4th INTERNATIONAL CONFERENCE ON MATHEMATICS
"An Istanbul Meeting for World Mathematicians"
1-3 July 2020, Istanbul, Turkey
This conference is dedicated to 67th birthday of Prof. M. Mursaleen

ECC in special ring and cryptographic application

Bilel Selikh[1], Abdelhakim Chillali[2], Douadi Mihoubi[1] and Nacer Ghadbane[1]

[1]Laboratory of Pures and Applied Mathematics, Department of Mathematics,
Mohamed Boudiaf University of Msila, Algeria,
[2]Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco,
E-mail(s): bilel.selikh@univ-msila.dz, abdelhakim.chillali@usmba.ac.ma
douadi.mihoubi@univ-msila.dz, nacer.ghadbane@univ-msila.dz

Abstract

Let F_{3^d} is the finite field of order 3^d with d be a positive integer, we consider $A_4 := F_{3^d}[\varepsilon] = F_{3^d}[X]/(X^4)$ is a finite quotient ring, where $\varepsilon^4 = 0$ [5]. In this paper, we will show an example of encryption and decryption. The motivation for this paper came from the observation that communications, industrial automation and many more. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security [6]. Firstly, we study the elliptic curve over this ring. Furthermore, we study the algorithmic properties by proposing effective implementations for representing the elements and the group law. Finally, we give an example cryptographic (encryption and decryption) with a secret key.

Keywords : Cryptography, Elliptic Curves, Finite Rings, Finite Field.

References:

[1] W. Bosma and H.W. Lenstra, *Complete System of Two Addition Laws for Elliptic Curves*, Journal of Number Theory, (1995).

[2] AZIZ BOULBOT, ABDELHAKIM CHILLALI and ALI MOUHIB, *Cryptographic Protocols on the non-commutative Ring R,* International Journal of Mathematical and Computational Methods, Volume 2, (2017).

[3] Mustapha ELHASSANI, Aziz BOULBOT, Abdelhakim CHILLALI and Ali MOUHIB*, Fully homomorphic encryption scheme on a non-Commutative ring R,* International Conference on Intelligent Systems and Advanced Computing Sciences(ISACS), (2019). Doi: 10.1109/ISACS48493.2019.9068892

[4] M. H. Hassib and A. Chillali, *Example of cryptography over the ring $F_{3^d}[\varepsilon]$, $\varepsilon^2 = 0$*, Latest trends in Applied Informatics and Computing , ISBN 978-1-61804-130-2, (2012), 71-73.

[5] My Hachem Hassib, Abdelhakim Chillali, Mohamed Abdou Elomary, *Elliptic Curves over the Ring $F_{3^d}[\varepsilon]$, $\varepsilon^4 = 0$*, International Mathematical Forum, Vol.9, 2014, no.24, 11911196 HIKARI Ltd, www.m-hikari.com, http://dx.doi.org/10.12988/imf.2014.4599.

[6] V. Miller, *Use of elliptic curves in cryptography*, in CRYPTO'85, LNCS 218, pp.417-426, Springer 1986.

[7] Abdelhamid Tadmori, Abdelhakim chillali and M'hamed Ziane, *Elliptic curves over ring $F_{2^d}[\varepsilon]$, $\varepsilon^4 = 0$*, Applied Mathematical Sciences, Vol. 9, 2015, no. 35, 1721 - 1733 HIKARI Ltd, www.m-hikari.com.

[8] A. Tadmori , A. Chillali AND M. Ziane, *Ecc over the ring $F_{2^d}[X]/(X^2)$ by using a password*, Gulf Journal of Mathematics, Vol 6, Issue 4 (2018) 72-78.