ABSTRACT

To realize a common-key block cipher process configuration with increased difficulty of key analysis and improved security. In a configuration for storing in a register an intermediate key generated by using a secret key transformation process and performing a transformation process on the register-stored data to generate a round key, a process of swapping (permuting) data segments constituting the register-stored data is executed to generate a round key. For example, four data segments are produced so that two sets of data segments having an equal number of bits are set, and a process of swapping the individual data segments is repeatedly executed to generate a plurality of different round keys. With this configuration, the bit array of each round key can be effectively permuted, and round keys with low relevance can be generated. A high-security cryptographic process with increased difficulty of key analysis can be realized.