Применение атаки различения на легковесные блочные шифры, основанные на ARX-операциях*

А. С. Сосков[1,†], Б. Я. Рябко[1,2]

[1]Институт вычислительных технологий СО РАН, Новосибирск, Россия

[2]Новосибирский государственный университет, Россия

[†]Контактный e-mail: sashasasha-1987@mail.ru

Рассмотрено применение атаки различения на ряд легковесных блочных шифров, основанных на ARX-операциях (сложение по модулю, циклический сдвиг и исключающее ИЛИ). Представлены экспериментальные результаты и теоретические оценки устойчивости легковесных шифров Speck, Simon, Simeck, HIGHT, LEA к атаке различения. Вывод, что семейство шифров Simeck не выдерживает эту атаку, сделан на основе прогнозов, полученных путем экстраполяции экспериментальных данных.

Ключевые слова: криптография, легковесные блочные шифры, атака различения, Speck, Simon, Simeck, HIGHT, LEA, ARX-based.

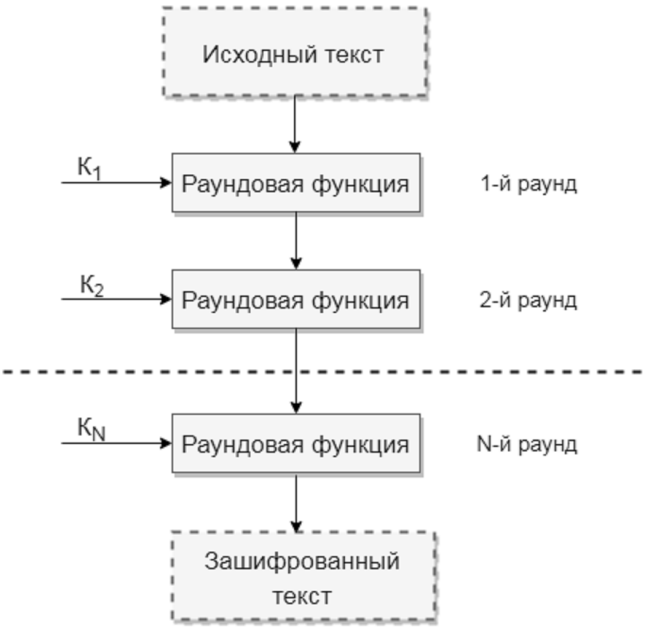
Библиографическая ссылка: Сосков А.С., Рябко Б.Я. Применение атаки различения на легковесные блочные шифры, основанные на ARX-операциях // Вычислительные технологии. 2019. Т. 24, № 3. С. 106–116. DOI: 10.25743/ICT.2019.24.3.008.

Введение

В последние годы наряду с персональными компьютерами, ноутбуками и смартфонами появилось большое количество устройств, которыми можно управлять через Интернет. Эти устройства сильно ограничены по вычислительной мощности, имеют малый объем и отличаются низким энергопотреблением. Примерами систем с такими устройствами являются многие элементы из “Интернета Вещей”, беспроводная сенсорная сеть, RFID-метки и др. Развитие указанных технологий делает чрезвычайно актуальными вопросы, связанные с их информационной безопасностью. Так как применение большинства “традиционных” шифров к этим устройствам практически невозможно из-за ограничений по вычислительной мощности, в последние 10–15 лет было предложено большое количество легковесных (lightweight) блочных алгоритмов, а в 2012 г. принят международный стандарт (ISO/IEC 29192), в котором указаны основные требования к алгоритмам легковесной криптографии.

В настоящей работе рассматриваются шифры итерационного типа (рис. 1), которые преобразуют блоки открытого текста постоянной длины в блоки шифротекста той же длины посредством циклически повторяющейся обратимой функции или так называемой раундовой функции [1].

*Title translation and abstract in English can be found on page 115.



