Signed decomposition method for scalar multiplication in elliptic curve cryptography

ABSTRACT

Addition chain is the solution to computability constraint of the problematic large number arithmetic. In elliptic curve cryptography, a point arithmetic on elliptic curve can be reduced to repetitive addition and doubling operations. Based on this idea, various methods were proposed, lately a decomposition method based on prime decomposition was put forward. This method uses a pre-generated set of rules to calculate an addition chain for n. Though the method shows it own advantage over others in some cases, but some improvements is still avail. We develop an enhancement version called signed decomposition method which takes rule from decomposition method as an input. We also generalize the idea of a prime rule to an integer rule. An improvement is done to the original add rule in decomposition method by allowing subtraction operation to terms. In so doing, we optimize the original form of add rule. The result shows not only an improvement over decomposition method but also become an all time superior compare to preceeding methods. Furthermore, having secret key in a form of rule will put up extra security to the message under communication.

Keyword: Binary method; Complementary recoding; Double and add; Non-adjacent form; Selectfont addition chain