Method and Apparatus for Encryption, Method and Apparatus for Decryption, and Computer-Readable Medium Storing Program

Abstract

To encrypt another piece of data during encrypting process of a certain piece of data, a memory 55 is provided in parallel with a feedback line 65 which feeds back data from an encrypting module 51using an encryption key K to a selector 54. When an interrupt IT for processing plaintext block data N_i is generated while plaintext block data M_i is processed, ciphertext block data C_i at timing of generation of the interrupt IT is made to be stored in a register 56. The ciphertext block data C_i stored in the memory 55 is made to be selected by the selector 54 at timing of completion of processing the plaintext block data N_i, and processing the plaintext block data M_{i+1} is started.

Fig 1