

**ENCRYPTION METHOD, PROGRAM FOR ENCRYPTION, MEMORY
MEDIUM FOR STORING THE PROGRAM, AND ENCRYPTION APPARATUS,
AS WELL AS DECRYPTION METHOD AND DECRYPTION APPARATUS**

ABSTRACT

The present invention relates to a cryptosystem. A keystream table [Ks] is a virtual data space. Every data of 1 byte in a secondary ciphertext E_2 provides a vector directional component IR. The data Ks (IR) in the keystream table [Ks] designated by the directional component IR of the vector is recognized as the quantitative component of the vector. By handling a secondary ciphertext E_2 of 1 byte as the address in the keystream table [Ks], the secondary ciphertext E_2 can be recognized as the directional component of the vector. A logical operation for the data Ks (IR) is performed, and the internal vector data V is sequentially replaced every 1 byte. An exclusive OR operation is performed between the internal vector data V and the primary ciphertext E_1 for generating a secondary ciphertext E_2 .

(See Fig. 1)