Таким образом, описаны матрицы вероятностей ключей неэндоморфных совершенных шифров и множества вероятностей шифробозначений в случае, когда мощность множества шифрвеличин равна двум. Отметим, что при $\lambda > 2$ эта задача сильно усложняется ввиду отсутствия аналога теоремы Биркгофа о дважды стохастических матрицах.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
5. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.

УДК 519.7 DOI 10.17223/2226308X/8/24

ПРЕДВАРИТЕЛЬНАЯ ОЦЕНКА МИНИМАЛЬНОГО ЧИСЛА РАУНДОВ ЛЕГКОВЕСНЫХ ШИФРОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИХ УДОВЛЕТВОРИТЕЛЬНЫХ СТАТИСТИЧЕСКИХ СВОЙСТВ[1]

А. И. Пестунов

Для новых легковесных блочных шифров (и нескольких известных шифров) проведена экспериментальная оценка минимального числа раундов, при котором в режиме CTR эти шифры обеспечивают удовлетворительные статистические свойства выходной псевдослучайной последовательности. Эксперименты проводились с помощью статистического теста «стопка книг» при длине выборки 2^{26} байт. В зависимости от шифра блоки представлялись в виде двух, трёх или четырёх 32-битовых слов и в качестве элементов тестируемой выборки брались первые слова каждого выходного блока. На вход шифра подавались блоки, где все слова, кроме второго, равны нулю, а второе слово менялось от 0 до $2^{24} - 1$.

Ключевые слова: *блочный шифр, легковесный шифр, статистический анализ, статистический тест, число раундов, псевдослучайные числа.*

Одно из применений итеративных блочных шифров — это генерация псевдослучайных чисел. Для этой цели часто используется режим CTR, подразумевающий последовательное шифрование значений некоторого счётчика и формирование псевдослучайной последовательности из выходных блоков или их частей. При этом удовлетворительные статистические свойства выходной последовательности могут быть обеспечены значительно меньшим числом раундов (обозначим его $R_{\min}$), чем полное число раундов шифра (обозначим его R). Очевидно, что сокращение числа раундов увеличит производительность шифров и позволит генерировать псевдослучайные числа быстрее. Причём даже если такой усечённый шифр имеет высоковероятные характеристики (линейные, дифференциальные, интегральные и пр.), он сможет генерировать псевдослучайные последовательности с удовлетворительными статистическими свой-

[1]Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).

ствами в силу того, что вероятность появления блоков с требуемыми на входе шифра свойствами может быть ничтожно малой.

Поскольку блочные шифры претендуют на универсальность, решая целый спектр прикладных задач (генерация псевдослучайных чисел является одной из них), то при создании новых шифров помимо R, возможно, имеет смысл указывать и $R_{\min}$, обеспечивающее удовлетворительные статистические свойства, не гарантируя криптографической стойкости. Уже сейчас при варьировании длины ключа задаётся различное число раундов у шифров, например AES, CLEFIA, Piccolo, SIMON или SPECK. В частности, для шифра AES предполагается, что 10 раундов должны обеспечивать отсутствие атак быстрее 2^{128}, 12 раундов — быстрее 2^{192}, а 14 раундов — быстрее 2^{256}.

В работе приводятся результаты статистического анализа легковесных итеративных блочных шифров (и нескольких известных), цель которого — осуществить предварительную оценку $R_{\min}$. Значительная часть реализаций шифров взята из библиотеки BLOC [1, 2].

Исследование проводилось при помощи статистического теста «стопка книг» [3, 4], который ранее уже применялся для анализа других блочных шифров [5 – 7]. Данный тест подразумевает вычисление статистики x^2, подчиняющейся распределению хи-квадрат, если элементы выборки равномерно распределены. Число степеней свободы в распределении хи-квадрат определяется параметром теста — количеством частей в структуре данных «стопка книг». В настоящей работе этот параметр равен 2, а число степеней свободы — 1.

При тестировании для каждого шифра варьировалось число раундов: 1, 2, 3 и т. д. Для каждого раунда генерировалось по 10 выборок (на 10 случайных мастер-ключах) размера 2^{26} байт (2^{24} 32-битовых слов) и по каждой из них вычислялась статистика x^2. Выборки генерировались следующим образом: в зависимости от шифра блоки представлялись в виде двух, трёх или четырёх 32-битовых слов и в качестве элементов выборки использовались первые слова каждого выходного блока; на вход шифра подавались блоки, где все слова, кроме второго, равны нулю, а второе слово менялось от 0 до $2^{24}-1$. Значения статистики x^2 сравнивались с квантилью хи-квадрат уровня значимости 0,05 с одной степенью свободы. При этом для каждой серии из 10 таких выборок подсчитывалось число $U_{0,05}$, означающее количество превышений статистикой x^2 данной квантили (табл. 1).

