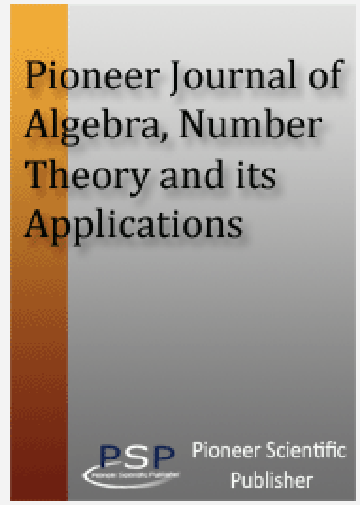
Pioneer Journal of Algebra, Number Theory and its Applications
Volume 2, Issue 1, Pages 45-60 (September 2011)

ISSN: 2231-1831



NEW ENCRYPTION SCHEME BASED ON MODIFIED REED MULLER CODES

El. Hadji Modou Mboup and Cheikh Thiecoumba Gueye

Abstract

It is devised a new cryptosystem based on modified Reed Muller codes $RM(r, m)$. The new cryptosystem is a modified version of Sidel'nikov's one. This allows to increase the security of the public key, and to reconsider Reed Muller codes as good candidates for using in secure encryption scheme. An efficient decoding with the Reed Muller decoding algorithm $RM(r, m)$ and an increased level of security against attacks of the Sidel'nikov's cryptosystem due to Minder and Shokrollahi are the main advantages of the modified version. Adding new columns implies longer codes, but this would not be a problem for decoding or deciphering because in decode one has only to deal with the words of the secret code belonging to the Reed Muller code $RM(r, m)$. So the decoding phase would not suffer from this modification.

Keywords and phrases: McEliece cryptosystem, Minder and Shokrollahi attack, Reed Muller code.