Общий принцип работы блочного шифра итерационного типа.
N — число раундов, K_1, K_2 K_N — раундовые ключи

Размер блока шифра — это фиксированный параметр, обычно равный 32, 48, 64, 96 или 128 битам. Раундовая функция шифра обрабатывает исходный текст определенное число раз, в итоге на выходе формируется зашифрованный текст. Такие итерации называются раундами. Количество раундов N задается авторами шифра. Обычно раундовые функции используют различные ключи, полученные из первоначального ключа (так называемое растягивание ключа), которые принято называть раундовыми ключами. Более детальное описание раундовой функции и формирования раундового ключа для каждого исследуемого в работе шифра приведено в [2 – 5].

Все блочные шифры должны быть устойчивы ко всем известным типам атак, в том числе и к атаке различения [6]. Цель такой атаки заключается в том, чтобы отличить зашифрованные данные от случайной последовательности. Если это удается, то обычно шифр не рекомендуется к практическому использованию.

В настоящей работе атака различения применяется к блочным шифрам Speck и Simon [2], Simeck [3], HIGHT [4], LEA [5]. Шифры Speck и Simon — два семейства легковесных блочных шифров, которые представлены Агентством национальной безопасности США в 2013 г., а в 2014 г. включены в международный стандарт ISO/IEC 29192. Оба семейства поддерживают различные размеры блоков для шифрования и ключа. Входной блок имеет размеры 32, 48, 64, 96, 128 бит, а секретный ключ — 64, 72, 96, 128, 144, 256 бит. Число раундов для шифрования зависит от выбранных параметров. В табл. 1 представлены параметры блока и ключа для шифров Speck и Simon и соответствующее число раундов, необходимое для шифрования.

Новое семейство легковесных блочных шифров Simeck спроектировано на основе шифров Speck и Simon. Как считают авторы шифра, Simeck работает быстрее и экономнее, обеспечивая примерно такую же информационную безопасность, что Speck и Simon. Шифр Simeck реализован для трех размеров блока (32, 64, 128 бит) и секретного ключа (64, 96, 128 бит).

Т а б л и ц а 1. Входные параметры шифров

Шифр	Размер блока, биты	Размер ключа, биты	Число раундов
Speck	32	64	22
«	48	96	23
«	64	128	27
Simon	32	64	32
«	48	96	36
«	64	128	44
Simeck	32	64	32
«	48	96	36
«	64	128	44
HIGHT	64	128	32
LEA	128	128	24

Шифр HIGHT предложен в 2006 г., он поддерживает 64-битный блок и 128-битный ключ. Шифр LEA предложен в 2013 г. Он поддерживает 128-битный блок и три размера ключа (128, 192, 256 бит). Число раундов определяется авторами шифра и зависит от выбранных параметров (табл. 1). Отметим, что на данный момент не было опубликовано сведений об атаках, которые позволили бы взломать какой-либо из указанных шифров с полным числом раундов. В работах [7, 8], где описаны наиболее успешные атаки на шифры Speck, Simon и Simeck, рассматриваются атаки на усеченное число раундов шифра. В работе [9] описана атака на 30 раундов шифра Simeck с входным блоком 48 бит и секретным ключом 96 бит (далее 48/96) (при полном числе раундов 36), требующая 2^{48} байт текста и 2^{92} операций шифрования, для Simeck 64/128 описана атака на 37 раундов шифра (при полном числе раундов 44), требующая 2^{63} байт текста и 2^{121} операций шифрования.

В настоящей работе с помощью статистического теста “стопка книг” проведено исследование легковесных блочных шифров Speck, Simon, Simeck, HIGHT, LEA на устойчивость к атаке различения. Представлены экспериментальные результаты, а также даны теоретические оценки, сколько блоков текста необходимо для того, чтобы отличить шифротекст от случайности.

Экспериментально установлено, что шифротекст после половины всех раундов шифра Simeck 48/96 не подчиняется равномерному распределению. На основании полученных экспериментальных данных построен прогноз, позволяющий предположить, что последовательность на выходе шифра Simeck 48/96 после полного числа раундов можно отличить от равномерного распределения, если ее размер составляет 2^{94} байт. Атака на шифр Simeck 48/96 с полным числом раундов представлена впервые[1]. Остальные семейства легковесных блочных шифров Speck, Simon, LEA, HIGHT показали хорошую устойчивость к атаке различения.

