

Název práce: Analýza proudové šifry QUAD

Autor: Marcel Čurilla

Katedra: Katedra algebry

Vedoucí diplomové práce: doc. Mgr. Štěpán Holub, Ph.D.

Abstrakt: Prúdová šifra QUAD bola predstavená na Eurocrypte autormi Côme Berbain, Henri Gilbert a Jacques Patarin [1]. Ukázali redukciu tejto šifry na problém riešenia m kvadratických rovníc n premenných nad konečným telesom známy, ako MQ problém. Pre zjednodušenie, autori uvažovali len prípad telesa GF(2). V tejto práci predstavím túto prúdovú šifru. Uvidiem dôkaz (redukciu) bezpečnosti šifry QUAD na MQ problém nad ľubovoľným konečným telesom GF(q). Popíšem základné metódy pre riešenie systému kvadratických rovníc nad konečným telesom, linearizáciu a relinearizáciu. Podrobnejšie sa budem venovať algoritmu XL, momentálne najrýchlejšiemu algoritmu na riešenie kvadratických systémov. V analýze šifry QUAD ukážem pre ktoré instancie je šifra QUAD prelomiteľná a naopak pre ktoré instancie je bezpečnosť zaručená.

Klíčová slova: prúdová šifra , QUAD, MQ problém, algoritmus XL