УДК 003.26.09; 519.688
Н.Загородна, С.Лупенко, А.Луцків
(Тернопільський національний технічний університет імені Івана Пулюя)

СУЧАСНІ АЛГЕБРАЇЧНІ КРИПТОАНАЛІТИЧНІ МЕТОДИ СИСТЕМ ЗАХИСТУ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

З метою дослідження криптостійкості сучасних алгоритмів шифрування актуальним є ефективне використання й вдосконалення існуючих, а також розробка принципово нових методів криптоаналізу. Все більшої актуальності набувають алгебраїчні криптоаналітичні методи, які можуть бути застосовані до симетричних та асиметричних, блокових та потокових шифрів. Враховуючи, що шифрування каналу зв'язку відбувається за допомогою симетричних шифрів сеансовими ключами, а шифрування сеансових ключів, з метою передачі незахищеними каналами зв'язку, відбувається за допомогою асиметричних алгоритмів шифрування, дане сімейство криптоаналітичних методів має досить широке застосування.

Під алгебраїчними криптоаналітичними методами мають на увазі методи, які передбачають представлення криптографічних перетворень ключа, вхідних та вихідних даних для шифрування у вигляді деякого рівняння [1,2]. Тоді сукупності таких перетворень формують систему рівнянь. На сьогодні є реалізації даного підходу для криптосистем, які мають практичне використання [3]. Проте, його застосування для широкого кола шифросистем у багатьох випадках носить теоретичний характер або не є в повній мірі дослідженим на даний час.

Можливість використання даного методу пов'язана з необхідністю розв'язання цілої низки теоретичних та прикладних задач, зокрема:

1) представлення алгоритму шифрування у вигляді системи рівнянь у аналітичній формі;

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

3) розв'язання системи рівнянь у кон'юнктивній нормальній формі.

Якщо п.1 і п.2 вимагають чіткої математичної формалізації криптоаналітичної системи, то п.3 пов'язаний з чисельним розв'язком відповідної системи рівнянь великої обчислювальної складності.

Література:

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. Nicolas T. Courtois, Sean O'Neil and Jean-Jacques Quisquater: Practical Algebraic Attacks on the Hitag2 Stream Cipher, In 12th Information Security Conference, ISC 2009, Pisa, Italy 7-9 September 2009, Springer LNCS 5735, pp. 167-176.