Статья организована следующим образом. В первом разделе дано описание примененной в работе атаки различения. В разд. 2 приведено описание статистического теста “стопка книг”, с помощью которого находились отклонения зашифрованной выборки от случайной. В разд. 3 представлены полученные экспериментальные данные, а в разд. 4 дана теоретическая оценка устойчивости анализируемых шифров к атаке различения.

[1]Предварительные результаты анонсированы в IACR Cryptology ePrint Archive `https://eprint.iacr.org/2018/047.pdf`, а также в трудах международной научной конференции SIBIRCON-2017 `https://ieeexplore.ieee.org/document/8109901`.

1. Описание атаки различения

Для определения устойчивости шифров к атаке различения использована следующая схема: выборка на выходе шифра с неполным числом раундов анализировалась с помощью статистического теста (так как структура шифра позволяет исследовать текст, зашифрованный после любого числа итераций раундовой функции, а не только после конечного числа раундов). Если отклонения от случайной последовательности удавалось найти, число раундов повышалось на 1 и повторялась процедура, описанная выше, до тех пор, пока статистический тест не отличал зашифрованную выборку от случайной. Таким образом, подавая на вход заведомо неслучайные последовательности разной длины, мы находили максимальное число раундов и минимальную требуемую длину последовательностей, при которых зашифрованная выборка оказывалась неслучайной. Затем минимальная требуемая длина для успешной атаки различения экстраполировалась на шифры с полным числом раундов и оценивалась возможность проведения такой атаки.

На вход функции шифрования подавались блоки, составленные из заведомо неслучайных последовательностей, которые формировались с помощью кодов Грея [10]. Рефлексивный двоичный код Грея (далее — код Грея) является упорядоченным множеством двоичных слов одинаковой длины, в котором два соседних слова различаются только в одном разряде. Используя коды Грея, можно получить последовательность любой размерности (это важно, так как для блока шифра, равного n битам, нужно подавать последовательность именно этого же размера) и любой длины. Например, если шифр имел 32-битный входной блок, требовалось построить множество 32-битных слов, чтобы подать их на вход. Для этого формировалось необходимое число слов кода Грея длины k бит, а затем слева к каждому слову "дописывались" $(32 - k)$ нуля для получения размера слова, равного 32 битам. Например, получались следующие числа: 00..00, 00..01, 00..11, 00..10 и т. д. Затем путем последовательного добавления этих чисел получался блок нужной длины и подавался на вход.

Рассмотрим подробно пример генерации кодов Грея для трех бит ($n = 3$) на основании кодов для двух бит ($n = 2$): коды Грея для двух бит выглядят таким образом: $00, 01, 11, 10$. Запишем коды в обратном порядке: $10, 11, 01, 00$. Затем к начальному списку допишем нули: $000, 001, 011, 010$, а к перевернутому списку — единицы: $110, 111, 101, 100$. Соединим эти два списка и получим последовательность кодов Грея для трех бит: $110, 111, 101, 100, 000, 001, 011, 010$. Аналогично коды Грея для n бит могут быть рекурсивно построены на основе кода для $n - 1$ бит.

2. Описание теста "стопка книг"

Для анализа зашифрованных данных применим статистический тест "стопка книг", который предложен в [11], его подробное описание дано в [12, 13][2].

Допустим, имеем выборку $X = (x_1, x_2, ..., x_N)$ из алфавита $A = (a_1, a_2, ..., a_s)$. С помощью теста "стопка книг" проверяем гипотезу H_0 о том, что элементы из выборки X равновероятны относительно друг друга, т. е. выполняется $P(x_N = a_i) = p^0 = 1/S$, $n = 1, ..., N,\ i = 1, ...s$. Первоначально все "буквы" алфавита находятся в произвольном

[2]Программная реализация теста выполнена Алексеем Лубкиным. Исходный код доступен по адресу: `https://github.com/sashasasha-1987/book-stack`.

