High Performance Lattice Cryptography

Results in Brief

Deciphering the path to unbreakable ciphers

As more widespread use of quantum computers becomes an ever-greater likelihood, our information systems will need tougher encryption. An EU-funded project believes the answer lies in lattice cryptosystems.

DIGITAL ECONOMY

© Thinkstock

The cryptosystems produced via cryptography are essential to the security of contemporary computer systems. A cryptosystem typically consists of three algorithms: one for key generation, one for encryption and one for decryption.

To make cryptosystems even harder to crack, the 'High performance lattice cryptography' (HIPERLATCRYP) project is developing powerful and provably secure public-key cryptosystems based on the hardness of high-dimensional Euclidean lattices.

Financed by the EU, the project is focusing on this avenue because the best-known Euclidean lattice problems are believed able to withstand cryptanalytic attacks based on future quantum computers. This kind of encryption has applications in telecommunications, e-commerce and other critical areas. Given their algorithmic simplicity, lattices are also ideal in devices with limited computational power, such as smart cards.

HIPERLATCRYP has been working on 'expressive' cryptographic algorithms that support convenient naming schemes for the handling of large populations of cryptographic actors.

To date, the project has collaborated with teams from France and the United States to develop attribute-based encryption and multiuser anonymous digital signatures, respectively.

The project will end in the autumn of 2014 and its results should provide the theoretical foundations for next-generation encryption using lattice cryptography.

Discover other articles in the same domain of application

Advances in detection of erratic heart rhythm

30 November 2022

Future proofing the connected world of quantum computing

29 May 2020

Blockchain technology makes secure, low-cost and simple payments a reality for all

26 June 2020

Centreing the citizen in demand response solutions

21 February 2024

Project Information

HIPERLATCRYP

Grant agreement ID: 268469

Project closed

Start date
1 October 2010

End date
30 September 2014

Funded under
Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Total cost
€ 100 000,00

EU contribution
€ 100 000,00

Coordinated by
UNIVERSITE DE LIEGE
Belgium

Last update: 3 October 2013