

Isogenies Graphs and Isogenies Cycles through Examples and Applications: The Rostovtev-Stolbunov cryptosystem

Emmanuel Fouotsa¹

The University of Bamenda, Uba
Higher Teacher Training College, Bambili
P.O;Box 39 Bambili (Cameroon)
emmanuel Fouotsa@yahoo.fr

Abstract. In this talk, we explain the construction of isogenies graphs and isogenies cycles for ordinary elliptic curves. We illustrate concepts with many examples. We end with a brief presentation and a security analysis of the Rostovtev-Stolbunov cryptosystem

Key words: Elliptic Curves-Isogenies-Graphs-Cycle.

References:

1. Alexander Rostovtsev and Anton Stolbunov, *Public key cryptosystem based on isogenies*, Saint-Petersburg State Polytechnical University, Department of Security and Information Protection in Computer System Russia.
2. Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, second edition, Springer 2009.