Cryptology ePrint Archive: Report 2011/184

Fortification of AES with Dynamic Mix-Column Transformation

Ghulam Murtaza and Azhar Ali Khan and Syed Wasi Alam and Aqeel Farooqi

Abstract: MDS Matrix has an important role in the design of Rijndael Cipher and is the most expensive component of the cipher. It is also used as a perfect diffusion primitive in some other block ciphers. In this paper, we propose a replacement of Mix Column Transformation in AES by equivalent Dynamic Mix Column Transformation. A Dynamic Mix Column Transformation comprises dynamic MDS Matrices which are based on default MDS Matrix of AES and m-bit additional key. Here m is a variable length that does not exceed the product of 31.97 and one less the number of encryption rounds. This mechanism increases a brute force attack complexity by m-bit to the original key and enforces the attackers to design new frameworks for different modern cryptanalytic techniques applicable to the cipher. We also present efficient implementation of this technique in Texas Instrument’s DSP C64x+ with no extra cost to default AES and in Xilinx Spartan3 FPGA with no change in AES throughput. We also briefly analyze the security achieved over it.

Category / Keywords: secret-key cryptography / Dynamic Mix-Column Transformation (DMCT), Dynamic MDS Matrix, Keyed AES Diffusion, Attacks on Block Ciphers, AES performance in DSP, AES performance in FPGA.

Date: received 9 Apr 2011

Contact author: azarmurtaza at hotmail com

Available formats: PDF | BibTeX Citation

Version: 20110412:194228 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]