порядке от 1 до S, который после анализа каждого элемента x_n из выборки X меняется по формуле

$$w^{n+1}(a) = \begin{cases} 1, & x_n = a, \\ w^n(a) + 1, & w^n(a) < w^n(x_n), \\ w^n(a), & w^n(a) > w^n(x_n). \end{cases}$$

Такая конструкция похожа на стопку книг, если представить, что номер книги обозначает ее позицию в стопке. Книга извлекается из стопки и после "прочтения" кладется сверху, а ее номер становится первым. Книги, которые первоначально находились сверху, сдвигаются вниз, а порядковые номера книг, которые находились снизу, не меняются. Если гипотеза H_0 окажется неверна, то самые часто используемые книги будут постоянно находиться около вершины стопки. Если же H_0 верна, то вероятность найти элемент x_n на любой позиции в "стопке книг" равна $1/S$.

Перед тестированием множество всех "букв" из алфавита делится на две непересекающиеся части: $A_1 = 1, 2, ..., M$ и $A_2 = M + 1, M + 2, ..., S$. Для x_n из выборки X подсчитывается количество элементов $w^n(x_n)$, вошедших в первую A_1 и вторую A_2 части. V_0 означает количество попаданий в верхнюю часть стопки книг, а $N - V_0$ — количество попаданий в нижнюю ее часть. Статистика x^2 вычисляется по формуле

$$x^2 = \frac{(V_0 - NP_1)^2}{NP_1} + \frac{((N - V_0) - N(1 - P_1))^2}{N(1 - P_1)},$$

где $P_1 = |A|/S$.

Известно, что x^2 асимптотически стремится к распределению χ^2 (в нашем случае с одной степенью свободы) [14]. Значение x^2 нужно сравнить с квантилем распределения χ^2 согласно заданной вероятности α. Если $x^2 < \chi^2_{1,\alpha}$, то гипотеза H_0 о равновероятности элементов из выборки X принимается, иначе — отвергается. В нашем эксперименте задана вероятность $\alpha = 0.99$, для которой $\chi^2_{1,0.99} = 6.6349$. Таблицу квантилей χ^2 можно найти в [14].

3. Экспериментальные результаты

На примере шифра Simeck покажем, как были получены экспериментальные результаты и каким образом их нужно интерпретировать. На вход исследуемых шифров подавались последовательности разной длины, составленные из кодов Грея. Полученный зашифрованный текст анализировался с помощью статистического теста "стопка книг". Если значение x^2 было больше величины квантиля $\chi^2_{1,0.99} = 6.6349$, делался вывод, что выходная последовательность неслучайна с вероятностью 99 %. Отметим, что все вычисления были выполнены на вычислительном комплексе ИВЦ НГУ.

В табл. 2 на примере шифра Simeck 32/64 показана зависимость степени случайности зашифрованной последовательности от числа раундов и размера подаваемой выборки. Проведено сто тестов для ста случайно выбранных ключей. Здесь Q — количество случаев, когда анализируемая выборка оказалась неслучайной; S — длина подаваемой на вход шифра последовательности; R — номер раунда, после которого анализировалась полученная выходная последовательность. Из таблицы видно, что при увеличении числа раундов зашифрованная последовательность становится все "более случайной", а увеличение длины зашифрованной выборки приводит к тому, что эта последовательность

Т а б л и ц а 2. Simeck 32/64. Зависимость степени случайности зашифрованной последовательности от числа раундов и размера подаваемой выборки

R	10	10	11	11	11
S, байты	2^{28}	2^{29}	2^{30}	2^{31}	2^{32}
Q	80	100	9	23	54

становится "менее случайной". Этот широко известный теоретический факт согласуется с подобными исследованиями для других шифров [15, 16].

В табл. 3 предоставлены результаты анализа шифра Simeck с параметрами 48/96 и 64/128. Проведено также сто тестов для ста случайно выбранных ключей. При выбранном уровне значимости 0.01 (т. е. $\alpha = 0.99$) можно сделать вывод, что атака различения успешно применена, если хотя бы в двух–трех тестах были отклонения зашифрованной последовательности от случайной. В этом случае атака различения успешно применена для 18 раундов, при этом минимальная требуемая длина подаваемой на вход выборки составляла $2^{38.5}$. Для Simeck с параметрами 64/128 атака различения успешно проведена для 19 раундов, при этом минимальная требуемая длина подаваемой на вход выборки составляла 2^{36}.

