What is BSbox-tools?

Dusan Bikov and Iliya Bouyukliev

Abstract

The problems related to representation, defining and computing the most important cryptographic properties of Boolean and Vector Boolean functions (S-boxes) require effective algorithms. With the increasing amount of input data, the problem requires more computational resources. To compute some of the cryptographic properties (linearity, autocorrelation, algebraic degree, differential uniformity) very effective algorithms have to be realized. These algorithms are suitable for parallel implementation.

BSbox-tools is developed software for representation, defining and computing the most important cryptographic properties of Boolean and Vector Boolean functions (S-boxes). For development of this software is use our CUDA oriented library BoolSPLG (Boolean S-box Properties Library for GPUs), a library with parallel algorithms for Boolean functions and S-boxes for GPU. To use this software there is no need knowledge of a programming language.