Секция «Математика и механика»

Алгебраическое представление стандарта шифрования AES

Волкова Надежда Викторовна
Студент
МГУ - Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: volk1189@yandex.ru

Advanced Encryption Standard (AES), также известный как Rijndael — симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и широко используется. Тем не менее, для него отчётливо изложено только инженерное описание, представленное в опубликованном Национальным Институтом Стандартов и Технологий в стандарте FIPS-197 AES, облегчающее задачу реализации этой схемы шифрования на ЭВМ.

В данной работе предлагается обобщить имеющееся описание и рассмотреть процессы шифрования и расшифрования как преобразования над кольцом многочленов с коэффициентами из поля Галуа $GF(2^8)$. Такая интерпретация даёт возможность описать необходимые для работы алгоритма свойства упомянутых в стандарте алгебраических структур в более простых терминах свойств многочленов и матриц, что затем позволяет изучить возможные модификации алгоритма и оценить вероятность успешного алгебраического криптоанализа.

Литература

1. Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Кудиц - Образ, 2002
2. Лилд Р., Нидеррайтер Г. Конечные поля. М.: "Мир 1988. Т.1-2.
3. Cid, C., Murphy, S. and Robshaw, M. Algebraic Aspects of the Advanced Encryption Standart. Springer–Verlag, 2006.
4. Barkan, E. and Biham, E. In How Many Ways Can You Write Rijndael? // ASIACRYPT 2002, volume 2501 of LNCS, pages 160-175. Springer-Verlag, 2002.
5. Daemen, J. and Rijmen, V. The Design of Rijndael: AES—The Advanced Encryption Standard. Springer–Verlag, 2002.
6. Ferguson, N., Shroeppel, R., and Whiting, D. // Proceedings of Selected Areas in Cryptography, LNCS, pages 103–111, Springer-Verlag, 2001.
7. National Institute of Standards and Technology. The Advanced Encryption Standard. Federal Information Processing Standards Publication (FIPS) 197, 2001.
8. Toli, I. and Zanoni, A. An Algebraic Interpretation of AES-128. // AES, Fourth International Conference, volume 3373 of LNCS, pages 84-97. Springer-Verlag, 2005.
9. Murphy, S. and Robshaw, M. Further comments on the structure of Rijndael. NIST AES website csrc.nist.gov/encryption/aes, August 2000.