В табл. 4 представлено максимальное количество раундов для семейства легковесных блочных шифров Simeck с различными размерами блока и ключей, после которых тест зафиксировал отличие зашифрованной выборки от случайной. Здесь S — длина подаваемой на вход шифра последовательности, необходимая для обнаружения "неслучайностей" у зашифрованной последовательности; R — количество раундов, после которого анализируемая выборка оказалась неслучайной. В скобках указано полное число раундов, заданное авторами этих шифров.

Все результаты, указанные в табл. 2–4, получены экспериментальным путем. Примечательно, что для Simeck 48/96 и Simeck 64/128 число раундов, после которого выборка с зашифрованными данными не является случайной, достаточно велико и составляет

Т а б л и ц а 3. Число раундов, после которых выходная последовательность неслучайна

Simeck 48/96										
R	9	10	11	12	13	14	15	16	17	18
S, байты	$2^{6.5}$	$2^{8.5}$	$2^{13.5}$	$2^{17.5}$	$2^{20.5}$	$2^{24.5}$	$2^{28.5}$	$2^{32.5}$	$2^{35.5}$	$2^{38.5}$

Simeck 64/128										
R	10	11	12	13	14	15	16	17	18	19
S, байты	2^{11}	2^{12}	2^{14}	2^{17}	2^{20}	2^{23}	2^{26}	2^{29}	2^{33}	2^{36}

Т а б л и ц а 4. Семейство легковесных блочных шифров Simeck. Экспериментальная атака

Размер блока/ключа, биты	R	S, байты
32/64	10 (32)	2^{29}
48/96	18 (36)	$2^{38.5}$
64/128	19 (44)	2^{36}

в первом случае около 50 % от общего числа раундов и 43 % во втором. Например, если увеличить вычислительную мощность системы, при помощи которой проводился эксперимент, шифр Simeck окажется неустойчив к такому типу атак в случае большего количества раундов, а может быть, и для полного числа раундов.

4. Прогнозы

Чтобы понять, устойчив ли шифр Simeck с такими входными параметрами к атаке различения, мы, основываясь на полученных экспериментальных результатах, экстраполировали минимальную длину последовательности, необходимую для успешной атаки различения на последующие раунды. Обозначим ее как $\hat{S}(r)$. Построение прогноза и доверительных интервалов выполнено методом, описанным в [17]:

$$\log_2 \hat{S}(r) = ar^2 + br + c. \tag{1}$$

Параметры уравнения регрессии (1) находились с помощью метода наименьших квадратов:

$$\begin{cases} c \cdot n + b \sum r_i + a \sum r_i^2 = \sum \log_2 S_i, \\ c \sum r_i + b \sum r_i^2 + a \sum r_i^3 = \sum \log_2 S_i r_i, \\ c \sum r_i^2 + b \sum r_i^3 + a \sum r_i^4 = \sum \log_2 S_i r_i^2. \end{cases} \tag{2}$$

В результате решения системы уравнений (2) для Simeck 48/96 получены значения коэффициентов уравнения регрессии: $c = -31.182$, $b = 4.3045$, $a = -0.0227$. После подстановки этих значений в уравнение (1) получено

$$\log_2 \hat{S}(r) = -0.0227r^2 + 4.3045r - 31.182.$$

Для Simeck 64/128 получены значения коэффициентов уравнения регрессии (1): $c = 1.6061$, $b = -0.1848$, $a = 0.1061$, оно приняло вид

$$\log_2 \hat{S}(r) = 0.1061r^2 - 0.1848r + 1.6061.$$

Затем для прогнозных значений были построены доверительные интервалы по формуле

$$\log_2 \hat{N}(r) \pm t_{f,\alpha} s_{ei},$$

где s_{ei} — стандартное отклонение ошибки прогноза, а $t_{f,\alpha}$ — квантиль t-распределения Стьюдента при степенях свободы $f = n - m - 1$ и уровне значимости α. Так как в нашем случае $f = 7, \alpha = 0.95$, то $t_{f,\alpha} = 2.365$. В свою очередь,

$$s_{ei} = s_u^2 \left(1 + \frac{1}{n} + \frac{(x_i - \overline{x})^2}{\sum\limits_i (x_i - \overline{x})^2} \right),$$

