## Abstract

In a data transformation apparatus for transforming two arbitrary pieces of data of A input data (101) and B input data (102), a first nonlinear transformation of the A input data is performed using a first key parameter (111), a transformed result (109) is output, an XOR operation of the transformed result and the B input data (102) is performed to output an XORed result as B intermediate data (106), and the B intermediate data is input to a next sub-transformation unit (122) as B input data. On the other hand, the B input data (102) is input to a next sub-transformation unit as A input data. A second nonlinear transformation of the B input data (102) is performed using a second key parameter (112), the transformed result is output, an XOR operation of the transformed result and the B intermediate data (106) is performed to output an XORed result as B intermediate data (108), and the B intermediate data is input to a next sub-transformation unit (123) as B input data. The above configurations is connected in a cascade and the last A intermediate data and B intermediate data are output as transformation result (103 and 104).