Cryptology ePrint Archive: Report 2013/011

Evolving balanced Boolean functions with optimal resistance to algebraic and fast algebraic attacks, maximal algebraic degree, and very high nonlinearity.

James McLaughlin and John A. Clark

Abstract: Using simulated annealing, we derive several equivalence classes of balanced Boolean functions with optimum algebraic immunity, fast algebraic resistance, and maximum possible algebraic degree. For numbers n of input bits less than 16, these functions also possess superior nonlinearity to all Boolean functions so far obtained with said properties.

Category / Keywords: Algebraic immunity, nonlinearity, metaheuristics, simulated annealing, stream ciphers, filter functions, algebraic attacks, fast algebraic attacks

Date: received 7 Jan 2013

Contact author: jmclaugh at cs york ac uk