

Poinsot, Laurent

Bent functions on a finite nonabelian group. (English) Zbl 1105.43002
J. Discrete Math. Sci. Cryptography 9, No. 2, 349-364 (2006).

A bent function on a finite nonabelian group is introduced in this paper; it is a natural generalization of a bent function on a finite abelian group introduced by *O. A. Logachev*, *A. A. Salnikov* and *V. V. Yashchenko* [*Discrete Math. Appl.* 7, 547–564 (1997; [Zbl 0982.94012](#))]. Using the theory of linear representations and noncommutative harmonic analysis of finite groups, several properties of such functions similar to the corresponding properties of traditional abelian bent functions are given.

Reviewer: [Tao Renji \(Beijing\)](#)

MSC:

[43A32](#) Other transforms and operators of Fourier type
[94A60](#) Cryptography
[33E99](#) Other special functions

Cited in **1** Review
Cited in **7** Documents

Full Text: [DOI](#)

References:

- [1] Biham E., *Journal of Cryptology* 4 (1) pp 3– (1991) · [Zbl 0729.68017](#) · [doi:10.1007/BF00630563](#)
- [2] Carlet C., *Journal of Complexity* 20 (2) pp 205– (2004) · [Zbl 1053.94011](#) · [doi:10.1016/j.jco.2003.08.008](#)
- [3] Davis J., *Journal of Algebraic Combinatorics* 3 pp 137– (1994) · [Zbl 0797.05018](#) · [doi:10.1023/A:1022446822561](#)
- [4] Dillon J. F., *Elementary Hadamard Difference Sets* (1974) · [Zbl 0346.05003](#)
- [5] Logachev O. A., *Discrete Math. Appl.* 7 (6) pp 547– (1997) · [Zbl 0982.94012](#) · [doi:10.1515/dma.1997.7.6.547](#)
- [6] Matsui M., *Lecture Notes in Computer Science* 765, in: *Advances in Cryptology Eurocrypt '93* pp 386– (1994) · [doi:10.1007/3-540-48285-7_33](#)
- [7] Peyré G., *Mathématiques à l'Université* (2004)
- [8] Pott A., *Discrete Applied Mathematics* 138 (1) pp 177– (2004) · [Zbl 1035.05023](#) · [doi:10.1016/S0166-218X\(03\)00293-2](#)
- [9] Rothaus O. S., *Journal of Combinatorial Theory A* 20 pp 300– (1976) · [Zbl 0336.12012](#) · [doi:10.1016/0097-3165\(76\)90024-8](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.