SCRAMBLER CIRCUIT

ABSTRACT

This invention is intended to provide a scrambler circuit capable of realizing a data processing device or an IC card having high security enough to prevent information in a memory or information on a bus from being decrypted. The scrambler circuit has to-be-processed data divided into two data blocks (B1 and B0) and processed data divided into two data blocks (B1' and B0'), and includes a first scrambler unit (231) that conducts first scrambling to the data block (B1) and that outputs first intermediate data, a first arithmetic unit (233) that performs an exclusive OR operation between the data block (B0) and the first intermediate data and that outputs the data block (B1'), a second scrambler unit (232) that conducts second scrambling to the data block (B1') and that outputs second intermediate data, and a second arithmetic unit (234) that performs an exclusive OR operation between the second intermediate data and the data block (B1) and that outputs the data block (B0').

Reference: FIG. 3