Abstract

GCD attack depends on modifying the cipher text and then get an access to the decryption of
the modified cipher text that is discarded identifying as due to bad implementation. In this paper
we mount a GCD attack on Demytko’s cryptosystem on elliptic curves. In this we implement the
attack by point addition with projective coordinates using a fast computation method. As this
involves working only with $x$-coordinates. We start with developing the formulas for the
projective coordinates $x : z$ generalizing the ideas of Montgomery and propose to use these
formulas to generate the polynomials for the GCD attack.

References

1. R. Balasubramanian “Elliptic Curves and Cryptography” proceedings of the advanced
   instructional workshop on Algebraic number theory, HBA (2003)325-345
2. I.F.Blake, G. Seroussi and N. P. Smart “Elliptic Curves in Cryptography”, volume 265 of
   London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge,
Implementation of GCD Attack with Projective Coordinates on Demytko’s Cryptosystem

2000.

Index Terms

Computer Science Security
Keywords

Elliptic Curves, Projective Coordinates and Demytko’s Cryptosystem.