где стандартная ошибка прогнозируемого показателя

$$s_u^2 = \frac{\sum (y_i - y_x)^2}{n - m - 1}.$$

Полученные прогнозные результаты для последующих раундов шифров Simeck 48/96 и Simeck 64/128 (зависимость размера подаваемой выборки от числа раундов, для которых атака различения проведена успешно) показаны в табл. 5. Чтобы атака была интересной для криптографического сообщества, время ее проведения должно быть меньше, чем время, затраченное на поиск ключа способом прямого перебора. Таким образом, рассматривались случаи, когда минимальная длина зашифрованной последовательности меньше длины 2^{key}. То есть нас интересовали случаи 2^{96} байта для шифра с 96-битным ключом и 2^{128} байта для шифра с 128-битным ключом.

Полученная путем экстраполяции минимальная длина выборки, при которой последовательность на выходе шифра Simeck 48/96 с полным числом раундов не является случайной, находится в интервале $2^{90.4}$—$2^{98.4}$ байта с вероятностью 0.95. Это означает, что шифр Simeck с 48-битным блоком и 96-битным ключом не является устойчивым к атаке различения.

Для шифра Simeck с 64-битным блоком и 128-битным ключом количество раундов, при котором тест нашел отклонения последовательности на выходе от случайной, равно 36. Это значение также близко к количеству полных раундов — 44.

В табл. 6 представлено полученное экспериментально максимальное число раундов, после которого зашифрованная выборка отличается от случайной, для других исследуемых в работе шифров. Здесь указано количество раундов, после которого анализируемая выборка оказалась неслучайной, в скобках дано полное число раундов шифра.

Т а б л и ц а 5. Оценочное число раундов и минимальная длина выборки, при которых возможна атака различения

Simeck 48/96						
R	19	20	21	34	35	36
S, байты	$2^{40.6} - 2^{44.2}$	$2^{43.9} - 2^{47.7}$	$2^{47.2} - 2^{51.2}$	$2^{85.2} - 2^{92.7}$	$2^{87.8} - 2^{95.5}$	$2^{90.4} - 2^{98.4}$

Simeck 64/128					
R	35	36	42	43	44
S, байты	$2^{122.3} - 2^{127.7}$	$2^{129.5} - 2^{135.1}$	$2^{177.3} - 2^{184.3}$	$2^{186.0} - 2^{193.2}$	$2^{195.0} - 2^{202.4}$

Т а б л и ц а 6. Число раундов и необходимая длина последовательности для анализа, после которых зашифрованная последовательность неслучайна

Шифр	Параметры шифра	Количество раундов	S, байты
Speck	32/64	5(22)	2^{27}
«	48/96	6(23)	$2^{33.5}$
«	64/128	6(27)	2^{31}
Simon	32/64	9(32)	2^{27}
«	48/96	12(36)	$2^{36.5}$
«	64/128	12(44)	2^{36}
Simeck	32/64	10(32)	2^{29}
«	48/96	18(36)	$2^{38.5}$
«	64/128	19(44)	2^{36}
HIGHT	64/128	10(32)	2^{32}
LEA	128/128	8(24)	2^{34}

Т а б л и ц а 7. Оценочное число раундов и минимальная длина выборки, при которых возможна атака различения

Шифр	Параметры шифра	Количество раундов
Speck	48/96	12(23)
«	64/128	13(27)
Simon	48/96	20(36)
Simeck	48/96	36(36)
«	64/128	36(44)
LEA	128/128	18(24)

Из табл. 6 видно, что число раундов, после которого зашифрованная выборка отличается от случайной для Simeck 48/96 и для Simeck 64/128, велико и составляет соответственно около 50 и 43 % от общего числа раундов. Для шифров Speck 48/96 и Speck 64/128 число таких раундов составляет примерно 25 и 20 %. Можно сделать вывод, что Speck гораздо более устойчив к атаке различения, чем Simeck.

