Shorter addition chain for smooth integers using decomposition method.

ABSTRACT

An efficient computation of scalar multiplication in elliptic curve cryptography can be achieved by reducing the original problem into a chain of additions and doublings. Finding the shortest addition chain is an NP-problem. To produce the nearest possible shortest chain, various methods were introduced and most of them depends on the representation of a positive integer n into a binary form. Our method works out the given n by twice decomposition, first into its prime powers and second, for each prime into a series of 2's from which a set of rules based on addition and doubling is defined. Since prime factorization is computationally a hard problem, this method is only suitable for smooth integers. As an alternative, the need to decompose n can be avoided by choosing n of the form p1 e1p2 e2⋯r er. This shall not compromise the security of ECC since its does not depend on prime factorization problem. The result shows a significant improvement over existing methods especially when n grows very large.

Keyword: Elliptic curves cryptography; Addition chain; Scalar multiplication; Binary method; Non-adjacent form; Complementary recoding.