

ABSTRACT

To realize an extended-Feistel-type common-key block-cipher process configuration for realizing a diffusion-matrix switching mechanism (DSM). In a cryptographic process configuration in which an extended Feistel structure having a number of data lines: d that is set to an integer satisfying $d \geq 2$ is applied, a plurality of multiple different matrices are selectively applied to linear transformation processes performed in F-function sections. A plurality of different matrices satisfying a condition in which a minimum number of branches for all of the data lines is equal to or more than a predetermined value are selected as the matrices, the minimum number of branches for all of the data lines being selected from among minimum numbers of branches corresponding to the data lines, each of the minimum numbers of branches corresponding to the data lines being based on linear transformation matrices included in F-functions that are input to a corresponding data line in the extended Feistel structure. According to the present invention, common-key block cipher based on the DSM with a high resistance to linear analysis and differential analysis is realized.