Основываясь на полученных экспериментальных результатах, мы с помощью полиномов низкой степени минимальную длину последовательности, необходимую для успешной атаки различения, экстраполировали на последующие раунды для всех указанных выше шифров. Наиболее интересные результаты отражены в табл. 7. В скобках указано полное число раундов, заданное авторами шифров.

Выводы

В настоящей работе применена атака различения на легковесные блочные шифры Speck, Simon, Simeck, HIGHT и LEA. Экспериментальное исследование показало, что шифры Speck, Simon, HIGHT устойчивы к атаке различения, а семейства шифров Simeck нет. Количество раундов, после которого зашифрованная последовательность является неслучайной, достаточно велико, для шифра Simeck 48/96 оно составляет около 50 % от общего числа раундов, а для Simeck 64/128 — 43 %. Теоретические оценки на основе полученных данных показали, что длина, при которой последовательность на выходе шифра Simeck 48/96 с полным числом раундов (36) не является случайной, находится в интервале $2^{90.4} - 2^{98.4}$ байта с вероятностью 0.95. Это означает, что Simeck 48/96 не является устойчивым к атаке различения. Отметим, что на данный момент в литературе нет описания успешных атак на этот шифр с полным числом раундов. Исследование показывает, что для повышения надежности шифра Simeck 48/96 необходимо увеличить количество раундов.

Благодарности. Работа выполнена при финансовой поддержке РФФИ (грант № 18-29-03005).

Список литературы / References

[1] **Junod, P., Canteaut, A.** Advanced linear cryptanalysis of block and stream ciphers. Amsterdam: IOS Press, 2011. 144 p.

[2] **Beaulieu, R., Shors, D., Smith, J. et al.** The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive: Report 2013/404. Available at: `http://eprint.iacr.org/2013/404` (accessed 25.10.2017).

[3] **Yang, G., Zhu, B., Suder, V. et al.** The simeck family of lightweight block ciphers. Cryptology ePrint Archive: Report 2015/612. Available at: `https://eprint.iacr.org/2015/612` (accessed 25.10.2017).

[4] **Hong, D., Sung, J., Hong, S. et al.** HIGHT: A new block cipher suitable for low-resource device // Intern. Works. on Cryptographic Hardware and Embedded Systems. Berlin; Heidelberg: Springer, 2006. P. 46–59.

[5] **Hong, D., Lee, J.K., Kim, D.C. et al.** LEA: A 128-bit block cipher for fast encryption on common processors // Intern. Works. on Inform. Security Applications. Cham: Springer, 2013. P. 3–27.

[6] **Kunzli, S., Meier, W.** Distinguishing attack on MAG. Available at: `http://www.ecrypt.eu.org/stream/papersdir/053.pdf` (accessed 25.10.2017).

[7] **Dinur, I.** Improved differential cryptanalysis of round-reduced speck // Intern. Works. on Selected Areas in Cryptography. Cham: Springer, 2014. P. 147–164.

[8] **Qiao, K., Hu, L., Sun, S.** Differential analysis on simeck and simon with dynamic key-guessing techniques // Intern. Conf. on Inform. Syst. Security and Privacy. Cham: Springer, 2016. P. 64–85.

[9] **Qin, L., Chen, H., Wang, X.** Linear hull attack on round-reduced simeck with dynamic key-guessing techniques // Australasian Conf. on Inform. Security and Privacy. Cham: Springer, 2016. P. 409–424.

[10] **Doran, R.W.** The Gray Code // J. of Universal Comput. Science. 2007. Vol. 13, No. 11. P. 1573–1597.

