Abstrakt

Na základě Kubického útoku od Itai Dinura a Adi Shamira a další, ve své podstatě podobné, metody jsme navrhli novou techniku linearizace polynomů, která se ukázala být silnější, než samotný Kubický útok. Navíc uvádíme detailní popis a formální důkaz nejen našich nálezů, nýbrž i Kubického útoku. Nakonec demonstrujeme výsledky našeho snažení na Triviu se zkráceným klíčem a inicializačním vektorem. Čistě technikami popsanými v této práci jsme dokázali linearizovat polynom reprezentující bit keystreamu po 621 inicializačních iteracích kryptosystému, v porovnání s 581 inicializačními iteracemi původní techniky.