ABSTRACT

It is desired to share one circuit by an encryption unit 200 and a decryption unit 500. A normal data transformation unit (FL) 251 and an inverse data transformation unit (FL^{-1}) 273 are located at point symmetry on a non-linear data transformation unit 220, and a normal data transformation unit (FL) 253 and an inverse data transformation unit (FL^{-1}) 271 are located at point symmetry on the non-linear data transformation unit 220. Therefore, the encryption unit 200 and the decryption unit 500 can be configured using the same circuits.