EFFICIENT BYTE PERMUTATION REALIZATIONS FOR COMPACT AES IMPLEMENTATIONS (ThuPmOR9)

Author(s) :

Tuomas Järvinen (Tampere University of Technology, Finland)
Perttu Salmela (Tampere University of Technology, Finland)
Panu Hämäläinen (Tampere University of Technology, Finland)
Jarmo Takala (Tampere University of Technology, Finland)

Abstract :

Advanced Encryption Standard (AES) algorithm incorporates a byte permutation operation which reorders the bytes within a 128−bit data block. This permutation can be described by reading the input data bytes into a 4x4 matrix called state in column wise and shifting the rows by one, two, or three bytes to the left. In decryption, the shifting is reversed, i.e., the rows are shifted to the right. While such shifting operations are straightforward if the computation is done with 128−bit data blocks at a time, they become more complex in area−efficient folded implementations where smaller than 128−bit data blocks are used. In such cases, a storage of data is required, either in the form of registers or memories. In this paper, efficient realizations of the byte permutations in AES algorithm, where the size of simultaneously computed data can be 1, 2, 4, or 8 bytes, are presented. All the realizations use the minimum number of storage elements implying area−efficiency.

Menu