ИССЛЕДОВАНИЕ СООТВЕТСТВИЯ НОВЫМ КРИТЕРИЯМ ОТБОРА ПОДСТАНОВОЧНЫХ КОНСТРУКЦИЙ СОВРЕМЕННЫХ БСШ

Мельничук Е.Д.
Харьковский национальный университет радиоэлектроники, Украина
E-mail: goabove1970@gmail.com

Аннотация — Рассматриваются показатели случайности *S*-блоков ряда современных шифров.

1. Введение

Известно, что все современные шифры после небольшого начального числа циклов зашифрования становятся случайными подстановками [1 — 4]. В связи с этим активно развиваются методы математическому описанию законов распределения вероятностей случайных подстановок и возможности их использования для построения дополнительных критериев отбора подстановок.

2. Основная часть

Изучим показатели случайности *S*-блоков ряда современных шифров. Нас будут интересовать группа показателей, характеризующих близость свойств *S*-блоков свойствам случайных подстановок. В их число вошли следующие показатели случайности: показатели комбинаторной группы; законы распределения переходов таблиц дифференциальных разностей (далее таблиц *XOR*) и таблиц линейных аппроксимаций (далее *LAT*) и др. Оценка отмеченных показателей будет выполняться на основе методики анализа комбинаторных показателей, а также построения таблиц *XOR* и *LAT* подстановок традиционными методами с последующим изучением законов распределения заполнений этих таблиц.

На основе представленных выше утверждений введены дополнительные критерии случайности.

Критерий 4. Подстановка удовлетворяет критерию случайности 4, если закон распределения однотипных переходов $\Pr\left(\Lambda_{\pi}(\Delta X,\Delta Y)=2k\right)$, $k=0,1,\ldots,k^*$ её таблицы *XOR* разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов [1], то есть наибольшее значение модуля разности теоретического и эмпирического интегральных законов распределения вероятностей удовлетворяет условию $|F_T(x_k)- F(x_k)|\le b$, где b является параметром 4, выбираемым экспериментальным образом.

Критерий 5. Подстановка удовлетворяет критерию случайности 5, если закон распределения однотипных переходов $\Pr\left(\lambda\cdot(\alpha,\beta)=2k\right)$, $k=0,1,\ldots,k^*$ её таблицы линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения [1], то есть наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_T(x_k)- F(x_k)|\le c$, где c является параметром критерия 5, выбираемым экспериментальным образом.

Наконец, с применением этих критериев введено новое понятие случайной подстановки. Оно сформулировано в следующем виде:

Подстановка является случайной, если вместе с выполнением критериев случайности (1 … 3) [1] для заполнений ячеек её *XOR* таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей (1) и (2) (выполняются критерии случайности 4 и 5).

В таблице 1 приведена оценка соответствия закона распределения таблицы *XOR* шифра Лабиринт теоретическому распределению парных разностей для *XOR* таблицы подстановки порядка 2^8.

Таблица 1

Элемент	Плотность	Теоретическая плотность	Теоретическая вероятность
0	32640	39363	0,605345
2	32130	19758	0,303855
4	255	4959	0,0762627
6	0	830	0,0127609

3. Заключение

Полученные результаты свидетельствуют, что практически все рассмотренные *S*-блоки, используемые в современных шифрах, не укладываются в рамки *S*-блоков случайного типа.

Более того оказалось, для обеспечения высоких криптографических показателей шифров совсем не требуются *S*-блоки со специальными свойствами. Наши проработки показали, что показатели стойкости, свойственные шифрам с специально отобранными подстановками можно реализовать с помощью *S*-блоков случайного типа (сгенерированных случайным способом) вообще (без каких-либо дополнительных ограничений на показатели случайности).

Опять мы можем констатировать вывод, что поиск *S*-блоков с улучшенными криптографическими показателями потерял всякий смысл. Стоящие задачи успешно решаются с помощью *S*-блоков, сгенерированных случайным образом.

4. Список литературы

[1] 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.

[2] 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.

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

[4] Лисицкая И.В. Дифференциальные свойства шифра FOX / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2. — С. 122 — 126.

INVESTIGATION OF THE SUITABILITY OF THE S-BOXES OF THE MODERN CIPHERS TO NEW SELECTION CRITERIA

Melnychuk E.D.
Kharkov National University of Radioelectronics, Ukraine

Abstract — The S-block randomness properties of some modern ciphers are considered. The results of the property comparison for several cases are presented.