After Sidelnikov proved in 1992 that the cryptosystem of Niederreiter is vulnerable, he designed his own cryptosystem in 1993. This new cryptosystem was based on McEliece schema, it was to be resistant to quantum computers and faster than McEliece cryptosystem. However, in 2007, Minder and Shokrollah proposed an attack proving that the cryptosystem of Sidelnikov was vulnerable as well. This thesis uses several well-known and several new theorems to describe algebraic characteristics of the Reed-Muller code, especially from the affinity point of view.

It proves that the attack proposed by Minder and Shokrollah really breaks the cryptosystem of Sidelnikov. Implementation of this attack in C/C++ language is presented in the conclusion of the thesis along with a table of duration of this attack on a personal computer.