1176-14-62 **Julia Bernatska*** (julia.bernatska@uconn.edu), Department of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, CT 06242. *Trigonal-Curve Cryptography.*

An approach to public-key cryptography based on the algebraic structure of trigonal curves will be considered. The complexity of addition laws on algebraic curves promises to increase security of the cryptographic algorithm. The interest to hyperelliptic curves in cryptography was aroused by the famous paper [**?**] where explicit formulas for addition in the Jacobian group of a hyperelliptic curve were presented. Cantor's algorithm made the implementation of hyperelliptic-curve cryptosystems simple and clear, and allowed to examine this family of cryptosystems.

In this talk a similar approach to addition in the Jacobian group of a trigonal curve will be presented. Explicit formulas for addition on $(3, 3m+1)$- and $(3, 3m+2)$-curves are obtained. Implementation of the cryptographic algorithm is illustrated by examples on simple trigonal curves. Also a comparison with the case of hyperelliptic curves is carried out.

References

[1] D. Cantor, Computing in the Jacobian of a Hyperelliptic curve, Mathematics of Computation, **48**:177 (1987), pp. 95–101.

(Received January 11, 2022)