ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА ПОЛНЫХ ВЕРСИЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ RIJNDAEL, SERPENT, THREEFISH

Фролов О.В.
Научный руководитель: д-р техн. наук , проф. Долгов В.И.
Харьковский национальный университет радиоэлектроники, Украина
E-mail: fglobus@gmail.com

Аннотация — Рассмотрены методики оценки дифференциальных свойств полных версий шифров *Rijndael*, *Serpent*, *Threefish*. Приведены результаты сравнения дифференциальных свойств данных шифров с аналогичными свойствами случайной подстановки.

1. Введение

Для решения задач защиты информации используют криптографические средства и методы. На сегодняшний день в информационном мире широко используются алгоритмы блочного симметричного шифрования.

Однако чтобы оценить качество разработанных шифров, необходимо производить анализ их криптографических свойств.

В докладе приводятся методики исследования дифференциальных свойств полных версий блочных симметричных шифров. Благодаря полученным результатам, подтверждается теория, предложенная на кафедре Безопасности информационных технологий касаемо того, что блочно симметричные шифры ведут себя как случайные подстановки.

2. Основная часть

Учитывая жесткую связь дифференциальных свойств свойств шифрующих преобразований с показателями их стойкости к атакам дифференциального криптоанализа, возникает желание более глубокого их изучения.

Хотелось бы отметить, что среднее значение максимумов таблиц *XOR* разностей является специфическим показателем *S*-блоков фиксированного порядка, не зависящим от циклового класса, к которому принадлежат подстановки. Исследования в данной работе говорят о том, что это свойство является характерным для шифрующих преобразований, не только для малых, но и для больших версий шифров тоже, в то время как многие их подходов к оценке дифференциальных свойств шифров строятся на основе изучения свойств входящих в шифр подстановочных преобразований (*S*-блоков), а не шифров в целом, как подстановок. Также стоит отметить, что решение близкой по постановке задачи выполнялось для малых моделей шифров, что было отмечено в статье Р.В. Олейникова [1].

Для исследования дифференциальных свойств блочных симметричных шифров, были построены таблицы дифференциальных разностей, найдены максимальные значения переходов данных таблицы. Данный анализ выполнялся при помощи разработанного программного обеспечения. Для нахождения максимального значения дифференциала таблица строилась и обрабатывалась построчно.

В таблице 1 представлены сравнительные результаты распределения значений ячеек таблицы *XOR*-разностей для 16-битных сегментов шифртекстов и случайной подстановки порядка 2^{16}.

Таблица 1

$2k$	Количество переходов (подстановка)	Количество переходов (Rijndael)	Количество переходов (Serpent)	Количество переходов (Threefish)
0	2605070418	2604948298	2604933270	2604928534
2	1302484861	1302476170	1302501597	1302508996
4	325626184	325620651	325614188	325612232
6	54271858	54268159	54265223,5	54265483,9
8	6784085	6783987,73	6782692,47	6782055,87
10	678418	678135,4	678425,133	678148,067
12	56535	56512,2	56524,067	56449,467
14	4038	4045,33	4027,133	4061,533
16	252	252,6	261,267	249,467
18	14	13,93	15,267	13,667
20	1	0	0	0

В таблице 2 представлены поцикловые значения максимумов полных дифференциалов для 16-битных сегментов с использованием 10 различных ключей для каждого шифра.

Таблица 2

Число циклов, r	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	16384	18,93	65536
2	8904,25	19,24	65536
3	1911.47	18,64	65536
4	19,24	18,33	42440,04
5	20,31	18,75	30704,23
6	18,83	19,21	9534,57
7	19,21	18,98	37,75
8	19,4	18,37	19,27
9	18,33	19,24	18,78
10	19,17	19,63	18,44

3. Заключение

Благодаря данному анализу можно удостовериться, что результирующие дифференциальные свойства не связаны со свойствами *S*–блоков шифра, а являются общим свойством шифра, как случайной подстановки. Хорошим примером служат результаты анализа шифра Threefish, в котором не используются *S*–блоки.

Также результаты говорят о том, что шифрующие преобразования асимптотически для различных ключей шифрования ведут себя как случайная подстановка, т.е. и для них оказываются справедливыми расчетные соотношения, что используются и для случайной подстановки.

4. Список литературы

[1] 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 PROPERTIES OF FULL VERSIONS OF THE BLOCK SYMMETRIC CIPHERS RIJNDAEL, SERPENT, AND THREEFISH

Frolov O.V.
Scientific adviser: Dolgov V.I.
Kharkov National University of Radioelectronics, Ukraine

Abstract — Methods of the differential properties evaluation of full versions of the block symmetric ciphers: Rijndael, Serpent, and Threefish are considered. The results of a ciphers' differential properties comparison with similar properties in a random permutation are presented.