Nimix : An involutary nonlinear vectorial boolean function

Jaydeb Bhaumik [*]

Dept. of ECE
Haldia Institute of Technology
Haldia 721657
India

Dipanwita Roy Chowdhury [†]

Dept. of CSE
Indian Institute of Technology
Kharagpur 721302
India

Abstract

This paper proposes a nonlinear involutary balanced vectorial Boolean function called '*Nimix*'. Its several properties and performance against linear and differential cryptanalysis are discussed here. The function has an interesting property that it is nonlinear as well as involutary. Also in this paper, the function *Nimix* has been used in AES for round key mixing instead of XOR. The function *Nimix* provides another layer of nonlinearity besides the non-linearity of substitution boxes. It is shown that application of *Nimix* does not affect the diffusion property of the round function. Strength of the modified AES against linear and differential attacks have been studied.

Keywords: *AES, key mixing, Involutary function, linear cryptanalysis, differential cryptanalysis*