УДК 003.26.09; 519.688

А. Луцків
(Тернопільський національний технічний університет імені Івана Пулюя)

ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ АЛГЕБРАЇЧНОГО МЕТОДУ КРИПТОАНАЛІЗУ

На сьогодні в криптології все більшої актуальності набувають алгебраїчні криптоаналітичні методи [1, 2], які теоретично можуть бути застосовані до симетричних та асиметричних, блокових та потокових шифрів. Практичне використання даного методу пов'язане з розв'язанням наступних задач:

1) автоматизованого представлення алгоритму шифрування у вигляді системи рівнянь у аналітичній формі з урахуванням вхідних даних алгоритму;

2) спрощення системи рівнянь у аналітичній формі;

3) перетворення аналітичної форми криптоалгоритму до кон'юнктивної нормальної форми;

4) розв'язання системи рівнянь великої розмірності у кон'юнктивній нормальній формі;

5) коректна інтерпретація розв'язків системи рівнянь.

Таким чином з метою практичного використання даного методу криптоаналізу доцільно створити програмну систему, яка б поєднувала в собі розв'язання усіх вищенаведених задач. Для цього можна скористатися наявними розробками з відкритим вихідним кодом, зокрема [3], які дають змогу розв'язувати п.1 — п.4. На даний момент відповідне програмне забезпечення адаптоване для дослідження потокових алгоритмів шифрування, що базуються на регістрах зсуву зі зворотніми зв'язками: Grain, Trivium, Bivium-B, HiTag2 та Crypto1. Проте дане програмне забезпечення, а саме програмна компонента п.4 у ряді випадків дає некоректні результати для деяких вхідних даних, а також є доцільність адаптувати її для виконання в системах із розподіленою пам'яттю. Розв'язання даної задачі можливе шляхом удосконалення наведеного програмного забезпечення.

Іншим обмеженням наведеного програмного забезпечення є неможливість досліджувати блокові шифри. Розв'язання цієї задачі можливе шляхом розробки математичного, алгоритмічного та програмного забезпечення, на основі ідей запропонованих у роботах Н. Куртуа [1, 2] та згаданої програмної системи [3].

Перелік посилань

1. Courtois N., Klimov A., Patarin J, Shamir A. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations B.Prenell (Ed.): EUROCRYPT 2000, LNCS 1807, pp.392-407, 2000. Springer-Verlag Berlin Heidelberg 2000.

2. Johannes Buchmann, Jintai Ding, Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. Dagstuhl Seminar Proceedings 09031. Symmetric Cryptography. [Електронний ресурс]. - Режим доступу: URL: http://drops.dagstuhl.de/opus/volltexte/2009/1945 — Назва з екрану.

3. Mate Soos Grain of Salt [Електронний ресурс]. - Режим доступу: URL: http://www.msoos.org/grain-of-salt/ — Назва з екрану.