

New construction of APN quadratic

Zahid Mounir

(Submitted on 19 Jul 2011)

The purpose of this paper is to detail the article of Carlet. Along the way I recall some interesting results in the theory of finite fields, I give (new) proofs of some known results, and then I generalize the construction of a family of APN function. The reference precedes each result, and in the absence of reference the proof is due to the author.

Keywords: boolean, bent, APN

Subjects: **Information Theory (cs.IT)**

Cite as: [arXiv:1107.3614](https://arxiv.org/abs/1107.3614) [cs.IT]

(or [arXiv:1107.3614v1](https://arxiv.org/abs/1107.3614v1) [cs.IT] for this version)

Submission history

From: Zahid Mounir [[view email](#)]

[v1] Tue, 19 Jul 2011 02:54:51 GMT (11kb)

[Which authors of this paper are endorsers?](#)

Download:

- [PDF](#)
- [PostScript](#)
- [Other formats](#)

Current browse context:

cs.IT

[< prev](#) | [next >](#)

[new](#) | [recent](#) | [1107](#)

Change to browse by:

[cs](#)

[math](#)

References & Citations

- [NASA ADS](#)

DBLP - CS Bibliography

[listing](#) | [bibtex](#)

[Zahid Mounir](#)

Bookmark (what is this?)



Science
WISE