ICRAMCS 2026

THE EIGHTH EDITION OF THE INTERNATIONAL CONFERENCE ON RESEARCH IN APPLIED MATHEMATICS AND COMPUTER SCIENCE
April 23-24-25, 2026 | Marrakech, Morocco

Twisted Hessian curve Binary over a ring

Communication Info

Authors:
Abdelâli GRINI

Regional Center of Education and Professional Training, Fez-Meknes, Meknes, Morocco

Keywords:
(1) Twisted Hessian curves
(2) Local ring
(3) Cryptography

Abstract

Elliptic curves are often used in cryptography, and this is where twisted Hessian curves [1] have their advantages: addition, doubling and tripling can be performed faster on twisted Hessian curves than on curves given by a Weierstrass equation. However, there are exponential time algorithms [2, 3] that compute discrete logarithms for the cyclic subgroup of the elliptic curve. To ensure maximum security of the cryptographic system, the elliptic curve must be properly chosen. For this objective, we present in this talk the twisted Hessian curve over the ring $\frac{F_2 n[X]}{X^2}$ which verifies this property because it increases the time needed to solve the discrete logarithm problem, we will prove that card $(HB^2_{a,d}) = 2^n\, card(HB_{a_0,b_0})$, which is beneficial and interesting in cryptography.

References

[1] Bernstein, D. J., Chuengsatiansup C., Kohel D., Lange T., Twisted Hessian Curves , Springer, 9230, 2015, 269-294.

[2] Koblitz, N., Menezes, A. Vanstone, S., The State of Elliptic Curve Cryptography}. Designs, Codes and Cryptography 19,2000, 173-193.

[3] Silverman, H. S., An Introduction to the Theory of Elliptic Curves. University of Wyoming, 2006.