CRYPTOGRAPHIC PROCESSING DEVICE, CRYPTOGRAPHIC PROCESSING METHOD, AND PROGRAM

Abstract

[Object] To realize cryptographic processing with improved diffusion properties and a high level of security.
[Solving Means] A cryptographic processing unit divides and inputs the constituent bits of data to be subjected to data processing to lines, and repeatedly performs a data converting operation using round functions on the data of the respective lines. The cryptographic processing unit inputs n/d-bit data obtained by dividing n-bit data as input data by a division number d to each line, and repeatedly performs a round calculation that is a calculation including a data converting operation using round functions. The n/d-bit data in each line having output data of the round calculations is divided into d/2 sets of data, and the divided data are combined to restructure d sets of n/d-bit data that are different from the output data of the round calculations of the previous stage. The restructured data is set as the input data for the round calculations of the next stage. With this structure, cryptographic processing with improved diffusion properties and a high level of security is realized.

Fig. 20