Finding an effective metric used for bijective S-box generation by genetic algorithms

State Agency for National Security

Georgi Ivanov, Nikolay Nikolov

Background

In cryptography, the science of information protection, highly nonlinear mappings are wished for. Most of all encryption algorithms are built on the basis of nonlinear components, providing the cryptographic strength necessary to avoid any cryptanalytic attacks. Otherwise, the whole system breaking is equivalent to solving a linear system of equations. Usually, the only nonlinear components in symmetric encryption algorithms, specifically in block ciphers, are substitution tables or S-boxes: n-input m-output binary mappings. Among them, (n x n) bijective S-boxes are particularly interested. There are lots of methods know for S-box generation. The three main classes of such methods are: pseudo-random generation, algebraic constructions and various heuristic approaches. Among the latter are the genetic algorithms. Genetic algorithms are applied with the purpose to find the optimal solution of an optimization problem. Related to S-boxes, genetic algorithms aim at producing S-boxes that possess cryptographic properties which are optimal with respect to several targeted criteria simultaneously. Unfortunately, S-boxes that are optimal with respect to all desired criteria do not exist due to the criteria contradiction available. Thus, not optimal but sub-optimal S-boxes, which strength is still satisfactory, are needed and searched for.

The origin of the problem

The problem, stated below, has arisen in result of the application of a specific genetic algorithm in order to obtain strong bijective S-boxes (n-input n-output vectorial Boolean functions). The genetic algorithm is used in combination with a cost or a fitness function taken to ascertain which individuals will survive to the next generation. The cost function is based on the so called Walsh-Hadamard Transform Spectrum, which has to be flat in order S-boxes with good nonlinearity to be obtained. The fitness function only role is the S-box nonlinearity to be calculated. Bent S-boxes are of the highest nonlinearity possible (their Walsh spectrum is flat entirely – all spectral coefficients are equal to $2^{n/2}$) but they are never balanced – something important and wished for. For that reason, S-boxes that are close to the Bent ones are needed (their cost, namely the difference between them and the Bent ones, is the smallest positive one possible).

The problem

The problem is related to finding any appropriate metric measuring the distance to an (2^n x 2^n) “flat” matrix of integer-valued elements, possessing equal absolute values of $2^{n/2}$, of two square matrices of equal dimensions (2^n x 2^n) with integer-valued elements and the sum of squares of all elements in each column is one and the same constant equal to 2^{2n}. The matrix, which is closer to the "flat" matrix with respect to the specified metric and different from it at the same time, is searched for.

Description:

Inputs: A, B and C matrices

Any two square matrices of equal dimensions with integer-valued elements, A(m x m) and B(m x m) respectively, where

(1) $m = 2^n$ for some integer $n > 7$; and

(2) the sum of squares of all elements in each column is one and the same constant equal to $m^2 = 2^{2n}$.

The optimal matrix C:

The optimal matrix with respect to our consideration is referred as the BENT matrix C(m x m) with "flat" integer-valued elements possessing equal absolute values ($= \sqrt{m} = 2^{n/2}$).

Searched output: matrix X

A sub-optimal matrix X(m x m) satisfying both of the conditions (1) and (2), which is as **closer** to the BENT matrix C(m x m) as possible (almost flat elements), and different from it at the same time (not all of the elements are the same).

The problem is related to the possible evaluation of both of the **distances**, between A and C, and B and C respectively, with the intention of picking the "flatter" matrix between A and B (the more **closer** to the BENT one).

Any metric (evaluation criterion), that is appropriate for measuring the distance between two such matrices and the BENT one, is needed. Hamming distance and Minkowski distance have already been tried.

Is there any other suitable?

It is necessary for the evaluation criterion:

1. To be sensitive enough, that is, to be able to detect any small changes in the matrix elements absolute values, which in turn adequately to bring an immediate effect on the ranking of the particular matrix evaluated.
2. To allow the maximal deviation, that is, the deviation between the matrix element of maximal absolute value and the value $2^{n/2}$ of all BENT matrix elements, to be detected as well.