УДК 003.26.09:004.032.24-004.272.3
М. Крутих, А. Луцків
(Тернопільський національний технічний університет імені Івана Пулюя)

КОМП'ЮТЕРНА СИСТЕМА ДЛЯ АЛГЕБРАЇЧНОГО КРИПТОАНАЛІЗУ АЛГОРИТМУ AES

З точки зору криптоаналітичного [1] дослідження доцільно розглядати спрощену версію даного алгоритму – S−AES. Цей алгоритм може бути використаний в навчальних цілях, щоб допомогти студентам, які вивчають криптографію та криптоаналіз, а також краще зрозуміти принципи роботи алгоритму AES.

S−AES [3] — це 16−бітний блоковий шифр з 16−бітним секретним ключем. Він складається з 2 раундів, де кожен раунд включає 4 основні операції, а саме NibbleSub, ShiftRow, MixColumn і KeyAddition.

Основною метою даної роботи є дослідження можливості алгебраїчної атаки [4] на алгоритм AES [2]. Для цього слід вирішити наступні завдання:

− дослідити етапи шифрування спрощеного алгоритму AES для визначення алгебраїчних залежностей для побудови системи лінійних рівнянь;

− проаналізувати спрощену версію даного алгоритму і аспекти створення його програмної реалізації для наочного представлення основних закономірностей шифрування;

− здійснити алгебраїчний криптоаналіз спрощеного алгоритму AES і визначити його криптостійкість до цієї атаки;

− створити програмну реалізацію алгебраїчного криптоаналізу, яка б могла знаходити невідомі біти ключа для шифру з розміром блоку 16 біт і довільною кількість раундів шифрування

− дослідити можливості використання алгебраїчного криптоаналізу проти повної версії алгоритму AES.

На основі аналізу спрощеної версії алгоритму AES, досліджено закономірності процесу шифрування з метою представлення його у вигляді системи алгебраїчних рівнянь. Створено програмну реалізацію даного алгоритму.

Реалізовано програмний продукт для побудови систем алгебраїчних рівнянь, розв'язання яких, дозволить знайти біти невідомого ключа.

Також розглянуто стандарт шифрування AES і здійснено порівняння з його спрощеною версією, для подальшого масштабування і використання наявних реалізацій і результатів до повної версії даного алгоритму.

Ведеться розробка програмного продукту для здійснення алгебраїчного криптоаналізу спрощеного алгоритму AES і, в перспективі, повної версії даного алгоритму.

1. Шнайер Б. Криптоанализ — М.: Триумф, 2002. — С. 19—22. — 816 с.

2. Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES).

3. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students - Cryptologia, XXVI (4), 2002.

4. Raphael Chung-Wei Phan, Impossible Differential Cryptanalysis of Mini-AES - Cryptologia, Vol. XXVII, No. 4, October 2003.