УДК 004.4

І.В. Вітрук, А.М. Луцків канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ DPLL-АЛГОРИТМУ ПРИ ЗДІЙСНЕННІ АЛГЕБРАЇЧНОГО КРИПТОАНАЛІЗУ ПОТОКОВИХ ШИФРІВ

I.V. Vitruk, A.M. Lutskiv Ph.D., Assoc. Prof.

FEATURES OF APPLYING DPLL-ALGHORITM TO THE ALGEBRAIC CRYPTANALYSIS OF STREAM CIPHERS

Суть алгебраїчного криптоаналізу потокового шифру полягає в знаходжені початкового стану регістрів зсуву заданого ключовими потоками бітів. Час є експоненційно залежним від довжини потоку ключа. Потокові шифри з нелінійними функціями генерування бітів ключа (NLCG) є непередбачваними. Кількість рівнянь отриманих представленням потоку ключа у алгебраїчній нормальній формі (АНФ) буде дорівнювати *j* – довжині потоку ключа. Але їх складність та довжина зростатимуть в *4*n* разів, де *n* – кількість регістрів зсуву. Генерування проміжних рівнянь:

$$S_{j+1}^{i} = V(v_i S_j^i * L_i + (1 - v_i) S_j^i) + (1 - V)((1 - v_i) S_j^i * L_i + v_i S_j^i),$$

де S_{j+1}^{i} - стан регістра зсуву *i* на етапі *j+1*, V – majority-біт, v_i – clocking-біт регістра зсуву *i*, L_i – функція зворотнього зв'язку регістра зсуву *i* представлена у вигляді матрці розміром *n*n* (*n* – кількість регістрів зсуву), S_{j+1}^{i} – стан регістра зсуву на етапі *j*.

Отримані стани регістрів зсуву об'єднують за допомогою вихідної функції $f(s_0, s_1, .., s_{n-1})$ для отримання кінцевих рівнянь в АНФ-формі:

$$\begin{cases} k_0 = f(m_0^0, n_0^1, ..., q_0^{n-1}) \\ ... \\ k_{l-1} = f(m_{l-1}^0, n_{l-1}^1, ..., q_{l-1}^{n-1}) \end{cases},$$

де k_{l-1} - це *l-1* біт потоку ключа на етапі, *l* – довжина потоку ключа, $m_{l-1}^0, n_{l-1}^1, ..., q_{l-1}^{n-1}$ – стани останніх бітів в рігістрі в відповідному зсуві на етапі *l-1*. *n* – кількість регістрів зсуву.

Рівняння отримані таким способом є потребують спрощення. Для цього використовуються алгоритми лінереалізації. Після чого відбувається перетворення рівнянь з АНФ до КНФ.

Інструменти розв'язання SAT-задач використовують алгоритм Девіса-Патнема-Логемана-Лавленд (DPLL) - алгоритм пошуку з поверненням для визначення здійсненності булевих формул, які записані у кон'юнктивній нормальній формі. DPLL є високоефективним алгоритмом і використовується у більшості інструментів розв'язання рівнянь. Проте DPLL-алгоритм є неоднозначним у часі розв'язання навіть для однорідних задач. Така неоднозначність зумовлена набором вхідних параметрів та вказівок щодо його роботи. Серед них можна виділити наступні правила: *поширення змінної*, виняток «чистих» змінних (задання значення змінним, що входять у рівняння лише з одною полярністю). Крім того DPLL-алгоритм чутливий до ресурсів пам'яті КС.

Авторами пропонується здійснення емпіричних досліджень по розв'язанню SAT-задач DPLL-алгоритмом з різними параметрами. Для цього використано програмні засоби: *CryptoMiniSAT, Sat4J*. Проведено аналіз результатів часу виконання та оптимізація вхідних параметрів у залежності від характеру системи рівнянь.