УДК 681.3.06

Р.В. Сергиенко

Львовский институт Сухопутных войск им. гетмана П. Сагайдачного НУ «ЛП», Львов

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕКОТОРЫХ ШИФРУЮЩИХ ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Одним из важных требований к шифрующим подстановочным преобразованиям является отсутствие корреляции с линейными преобразованиями, а также низкое значение автокорреляции. К числу распространенных инструментов оценки таких преобразований относят аппарат булевой алгебры, позволяющий оценить стойкость шифрующего преобразования к различным видам атак.

Проведен анализ критериев и показателей, характеризующих криптографические свойства преобразования. Показано, что сбалансированность, корреляционная иммунность, строгий лавинный критерий (СЛК), значение автокорреляционной функции являются адекватными показателями эффективности шифрующего преобразования. Показано, что вышеуказанные показатели являются определяющими для выбора блока нелинейных замен как примитива раундовой функции поточного шифра.

Представлены результаты исследования криптографических свойств блоков нелинейных замен отечественных и зарубежных шифров, представленных на конкурсы криптоалгоритмов.

Приведенные результаты свидетельствуют о том, что выбор S-блока случайным образом (генерация с последующей проверкой соответствия критериям выбора) приемлемы только для небольших размерностей, например $2^4 \rightarrow 2^4$, тогда как для больших размерностей это является довольно длительным процессом, в особенности при предъявлении жестких критериев отбора. Однако многие отечественные и зарубежные исследователи прибегают к таким методам с целью минимизировать возможность описания блока нелинейных замен алгебраическими способами.

Отмечено, что показатели эффективности блоков нелинейных замен характеризуются компромиссом между дельта-равномерностью, отражающей дифференциальные свойства подстановки, и корреляционными свойствами, важными для поточных шифров.

Список литературы

1. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.

2.Молдавян А.А. Криптография. Скоростные шифры / А.А. Молдавян, Н.А. Молдавян, Н.Д. Гуц, Б.В. Изотов. – СПб.: БХВ-Петербург, 2002, – 493 с.

3.Seberry J. Pitfalls in Designing Boxes (Extended Abstract) / J. Seberry, X.M. Zhang, Y. Zheng // Copyright © Springer-Verlag. – 1998. – P. 384-396.

4. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students, Cryptologia, XXVI (4), 2002. – 298 p.

5. Кузнецов А.А. Симметричный криптографический алгоритм ADE / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко / Радиотехника: Всеукр. межвед. науч.-техн. сб. – Х.: ХТУРЭ, 2007. – Т. 6, Вып. 2. – С. 241-249.

6. *Долгов В.И. Анализ циклических свойств блочных шифров / В.И. Долгов, И.В. Руженцев, И.В Лисицкая. // Прикладная радиоэлектроника. – Х.: ХТУРЭ, 2007. – № 2. – С. 257-263.*