УДК 003.26.09:004.032.24-004.272.3
М. Крутих, А. Луцків, канд. техн. наук, доцент
Тернопільський національний технічний університет імені Івана Пулюя

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АЛГЕБРАЇЧНОГО КРИПТОАНАЛІЗУ СПРОЩЕНОГО АЛГОРИТМУ AES

M. Krutykh, A. Lutskiv

SOFTWARE FOR ALGEBRAIC CRYPTANALYSIS OF SIMPLIFIED AES ALGORITHM

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 концепції, що лежать в звичайному алгоритмі AES.

S−AES [3] — це 16−бітний блоковий шифр з 16−бітовим 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 створення програмної реалізації для здійснення алгебраїчного криптоаналізу спрощеного алгоритму AES [4]:

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

− проаналізувати спрощену версію цього алгоритму;

− створити програмну реалізацію для шифрування і дешифрування спрощеного алгоритму AES;

− програмно реалізувати алгебраїчний криптоаналіз для знаходження невідомих бітів ключа для шифру з розміром блоку 16 біт і довільною кількістю раундів шифрування;

− дослідити можливості подальшого використання цієї програми для інших шифрів та повної версії алгоритму AES.

На даний час було розглянуто спрощену версію алгоритму AES і досліджено закономірності процесу шифрування з метою представлення його у вигляді системи алгебраїчних рівнянь. Створено програмну реалізацію даного алгоритму.

Було реалізовано програмний продукт для побудови систем алгебраїчних рівнянь, розв’язання яких, дозволить знайти біти невідомого ключа.

Також розглянуто стандарт шифрування AES [2] і здійснено порівняння з його спрощеною версією, для подальшого масштабування і використання наявних реалізацій і результатів до повної версії даного алгоритму.

Наразі, ведеться розроблення програмного модуля для спрощення системи лінійних алгебраїчних рівнянь для подальшого їх розв'язання з метою отримання бітів ключа.

Література:

1. Шнайер Б. Криптоанализ — М.: Триумф, 2002. — 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. Sean Simmons, Algebraic Cryptanalysis of Simplified AES - Cryptologia, Vol. 33, Issue 4, 2009.