

**APPARATUS FOR PROCESSING NON-POLYNOMIAL OPERATION ON
HOMOMORPHIC ENCRYPTED MESSAGES AND METHODS THEREOF**

ABSTRACT

A method of operating a homomorphic ciphertext is disclosed. The method of operating a homomorphic ciphertext includes receiving a non-polynomial operation command with respect to a homomorphic ciphertext, computing an approximate polynomial function corresponding to the non-polynomial operation, performing an operation of the homomorphic ciphertext using the computed polynomial function, and outputting the operated homomorphic ciphertext, wherein the approximate polynomial function is a second approximate polynomial function which is obtained by extending a first approximate polynomial function to have a second range wider than the first range having a preset accuracy with the non-polynomial operation within a first range.

Fig. 4