ДИФФЕРЕНЦИАЛЬНЫЕ И ЛИНЕЙНЫЕ СВОЙСТВА УКРАИНСКИХ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Настенко А.А.
Научный руководитель: д-р техн. наук, проф. Долгов В.И.
Харьковский национальный университет радиоэлектроники, Украина
E-mail: nastenko@hotmail.ru

Аннотация — Рассматриваются дифференциальные и линейные свойства полных версий шифров, представленных на конкурс по выбору нового украинского стандарта блочного симметричного шифрования и выполняется сравнение этих свойств с аналогичными свойствами случайных подстановок.

1. Введение

В работе речь идёт о дополнительном обосновании центрального положения новой методологии [1], состоящего в том, что все современные блочные симметричные шифры асимптотически являются случайными подстановками [2 — 4]. Выполняется сравнение дифференциальных и линейных свойств блочных симметричных шифров, представленных на прошедшем украинском конкурсе, с применением новой методики, описанной нами ранее в работе [2].

2. Основная часть

В первой серии экспериментов были рассмотрены дифференциальные свойства на первых десяти циклах шифров Мухомор, Калина, Лабиринт и *ADE* для 30 случайно взятых мастер-ключей. В таблице 1 обобщены результаты таких экспериментов.

Таблица 1

Количество циклов	Калина	*ADE*	Лабиринт	Мухомор
1	19,47	65536	19,4	19,13
2	19,0	19,7	19,75	18,8
3	19,13	19,23	18,93	19,4
4	19,2	19,57	19,21	19,13
5	19,27	19,0	19,1	19,07
6	18,87	19,1	19,42	19,6
7	19,47	19,3	19,12	19,27
8	19,2	19,12	19,3	19,13
9	19,0	19,43	19,42	19,13
10	19,33	19,3	19,12	19,27

Из представленных данных видно, что полные версии шифров, также как и малые их модели [3] действительно после нескольких начальных циклов зашифрования приходят к стационарным состояниям, повторяющим дифференциальные показатели случайных подстановок.

Во второй серии экспериментов были рассмотрены поцикловые значения модулей максимумов таблиц линейных аппроксимаций для вышеуказанных шифров тоже для 30 случайно взятых мастер-ключей и первых десяти циклов. Результаты этих экспериментов представлены в таблице 2.

Из представленных результатов видно, что и по значениям максимумов таблиц линейных аппроксимаций современные блочные симметричные шифры приходят к стационарным состояниям, повторяющим линейные свойства случайных подстановок (после некоторого небольшого количества циклов шифрующего преобразования).

Таблица 2

Количество циклов	Калина	ADE	Лабиринт	Мухомор
1	11008,4	824,3	790,2	32768
2	817,3	818,7	839,3	3914,4
3	817,7	827,5	835,2	9523,2
4	814,1	824,7	832,5	1224,6
5	837,5	831,8	885,4	811,2
6	810,2	814,3	810,3	832,8
7	820,3	820,5	834,4	827,4
8	837,5	823,1	835,7	822,4
9	809,7	810,2	809,2	826,8
10	821,5	821,7	806,1	802,8

3. Заключение

В работе рассмотрены дифференциальные и линейные свойства шифров, представленных на прошедший украинский конкурс по выбору национального стандарта шифрования.

Полученные результаты исследований являются дополнительным свидетельством того, что полные версии шифров асимптотически становятся случайными подстановками. А это означает, что показатели стойкости блочных симметричных шифров могут быть получены расчётным путём из формул, определяющих значения максимумов XOR таблиц и смещений таблиц линейных аппроксимаций, полученных для случайных подстановок [5].

4. Список литературы

[1] Лисицкая И.В. Методология оценки стойкости блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. — 2011. — № 163. — С. 123 — 133.

[2] Лисицкая И.В. Большие шифры случайные подстановки. / И.В. Лисицкая, А.А. Настенко // Межведомственный научн. технический сборник Радиотехника. — 2011. — Вып. 166. — С. 50 — 55.

[3] Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / В.И. Долгов, А.А. Кузнецов, С.А. Исаев. // Электронное моделирование. — 2011. — Т 33, № 6. — С. 81 — 99.

[4] Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. — 2011. — Т.10, №2 — С. 135 — 140.

[5] Олейников Р.В. Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. — 2010. — Т.9, № 3. — С. 326 — 333.

DIFFERENTIAL AND LINEAR PROPERTIES OF THE UKRAINIAN BLOCK SYMMETRIC CIPHERS

Nastenko A.A.
Scientific adviser: Dolgov V.I.
Kharkov National University of Radioelectronics, Ukraine

Abstract — The report presents the differential and linear properties of ciphers submitted to the Ukrainian competition, additionally proving the validity of the hypothesis, that symmetric block ciphers are asymptotically random substitutions.