Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

Power of Frobenius Endomorphism and its Performance on PseudoTNAF System

Yunos, F. *[1], Yusof, A. M.[2], Hadani, N. H.[3], Ariffin, M. R. K.[1,3], and Sapar, S. H.[1,3]

[1]*Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Malaysia*
[2]*Faculty of Science and Natural Resource, Universiti Malaysia Sabah, Malaysia*
[3]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*

E-mail: faridahy@upm.edu.my
**Corresponding author*

Received: 15 June 2021
Accepted: 8 October 2021

Abstract

Let E be an elliptical curve defined over F_{2^m} and the mapping τ is a Frobenius endomorphism from the set F_{2^m} to itself. The Koblitz curve is a special curve whose τ has been used to improve the calculation performance of its scalar multiplication, nP where P is a point on the curve E. Moreover, the multiplier, n is τ -adic non adjacent form (TNAF) expansion where its digit is generated by the repeated division of an integer in the ring of $Z(\tau)$ by τ. Previous research has found that the power of Frobenius endomorphism τ^m has some advantages in TNAF, Reduced TNAF and their equivalent i.e. pseudoTNAF expansions. In this paper, new finding of τ^m based on v-simplex and arithmetic sequences is provided. With this approach, the performance of converting modulo $\rho\frac{\tau^m-1}{\tau-1}$ to $r+s\tau$ an element of $Z(\tau)$ in pseudoTNAF's system is enhanced.

Keywords: cryptography; field; Frobenius endomorphism; Koblitz curve; number of elliptic points; sequence of arithmetic; sequence of simplex; τ-adic non adjacent.