

ABSTRACT

The present disclosure according to at least one embodiment provides a method of processing operations of a polynomial-based security algorithm, the method being performed by a computing system. The method comprises identifying a plurality of operations using secret information in the polynomial-based security algorithm, generating a random index to be applied to the identified operations, and performing the operations using the random index.

Figure 1 accompanies.