Hard mathematical problems as basis for new cryptographic techniques

April 1 2016

RUB researchers develop new cryptographic algorithms that are based on particularly hard mathematical problems. They would be virtually unbreakable.

Cryptographic methods are typically created following the ad-hoc principle: somebody comes up with an algorithm; others attempt to break it – if they don't succeed, it means that the algorithm is secure. The team headed by Prof Dr Eike Kiltz who holds the Chair for Cryptography at the Ruhr-Universität Bochum opted for a different approach. They base their security algorithms on hard mathematical problems.

"If somebody succeeded in breaking those algorithms, he would be able to solve a mathematical problem that the greatest minds in the world have been poring over for 100 or 200 years," compares Kiltz. The mathematicians make the algorithms so efficient that they can be implemented into microdevices, such as electric garage openers.

Lattice problem: finding the optimal difficulty level

The algorithms are based, for example, on the hardness of the following lattice problem: imagine a lattice to have a zero point in one specific location. The challenge is to find the point where two lattice lines intersect and that is closest to zero point. In a lattice with approx. 500 dimensions, it is impossible to solve this problem efficiently.

The researchers test various parameters that render the lattice problem simpler or harder and use it as basis for developing a cryptographic algorithm which could be implemented even in small devices.

Authentication protocols almost finalised

Lattice-based authentication algorithms developed by the team are fairly advanced. "We are about to finalise them," says Eike Kiltz. Authentication protocols are necessary whenever an object has to prove its identity, for example an electric garage opener at the respective door. This is how it could work in the protocol: the opener authenticates itself at the garage door by proving that it knows an internal secret, for example an intersection point close to the zero point in the lattice.

Kiltz's group is currently also researching into lattice-based encryption methods. They are necessary if two parties wish to exchange a secret message. The Ruhr-Universität Bochum's science journal Rubin reports about the mathematicians' work.

Provided by Ruhr-Universitaet-Bochum

Citation: Hard mathematical problems as basis for new cryptographic techniques (2016, April 1) retrieved 26 April 2024 from https://phys.org/news/2016-04-hard-mathematical-problems-basis-cryptographic.html