Cryptology ePrint Archive: Report 2011/033

The Geometry of Flex Tangents to a Cubic Curve and its Parameterizations

Jean-Marc Couveignes and Jean-Gabriel Kammerer

Abstract: We show how the study of the geometry of the nine flex tangents to a cubic produces many pseudo-parameterizations, including the ones given by Icart, Kammerer, Lercier, Renault and Farashahi.

Category / Keywords: public-key cryptography / elliptic curve cryptosystem

Date: received 19 Jan 2011, last revised 1 Sep 2011

Contact author: couveig at univ-tlse2 fr

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Note: Two sections added.

Version: 20110902:054016 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]