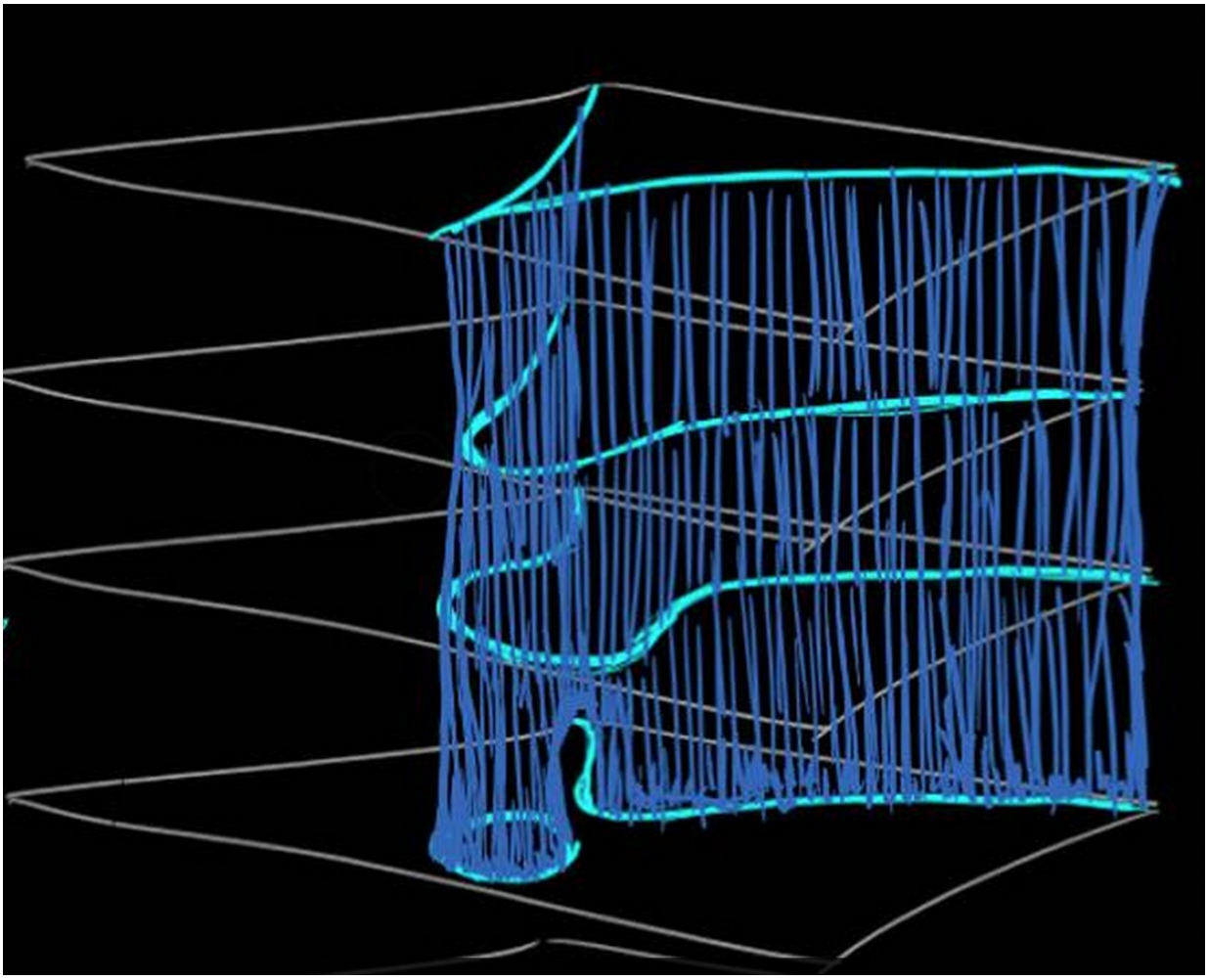
Researcher develops algorithm to improve information security tools

July 16 2018



Elliptical curves. Credit: Denis Khleborodov.

Cryptography is a science of data encryption providing its confidentiality and integrity. After cryptographic transformations (the basis of encryption algorithms) are applied, only users that possess a relevant key can have access to the initial text.

Transformations based on elliptical curves have been widely used for data protection recently. They provide the same security levels as other types of cryptographic algorithms but require substantially shorter keys. These transformations are in high demand due to the fact that modern technologies aim at the reduction of memory and computational power consumption.

Mobile devices, blockchain technologies, and the Internet of things require new safety measures, raising the demand for new cryptographic transformation algorithms with lower computational power consumption. The Internet of things is a concept according to which devices communicate not only with the users, but also with each other. Blockchain technologies also cover the Internet of things, and personal mobile devices and are based on digital signature technology.

The main mathematical operation in transformations based on elliptical curves is scalar multiplication, in which a point on an elliptical curve is multiplied by a parameter (scalar). The main disadvantage of scalar multiplication is its high calculational complexity, which may be reduced by using efficient algorithms with lower complexity and therefore lower computational power consumption.

"In the course of the study we found an algorithm and identified different parameters of its operation. When these parameters are used, and depending on available memory volumes and the value of the scalar, the algorithm allows us to perform scalar multiplication—the main operation on the elliptical curve—with minimum computational power consumption," said Denis Khleborodov, the author of the article, Ph.D.,

CCIE Security, and a researcher at MSU.

The new algorithm is based on window non-adjacent form of scalar representation that is classified as an algorithm with a precomputation step. Precomputations are single-time calculations that are performed before the main part of the work, and their results are saved in the memory. The main advantage of algorithms with precomputations is the division of calculation into two parts: the precomputations themselves followed by the new calculations reusing their results. Therefore, the computational complexity of consecutive scalar multiplication operations is reduced.

The author also performed comparative analysis of the obtained result with another effective algorithm based on the same method. The scientist managed to reduce the average computational complexity of the precomputation stage by 5 percent to 46 percent, and of the main stage—by 4 percent to 22 percent depending on the input data.

The new algorithm may be used on blockchain platforms for digital signing of transactions and authentication, as well as on the Internet of things for the authentication of its devices, in session keys development protocols for the encryption of transferred data, and to secure the integrity of transmitted information.

"We expect to develop an improved algorithm based on the sliding window non-adjacent form of scalar representation, i.e. with changeable parameters of precomputations. We also want to adapt the algorithms for simultaneous calculations. The results may be used in security features of the Internet of things and blockchain platforms," concluded the scientist.

More information: Denis Khleborodov, Fast elliptic curve point multiplication based on window Non-Adjacent Form method, *Applied*

PHYS.ORG

Mathematics and Computation (2018). DOI: 10.1016/j.amc.2018.03.112

Provided by Lomonosov Moscow State University

Citation: Researcher develops algorithm to improve information security tools (2018, July 16) retrieved 1 May 2024 from https://phys.org/news/2018-07-algorithm-tools.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.