

МЕТОДЫ ВЕРИФИКАЦИИ РЕАЛИЗАЦИЙ АЛГОРИТМОВ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Нейванов А.В.

Научный руководитель – к.т.н., доц. Олейников Р.В.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. Безопасности информационных технологий, тел. (057) 702-14-25), E-mail: andrey.neyvanov@gmail.com.

The given work is devoted to modern developments of operation validation system. It used for testing symmetric block cipher algorithms developed by different independent developers. In this work reviewed Known Answer Test and Monte Carlo Test. They were used to test standard version of ciphers introduced for Advanced Encryption Standard candidate algorithm.

На данный момент является актуальной проблема реализации блочных симметричных шифров (БСШ) и их режимов работы (как аппаратных, так и программных версий) в связи с необходимостью обеспечения таких базовых услуг защиты информации как конфиденциальность и целостность.

БСШ представляет собой функцию, входными параметрами которой выступают открытый текст и ключ, а выходным – криптограмма. Данная функция является обратимой, что позволяет нам при знании шифртекста и ключа получить открытый текст.

Сами по себе шифрующая функция и функция обратная ей, а также режимы их работы являются сложными алгоритмами, содержащими большое количество различных операций. Необходимость проверки корректности их реализаций вызвана следующими требованиями:

- корректностью алгоритмической реализации;
- корректным функционированием программной и аппаратно-программной реализации.

Некорректная алгоритмическая реализация как и некорректное функционирование могут приводить к снижению криптографической стойкости БСШ, что приводит к возможности реализации криптоаналитических атак со сложностью меньшей чем атака «грубая сила».

Тесты «Известных ответов» и «Монте Карло» были использованы в NIST SP 800-17 и NIST SP 800-20. Данные методики позволяют решить проблему верификации реализаций алгоритмов БСШ посредством выявления ошибок реализации логических операций и ошибок использования памяти.

Рассмотренные тесты были реализованы автором программно на языке “С++” и могут быть применены для тестирования реализаций алгоритмов БСШ на программной и аппаратно-программной платформе.