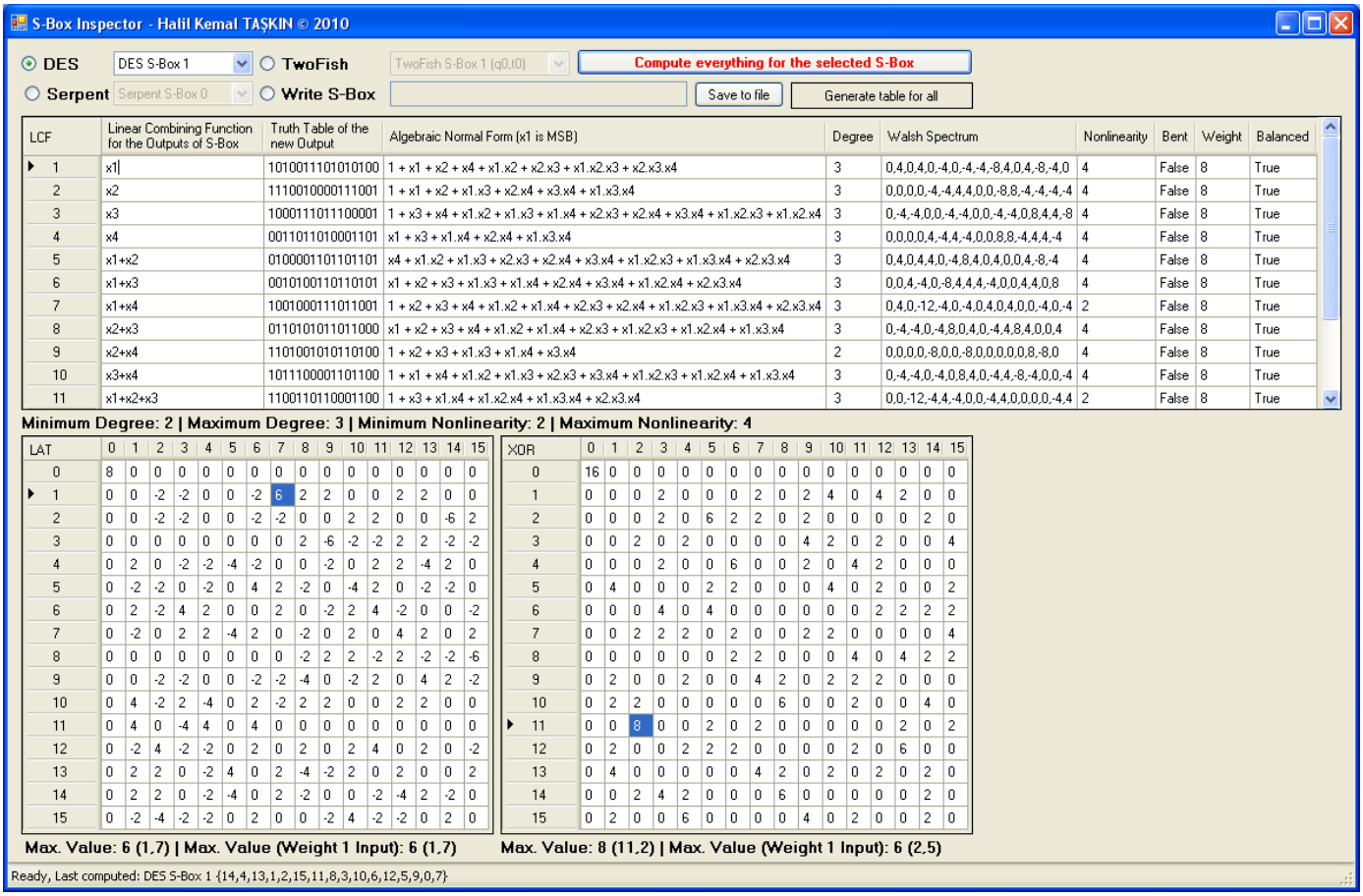
S-Box Inspector

Author: Halil Kemal TAŞKIN



This program computes some properties (Linear Approximation Table, XOR table and some properties of linear combinations of the S-Box outputs) of 4x4 S-Boxes. DES, Serpent and TwoFish S-Boxes are predefined in the program. Also it is able to write another 4x4 S-Box.

The program has been written with Visual Basic .NET using Visual Studio 2008. So .NET Framework 3.5 is required to run the program. There is no any third party algorithm used in the program. All algorithms were written by myself. Usage of the program is very easy. There are 4 radio buttons (○) which allows to choose encryption systems and special S-Box.

If you choose any of the radio button, other sections will be disabled. Once, you have chosen the radio button and the corresponding S-Box from the Combobox ( ), clicking to “Compute everything for the selected S-Box” button will start to compute all data related with the selected S-Box.

First, Linear Combination Functions section will be computed. It will compute the following properties:

- Linear Combining Function for the Outputs of S-Box
- Truth Table of the new Output
- Algebraic Normal Form
- Degree
- Walsh Spectrum
- Nonlinearity
- Bent
- Weight
- Balanced

After that, LAT and XOR table will be computed. Once they have been computed, at the bottom of the tables maximum values for each table and maximum values for input values with weight 1 (i.e. inputs 1,2,4,8) are shown. Also maximum values are highlighted at the tables.

“Write S-Box” mode allows to write any 4x4 S-Box. Once you’ve clicked the radio button, it shows some information message about the input format and usage. And after writing the S-Box values when you click the button “Compute everything for the selected S-Box”, it tries to recognize the written data and asks for the written S-Box values are recognized correctly or not. If there is any mistake, you can return back and correct the mistake.

At the status bar, the corresponding S-Box will be shown after all operations has been completed.

Also, there is a useful button, called “Save to file” which enables to save the generated data to a file. Once you’ve clicked at the button, it will ask for the path of file. There are two available file formats: TXT and CSV. TXT mode saves the file as a simple text file and CSV mode saves the file as a comma seperated values file which allows to use the file in Excel.

Also there is a special button, called “Generate table for all”. This button generates a table (in CSV format) which consists informations for all S-Boxes of DES, Serpent and TwoFish.