

ABSTRACT

MULTIPLICATION METHODS, NON-TRANSITORY COMPUTER-READABLE MEDIA, AND MULTIPLICATION DEVICES

According to various embodiments, a multiplication method may be provided. The multiplication method may include: providing a prime number p , a first polynomial and a second polynomial; determining a first discrete Galois transform based on the first polynomial and the prime number; determining a second discrete Galois transform based on the second polynomial and the prime number; determining a point-wise product of the first discrete Galois transform and the second discrete Galois transform; determining an inverse discrete Galois transform based on the point-wise product; and determining a polynomial product of the first polynomial and the second polynomial based on the inverse discrete Galois transform.

[Figure 4]