DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

Multiplication of Binary Polynomials - Revisited

Magnus Gausdal Find
Cryptographic Technology Group
National Institute of Standards and Technology

Tuesday, 29 September, 2015 at 14:15

IMADA's Seminar Room

Abstract:

Multiplication of binary polynomials is a fundamental problem, used as a subroutine in many situations such as finite field arithmetic and elliptic curve cryptography. We revisit the problem of multiplication of binary polynomials, with the goal of constructing small circuits over the basis (AND,XOR) computing binary polynomial multiplication.

We develop a systematic way to generate recurrence relations similar to classic recurrence relations such as Karatsuba's technique. For this we use multiplicative complexity as a guiding principle. Applying this technique together with heuristic optimizations we obtain improvements over recent work. To our own surprise we find smaller circuits for multiplication of polynomials for low degrees such a 9 an 14. Combining this with known recurrence relations we obtain improvements for more than 40 values for n in the interval 2,3,..,100.

Joint work in progress with Joan Boyar, Ramn Collazo-Martis, and René Peralta

Host: Joan Boyar