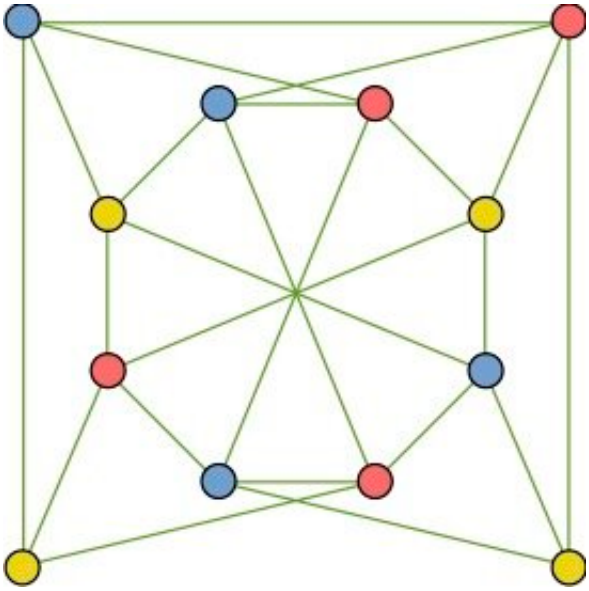
Securing data transfers with relativity

November 3 2021



A graph with its 3-colouring. For each edge, we check that the two connected vertices are of different colours. Credit: © University of Geneva, All rights reserved

The volume of data transferred is constantly increasing, but the absolute security of these exchanges cannot be guaranteed, as shown by cases of hacking frequently reported in the news. To counter hacking, a team from the University of Geneva (UNIGE), Switzerland, has developed a new system based on the concept of zero-knowledge proofs, the security of which is based on the physical principle of relativity: information cannot travel faster than the speed of light. Thus, one of the fundamental principles of modern physics allows for secure data transfer. This system

allows users to identify themselves in complete confidentiality without disclosing any personal information, promising applications in the field of cryptocurrencies and blockchain. These results can be read in the journal *Nature*.

When a person—the so called "prover"—wants to confirm their identity, for example when they want to withdraw money from an ATM, they must provide their personal data to the verifier, in our example the bank, which processes this information (e.g. the identification number and the pin code). As long as only the prover and the verifier know this data, confidentiality is guaranteed. If others get hold of this information, for example by hacking into the bank's server, security is compromised.

Zero-knowledge proof as a solution

To counter this problem, the prover should ideally be able to confirm their identity, without revealing any information at all about their personal data. But is this even possible? Surprisingly the answer is yes, via the concept of a zero-knowledge proof. "Imagine I want to prove a mathematical theorem to a colleague. If I show them the steps of the proof, they will be convinced, but then have access to all the information and could easily reproduce the proof," explains Nicolas Brunner, a professor in the Department of Applied Physics at the UNIGE Faculty of Science. "On the contrary, with a zero-knowledge proof, I will be able to convince them that I know the proof, without giving away any information about it, thus preventing any possible data recovery."

The principle of zero-knowledge proof, invented in the mid-1980s, has been put into practice in recent years, notably for cryptocurrencies. However, these implementations suffer from a weakness, as they are based on a mathematical assumption (that a specific encoding function is difficult to decode). If this assumption is disproved—which cannot be ruled out today—security is compromised because the data would

become accessible.

Today, the Geneva team is demonstrating a radically different system in practice: a relativistic zero-knowledge proof. Security is based here on a physics concept, the principle of relativity, rather than on a mathematical hypothesis. The principle of relativity—that information does not travel faster than light—is a pillar of modern physics, unlikely to be ever challenged. The Geneva researchers' protocol therefore offers perfect security and is guaranteed over the long term.

Dual verification based on a three-colorability problem

Implementing a relativistic zero-knowledge proof involves two distant verifier/prover pairs and a challenging mathematical problem. "We use a three-colorability problem. This type of problem consists of a graph made up of a set of nodes connected or not by links," explains Hugo Zbinden, professor in the Department of Applied Physics at the UNIGE. Each node is given one out of three possible colors—green, blue or red—and two nodes that are linked together must be of different colors. These three-coloring problems, here featuring 5,000 nodes and 10,000 links, are in practice impossible to solve, as all possibilities must be tried. So why do we need two pairs of checker/prover?

"To confirm their identity, the provers will no longer have to provide a code, but demonstrate to the verifier that they know a way to three-color a certain graph," says Nicolas Brunner. To be sure, the verifiers will randomly choose a large number of pairs of nodes on the graph connected by a link, then ask their respective prover what color the node is. Since this verification is done almost simultaneously, the provers cannot communicate with each other during the test, and therefore cannot cheat. Thus, if the two colors announced are always different, the

verifiers are convinced of the identity of the provers, because they actually know a three-coloring of this graph.

"It's like when the police interrogates two criminals at the same time in separate offices: it's a matter of checking that their answers match, without allowing them to communicate with each other," says Hugo Zbinden. In this case, the questions are almost simultaneous, so the provers cannot communicate with each other, as this information would have to travel faster than light, which is of course impossible. Finally, to prevent the verifiers from reproducing the graph, the two provers constantly change the color code in a correlated manner: what was green becomes blue, blue becomes red, etc. "In this way, the proof is made and verified, without revealing any information about it," says the Geneva-based physicist.

A reliable and ultra-fast system

In practice, this verification is carried out more than three million times, all in less than three seconds. "The idea would be to assign a graph to each person or client," says Nicolas Brunner. In the Geneva researchers' experiment, the two prover/verifier pairs are 60 meters apart, to ensure that they cannot communicate. "But this system can already be used, for example, between two branches of a bank and does not require complex or expensive technology," he says. However, the research team believes that in the very near future this distance can be reduced to one meter. Whenever a data transfer has to be made, this relativistic zero-knowledge proof system would guarantee absolute security of data processing and could not be hacked. "In a few seconds, we would guarantee absolute confidentiality," concludes Hugo Zbinden.

More information: Sébastien Designolle, Experimental relativistic zero-knowledge proofs, *Nature* (2021). DOI: 10.1038/s41586-021-03998-y.

www.nature.com/articles/s41586-021-03998-y

Provided by University of Geneva