Таблица 1

Символические обозначения

$U_{0,05}$	0–2	3–5	6–7	8–10
Обозначение	—	$\mp$	$\pm$	+

Поскольку статистические свойства шифра улучшаются с ростом числа раундов, то при определённом числе раундов распределение выборки не отличается от равномерного. Данное число (обозначим его через $\hat{R}_{\min}$) возьмём в качестве предварительной оценки для $R_{\min}$. Результаты экспериментов показали, что в среднем рассмотренные блочные шифры сохраняют удовлетворительные статистические свойства при сокращении числа раундов в них до 10–30 % от полного числа раундов (табл. 2 и 3).

Статистический анализ, результаты которого представлены здесь, является предварительным в том смысле, что он даёт минимальную границу $R_{\min}$. В частности, более тщательный подбор входной последовательности и использование других статистических тестов может «забраковать» большее число раундов.

Таблица 2

Блочные шифры, для которых отклонения от равномерного распределения фиксируются при более чем 13 раундах

Раунды	1–14	15	16	17	18–24	25	26–27	28–29	30	$R_{\min}$	R	%
Simon	+	∓	—	∓	—	—	—	—	—	18	32–72	25–56
Katan64	+	+	+	+	+	+	—	+	—	30	254	12
Ktantan64	+	+	+	+	+	+	—	+	—	30	254	12

Таблица 3

Блочные шифры, для которых отклонения от равномерного распределения фиксируются не более чем при 13 раундах

Раунды	1	2	3	4	5	6	7	8	9	10–13	14	$\hat{R}_{\min}$	R	%
XTEA	+	+	—	—	—	—	—	—	—	—	—	3	32	6
SPECK	+	+	+	+	+	—	—	—	—	—	—	6	22–34	15–23
CLEFIA	+	+	+	+	+	—	—	—	—	—	—	6	18–26	19–28
Piccolo	+	+	+	+	+	—	—	—	—	—	—	6	25–31	16–20
KLEIN	+	+	∓	—	—	—	—	—	—	—	—	4	12–20	10–17
mCrypton	+	+	+	—	∓	—	—	—	—	—	—	6	12	25
LED	+	+	+	—	—	—	—	—	—	—	—	4	32–48	6–10
Noekeon	±	—	—	—	—	—	—	—	—	—	—	2	16	6
MIBS	+	—	—	—	—	—	—	—	—	—	—	2	32	3
IDEA	+	—	—	—	—	—	—	—	—	—	—	2	8.5	12
AES	+	+	+	—	—	—	—	—	—	—	—	4	10–14	21–30
DESXL	+	—	—	—	—	—	—	—	—	—	—	2	8	25
Lblock	+	+	+	+	+	+	+	±	—	—	—	9	32	25
Present	+	+	+	+	+	+	+	±	—	—	—	9	31	26
Twine	+	+	+	+	+	+	+	+	—	—	—	9	36	22
Hight	+	+	+	+	+	+	+	+	+	—	—	10	32	28
Sea	+	+	+	+	+	+	+	+	+	—	—	10	51	18
Skipjack	+	+	+	+	+	+	+	+	+	+	—	14	32	34

Более детальный анализ с подробным описанием экспериментов планируется опубликовать в одной из последующих работ.

ЛИТЕРАТУРА

1. *Cazorla M., Marquet K., and Minier M.* Survey and benchmark of lightweight block ciphers for wireless sensor networks // Proc. 10th Intern. Conf. SECRYPT-2013, July 2013, Reykjavik, Iceland. P. 543–548.
2. *Cazorla M., Gourgeon S., Marquet K., and Minier M.* BLOC Library: Implementations of lightweight block ciphers on a WSN430 sensor [Электронный ресурс]. `http://bloc.project.citi-lab.fr/library.html/`
3. *Рябко Б. Я., Пестунов А. И.* «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. 2004. Т. 40. № 1. С. 73–78.
4. *Пестунов А. И.* Теоретическое исследование свойств статистического теста «стопка книг» // Вычислительные технологии. 2006. Т. 11. № 6. С. 96–103.
5. *Рябко Б. Я., Монарев В. А., Шокин Ю. И.* Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. Т. 41. № 4. С. 385–394.
6. *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
7. *Pestunov A.* Statistical analysis of the MARS block cipher // Cryptology ePrint Archive. 2006. Report No. 2006/217. `https://eprint.iacr.org/2006/217/`