

An improved binary method for scalar multiplication in elliptic curve cryptography

ABSTRACT

Problem statement: Until recently, many addition chain techniques constructed to support scalar multiplication operation have been proposed tailored to limited computational resources. In securing the efficiency of ECC point operation, the combinations of the two basic operations, point addition and doubling are mostly implemented. Using binary method, the operation of doubling depends solely on the length of binary representation itself, so the most probable way to reduce the total number of the whole operation is by reducing the number of addition operation. This limitation is quite problematic. Approach: In this study we proposed an improved binary method which reads input block by block basis. Instead of having to add one to current chain every time non zero digit appears, this method requires one addition for every non zero block. A mapping table is used to store all possible binary string and its decimal version. For every block, its decimal value is extracted from the table and this value will be added to the current chain. In return, it requires precomputations for all possible combination of input blocks. Results: The new method showed a significant reduction in the number of required additions and the magnitude of improvement varies according to the key size. Conclusion: The algorithm is suitable to be adapted into cryptographic system especially as the need for bigger key size is growing rapidly.

Keyword: Scalar multiplication; Elliptic curve; Binary representation; Addition chains