[11] **Рябко Б.Я., Пестунов А.И.** "Стопка книг" как новый статистический тест для случайных чисел // Пробл. передачи информации. 2004. Т. 40, № 1. С. 73–78.
Ryabko, B.Ya., Pestunov, A.I. "Book Stack" as a new statistical test for random numbers // Probl. of Inform. Transmission. 2004. Vol. 40, No.1. P. 66–71.

[12] **Ryabko, B., Fionov, A.** Basics of contemporary cryptography for IT practitioners. USA: World Scientific, 2005. 207 p.

[13] **Ryabko, B., Monarev, V.** Using information theory approach to randomness testing // J. of Statistical Planning and Inference. 2005. Vol. 133, No. 1. P. 95–110.

[14] **Кендалл М. Дж., Стьюарт А.** Теория распределений. Т. 1. М.: Наука, 1966. 553 с.
Kendall, M.G., Stuart, A. The advanced theory of statistics. V. 1. Moscow: Nauka, 1966. 553 p. (In Russ.)

[15] **Doroshenko, S., Ryabko, B.** The experimental distinguishing attack on RC4. Cryptology ePrint Archive: Report 2006/070. Available at: `https://eprint.iacr.org/2006/070.pdf` (accessed 25.10.2017).

[16] **Lubkin, A., Ryabko, B.** The distinguishing attack on ZK-Crypt cipher. eSTREAM, ECRYPT Stream Cipher Project. Report 2005/076. Available at: `http://www.ecrypt.eu.org/stream/papersdir/076.pdf`

[17] **Фёрстер Э., Рёнц Б.** Методы корреляционного и регрессионного анализа: Руководство для экономистов. М.: Финансы и статистика, 1983. 302 с.
Förster, E., Rönz, B. Methoden der Korrelations und Regressionsanalyse: Ein Leitfaden für Ökonomen. Berlin: Verlag Die Wirtschaft, 2009. 144 p.

Поступила в редакцию 11 мая 2018 г.,
с доработки — 24 октября 2018 г.

The distinguishing attack on ARX-based lightweight block ciphers

Soskov, Alexander S.[1,*], Ryabko, Boris Ya.[1,2]

[1]Institute of Computational Technologies SB RAS, Novosibirsk, 630090, Russia
[2]Novosibirsk State University, Novosibirsk, 630090, Russia

[*]Corresponding author: Soskov, Alexander S., e-mail: sashasasha-1987@mail.ru

The distinguishing attack on modern lightweight ARX-based block ciphers was applied. Distinguishing attack is any form of cryptanalysis on data encrypted by a cipher that allows an attacker distinguishing the encrypted data from random data.

Purpose. Modern symmetric-key ciphers must be designed to be immune to such an attack. The purpose of the work was to estimate the resistance of lightweight ciphers Speck, Simon, Simeck, HIGHT, and LEA to a distinguishing attack.

Methodology. We note that these ciphers are iterated block ciphers. It is means that they transform blocks of plain text into blocks of cipher text by using the cyclically repeated invertible function known as the round function where each iteration is to be referred as a round. We have experimentally found a maximum number of rounds where encrypted data looked like random bit-sequence by using statistical test "Book Stack". Then we extrapolated the theoretical length required for a successful distinguishing attack on cipher with full-number rounds by a polynomial of a low degree. Note that cryptography attack is considered as successful if the length of the encrypted sequence is less than the length 2^K (K — key size).

Originality/value. Our experiments and estimations show, that Simeck with 48-bit block size and 96-bit key size is not immune to distinguishing attack. We recommended increasing the number of rounds by 15–20 % in order to improve the reliability of the Simeck 48/96.

Keywords: distinguishing attack, lightweight block cipher, ARX-based cipher, Speck, Simon, Simeck, HIGHT, LEA.

Cite: Soskov, A.S., Ryabko, B.Ya. The distinguishing attack on ARX-based lightweight block ciphers // Computational Technologies. 2019. Vol. 24, No. 3. P. 106–116. (In Russ.) DOI: 10.25743/ICT.2019.24.3.008.

Acknowledgements. This research was partly supported by RFBR (grant No. 18-29-03005).

Received May 11, 2018
Received in revised form October 24, 2018