Cryptology ePrint Archive: Report 2011/364

The Value 4 of Binary Kloosterman Sums

Jean-Pierre Flori and Sihem Mesnager and Gérard Cohen

Abstract: Kloosterman sums have recently become the focus of much research, most notably due to their applications in cryptography and their relations to coding theory.

Very recently Mesnager has showed that the value 4 of binary Kloosterman sums gives rise to several infinite classes of bent functions, hyper-bent functions and semi-bent functions in even dimension.

In this paper we analyze the different strategies used to find zeros of binary Kloosterman sums to develop and implement an algorithm to find the value 4 of such sums. We then present experimental results showing that the value 4 of binary Kloosterman sums gives rise to bent functions for small dimensions, a case with no mathematical solution so far.

Category / Keywords: foundations / Kloosterman sums, elliptic curves, Boolean functions, Walsh-Hadamard transform, bent functions

Date: received 5 Jul 2011

Contact author: flori at enst fr