

Cryptology ePrint Archive: Report 2011/400

On a generalized combinatorial conjecture involving addition $\pmod{2^k - 1}$

Gérard Cohen and Jean-Pierre Flori

Abstract: In this note, we give a simple proof of the combinatorial conjecture proposed by Tang, Carlet and Tang, based on which they constructed two classes of Boolean functions with many good cryptographic properties. We also give more general properties about the generalization of the conjecture they propose.

Category / Keywords: foundations / combinatorics, addition, boolean functions

Date: received 26 Jul 2011, last revised 14 Feb 2012

Contact author: flori at enst fr

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: Corrected wrong formulation of our slight extension to the TCT conjecture. In particular, the TD conjecture is NOT included in the proved cases.

Version: 20120214:095906 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]