Abstrakt

Cieľom diplomovej práce bolo preskúmať možnosti využitia algoritmu PSO v kryptoanalýze. PSO algoritmus sme aplikovali na riešenie problému jednoduchej zámeny a útoku na šifrový systém DES. Pre jednoduchú zámenu sme pomocou modifikácie diskrétnej verzie PSO dosiahli lepšie alebo porovnateľné výsledky než pomocou iných biologicky motivovaných algoritmov. Navrhli sme spôsob ako využiť PSO na útok na DES a zlomili sme 2-kolový DES pri znalosti len 20 ľubovoľných otvorených a im prislúchajúcich šifrových textov. Analyzovali sme, prečo táto metóda nevedie k úspechu pre viac ako 4-kolový DES. V závere práce sme popísali základné princípy diferenčnej kryptoanalýzy pre DES a navrhli sme špecifickú modifikáciu algoritmu PSO na hľadanie optimálnej diferenčnej charakteristiky pre útok na DES. Pre jednoduché problémy PSO algoritmus funguje veľmi efektívne, pre sofistikované systémy ako DES však bez zabudovania hlbokých znalostí o systéme do algoritmu nie je možné dosiahnuť výraznejšie výsledky.