ABSTRACT

The present invention can be applied to a cipher processing apparatus, which includes a function F having a configuration of repeating process and inside of the function F, a function f having a configuration of repeating process is included. According to the invention, the cipher processing apparatus is configured by registers 301 through 303 for temporarily holding data, selectors A through C, 311 through 313, and a function f operating circuit 323 for transforming data. An output data from the function f operating circuit 323 is held in the register C 303, and the selector C 313 selects either to repeat the data transformation by the function operating circuit 323 or not. When a cipher processing apparatus includes a function F having a configuration of repeating process and inside of the function F, a function f having a configuration of repeating process is included, the cipher processing apparatus can be embodied efficiently, which enables to reduce the circuit scale and to save electric power.