# Реферат

Обсяг роботи 80 сторінок, 9 ілюстрацій, 9 таблиць, 4 додатки, 13 джерел літератури.

Об’єктом дослідження роботи є кубічні атаки з малими степенями макстермів на криптосистеми, в яких наявні відкриті змінні. Це новий перспективний тип криптоатаки, аналіз застосування якого дозволить виявити вразливі класи шифрів та удосконалити схеми потокового шифрування. Оскільки такі схеми є широко розповсюдженими, то перевірка їх стійкості до нових типів атаки є актуальною задачею.

Предметом дослідження є аналіз кількості сприятливих функцій для кубічної атаки з макстермами малих степенів в залежності від степеня функції та кількості відкритих та секретних змінних, а також оцінка успішності атаки для різних кількостей змінних. Сприятливість функції в даному контексті означає можливість побудови системи рівнянь від бітів секретного ключа, ранг якої в точності дорівнює кількості секретних змінних.

У результаті роботи аналітично отримано вираз для опису залежності кількості сприятливих функцій від різних степенів функції та різної кількості змінних за умови існування макстермів лише першого степеня. Для перевірки правильності формули було розроблено програмну реалізацію алгоритму перебору і підрахунку кількості сприятливих функцій, основною ідеєю якої є використання генератора потенційно сприятливих булевих функцій і застосування до його виходу алгоритмів кубічної атаки для побудови системи рівнянь на основі знайдених суперполіномів. Результати аналітичних розрахунків повною мірою відповідають результатам, отриманим програмним способом.

Була розрахована імовірність успіху атаки для різних комбінацій кількостей відкритих і секретних змінних, що дозволило виявити, що при збільшенні різниці між відкритими та секретними змінними імовірність успіху атаки прямує до одиниці, а в найгіршому випадку сприятливої функції, тобто, коли кількість відкритих змінних дорівнює кількості секретних, для значної кількості змінних імовірність є близькою до нуля. Таким чином, для забезпечення прийнятного рівня імовірності успіху атаки, доцільно розглядати більші степені макстермів

Отримані математичні співвідношення та результати програмних розрахунків можуть бути підґрунтям для дослідження кубічних атак із більшими степенями макстермів, що є перспективною задачею.

КУБІЧНІ АТАКИ, МАКСТЕРМИ, СУПЕРПОЛІНОМИ.