

УДК 003.26

Ponomarenko Ye.¹, Nelasa H.²

¹student of group RT-810m NU "Zaporizhzhia Polytechnic"

²PhD (Information protection systems), professor NU "Zaporizhzhia Polytechnic"

USING OF ELLIPTIC CURVES ISOGENIES IN CRYPTOGRAPHIC PROTOCOLS

Existing public-key cryptography is based on the difficulty of factoring and the difficulty of calculating elliptic curve discrete logarithms. Because these two problems can be easily and effectively solved by a sufficiently large-scale quantum computer, now in development are approaches that appear to be resistant to the hacker attack within the access to a quantum computer. Even if such a quantum computer does not exist today, the prospect of its creation in the near future makes it necessary to prepare a cryptographic infrastructure and protect our data now.

Cryptosystems are being developed which security is based on various hard mathematical problems that cannot be solved by a large-scale quantum computer.

In cryptography, isogeny is the rational mapping of points from one curve to another. The algorithm developed by J. Velu [2], implemented in the work, allows to calculate the function for such mapping.

The features of the use of elliptic curves isogenies in cryptographic protocols are studied. Cryptosystems based on isogenies allow us not only to improve already used, but also to implement fundamentally new cryptographic protocols. Such cryptosystems are resistant to quantum attacks.

The reviewed Diffie-Hellman protocol using supersingular curve isogenies (SIDH), which is similar in structure to the standard algorithm, but uses supersingular elliptic curves and isogenies between them as a mathematical basis. This algorithm was proposed by Jao and DeFeo in [3]. Despite the use of elliptic curves, the security of the algorithm is provided not by the hardness of the elliptic curve discrete logarithm problem, but by the hardness of computing large-scale isogenies between two elliptic curves.

REFERENCES

1. Rostovtsev A., Stolbunov A. Public-Key Cryptosystem Based on Isogenies, Saint Petersburg, 19 p. (2006).
2. J. V'elu, Isog'enies entre courbes elliptiques, C.R. Acad. Sc. Paris, S'erie A., 273 pp. 238-241 (1971).
3. David Jao, Luca De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, Canada, 15 p. (2011).