

Cryptology ePrint Archive: Report 2011/547

The Single Cycle T-functions

Zhaopeng Dai and Zhuojun Liu

Abstract: In this paper the single cycle T-functions are studied. Making use of the explicit formulas of sum and product of 2-adic integers, we present the necessary and sufficient conditions on the generalized polynomial $\widetilde{p}(x) = a_0 \substack{+ \\ \oplus} a_1 x \substack{+ \\ \oplus} \cdots \substack{+ \\ \oplus} a_d x^d \pmod{2^n}$ being a single cycle T-function. Furthermore, for any given generalized polynomial, we can deduce some expressions about its coefficients by which we can determine whether it is single cycle or not.

Category / Keywords:

Date: received 4 Oct 2011

Contact author: dzpkbzy at sina com

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

Version: 20111011:181639 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]