Improving the performance of {0,1,3}-NAF recoding algorithm for elliptic curve scalar multiplication

ABSTRACT

Abstract: Although scalar multiplication is highly fundamental to elliptic curve cryptography (ECC), it is the most time-consuming operation. The performance of such scalar multiplication depends on the performance of its scalar recoding which can be measured in terms of the time and memory consumed, as well as its level of security. This paper focuses on the conversion of binary scalar key representation into {0, 1, 3}-NAF non-adjacent form. Thus, we propose an improved {0, 1, 3}-NAF lookup table and mathematical formula algorithm which improves the performance of {0, 1, 3}-NAF algorithm. This is achieved by reducing the number of rows from 15 rows to 6 rows, and reading two (instead of three) digits to produce one. Furthermore, the improved lookup table reduces the recoding time of the algorithm by over 60% with a significant reduction in memory consumption even with an increase in key size. Specifically, the improved lookup table reduces the memory consumption by as much as 75% for the big key, which shows its higher level of resilience to side channel attacks.

Keyword: Elliptic Curve Cryptosystem (ECC); Scalar multiplication algorithm; {0, 1, 3}-NAF method; Non-Adjacent Form (NAF)