A Deterministic Optimization Approach for Generating Highly Nonlinear Balanced Boolean Functions in Cryptography

H. M. Le[1], **H. A. Le Thi**[2], **D. T. Pham**[3], **and P. Bouvry**[4]

Abstract: Boolean functions play an important role in cryptography, especially in S-box analysis. They are elementary building blocks for various cryptographic algorithms - stream ciphers, block ciphers, hash functions, etc. Cryptography needs ways to find good Boolean functions so that ciphers can resist cryptanalytic attack. The main properties required are high nonlinearity and low autocorrelation, so that linear cryptanalysis and differential cryptanalysis do not succeed faster than exhaustive key search. These properties have been widely studied in the literature.

We propose in this work a deterministic continuous approach for constructing highly nonlinear balanced Boolean functions, which is an interesting and open question in Cryptography. Our approach is based on DC (Difference of Convex functions) programming and DCA (DC optimization Algorithms). We first formulate the problem in the form of a combinatorial optimization problem, more precisely a mixed 0-1 linear program. By using exact penalty technique in DC programming, this problem is reformulated as polyhedral DC program. We next investigate DC programming and DCA for solving this latter problem. Preliminary numerical results show that the proposed algorithm is promising and more efficient than somes existing heuristic algorithms.

Index Terms: Cryptography, Boolean function, nonlinear balanced Boolean function, nonlinearity, DC programming, DCA, mixed 0-1 linear program, exact penalty.

[1,2] Laboratory of Theoretical and Applied Computer Science (LITA EA 3097)
UFR MIM, University of Paul Verlaine - Metz
Ile du Saulcy, 57045 Metz, France
lehoai@uni-metz.fr, lethi@uni-metz.fr

[3] Laboratory of Modelling, Optimization & Operations Research
National Institute for Applied Sciences - Rouen BP 08, Place Emile Blondel F 76131
Mont Saint Aignan Cedex, France
pham@insa-rouen.fr

[4] Computer Science Research Unit, University of Luxembourg
Campus Kirchberg, 6 Rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
pascal.bouvry@uni.lu