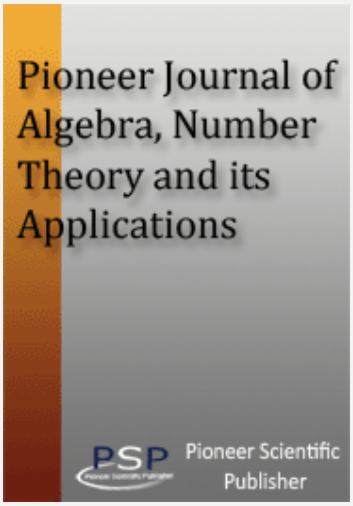
Pioneer Journal of Algebra, Number Theory and its Applications

Volume 4, Issue 1, Pages 5-34 (September 2012)

ISSN: 2231-1831



PROPOSAL FOR A NEW EQUATION SYSTEM MODELLING OF BLOCK CIPHERS AND APPLICATION TO AES 128

Michel Dubois and Eric Filiol

Received September 6, 2012

Abstract

One of the major issues of cryptography is the cryptanalysis of cipher algorithms. Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required. Some mechanisms for breaking codes include differential cryptanalysis, advanced statistics and brute-force.

Recent works also attempt to use algebraic tools to reduce the cryptanalysis of a block cipher algorithm to the resolution of a system of quadratic equations describing the ciphering structure. As an example, Nicolas Courtois and Josef Pieprzyk have described the AES-128 algorithm as a system of 8000 quadratic equations with 1600 variables. Unfortunately, these approaches are, currently, deadlocks because of the lack of efficient algorithms to solve large systems of equations.

In our study, we will also use algebraic tools but in a new way: by using Boolean functions and their properties. A Boolean function is a function from $F_2^n \to F_2$ with $n > 1$, characterized by its truth table. The arguments of Boolean functions are binary words of length n. Any Boolean function can be represented, uniquely, by its algebraic normal form which is an equation which only contains additions modulo 2-the XOR function – and multiplications modulo 2 – the AND function.

Our aim is to describe a block cipher algorithm as a set of Boolean functions then calculate their algebraic normal forms by using the Möbius transforms. After, we use a specific representation for these equations to facilitate their analysis and particularly to try a combinatorial study. Through this approach we obtain a new kind of equations system. This equations system is more easily implementable and could open new ways to cryptanalysis.

To test our approach we first apply this principle to the mini-AES cipher and in a second time to AES-128 algorithm.

Keywords and phrases: block cipher, Boolean function, cryptanalysis, AES.