блочных шифров, обеспечивающего сложную нелинейную зависимость битов раундовых ключей от битов основного ключа.

ЛИТЕРАТУРА

1. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: Юрайт, 2016. 209 с.
2. *Fomichev V. M. and Koreneva, A. M.* Mixing properties of Modified Additive Generators // J. Appl. Indust. Math. 2017. V. 11. No. 2. P. 215–226.
3. *Фомичёв В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.
4. МР 26.2.003-2013 «Информационная технология. Криптографическая защита информации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89». М.: ТК 26, 2013.

УДК 519.1 DOI 10.17223/2226308X/11/21

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕКОТОРЫХ «ЛЕГКОВЕСНЫХ» АЛГОРИТМОВ

К. В. Максимов, И. И. Хайруллин

Систематизированы подходы к построению блочных алгоритмов «легковесной» криптографии, изучены некоторые «легковесные» алгоритмы на основе сетей Фейстеля и SP-сетей и оценены их перемешивающие и нелинейные свойства. Определены понятия показателя сильной нелинейности (наименьшее число раундов, при котором каждая координатная функция выходного блока является нелинейной) и показателя совершенности (наименьшее число раундов, при котором каждый бит выходного блока существенно зависит от всех битов входного блока). Для алгоритмов PRESENT, MIDORI, SKINNY, CLEFIA и LILLIPUT получены точные значения экспонентов матриц существенной зависимости, построенных для раундовых функций (соответственно 3, 3, 6, 5, 5), оценки показателей совершенности (4, 3, 6, 5, 5) и показателей сильной нелинейности (1, 1, 1, 2, 2). Экспериментально установлено, что на протяжении 500 раундов каждая координатная функция выходного блока является нелинейной.

Ключевые слова: *«легковесная» криптография, сеть Фейстеля, SP-сеть, матрица существенной зависимости, экспонент матрицы, показатель сильной нелинейности, показатель совершенности.*

Введение

Основные направления развития криптографии во многом связаны с развитием средств связи, информационных технологий и вычислительной техники. Именно прогресс в этих областях сделал возможным повсеместное использование компактных устройств с малой вычислительной мощностью, имеющих доступ к сети Интернет и реализующих концепцию «Интернета вещей». Примерами таких устройств могут служить радиочастотные метки (RFID), средства автоматизированных систем управления технологическими процессами (SCADA), беспроводные сенсоры, электронные средства идентификации личности [1].

Жёсткие ограничения на внутренние вычислительные ресурсы таких устройств делают затруднительным или невозможным использование классических криптографических алгоритмов. Это привело к возникновению нового раздела криптографии — «легковесной» криптографии (lightweight cryptography), задачей которой является создание стойких криптографических алгоритмов и протоколов с приемлемой стойкостью в условиях ограниченных ресурсов [1].

Актуальной задачей является оптимизация параметров «легковесных» алгоритмов блочного шифрования. В работе систематизированы основные подходы к построению существующих «легковесных» алгоритмов и оценены следующие характеристики некоторых алгоритмов:

— нелинейность всех координатных функций раундового преобразования;
— перемешивающие свойства раундового преобразования;
— устойчивость признака нелинейности преобразования.

Для оценки нелинейности алгоритмов блочного шифрования введено понятие *показателя сильной нелинейности* (exponent of strong non-linearity) — это наименьшее число раундов, при котором все координатные булевы функции раундового преобразования являются нелинейными.

1. Объекты исследования

При построении «легковесных» блочных алгоритмов шифрования применяются следующие архитектурные решения, отличающие их от классических блочных шифров [1]:

— уменьшение размеров основных параметров алгоритма, например размера блока до 64 бит со 128 бит, использование ключей длины 64, 80 и 128 бит;
— использование упрощённого ключевого расписания;
— проектирование алгоритмов на основе хорошо изученных и широко применяемых операций, осуществляющих элементарные линейные/нелинейные преобразования;
— уменьшение размеров данных, используемых в конкретных операциях, например отказ от 8-битовых s-боксов в пользу 4-битовых;
— использование необременительных с точки зрения ресурсоёмкости, но эффективных преобразований (битовые перестановки, сдвиговые регистры и пр.).

На сегодняшний день известно достаточно большое количество «легковесных» блочных алгоритмов шифрования и на основе SP-сетей, и на основе сетей Фейстеля [1]. Оба подхода имеют свои преимущества и недостатки в контексте построения алгоритмов в условиях ограниченных ресурсов.

С целью оценки возможностей оптимизации параметров и поиска новых синтезных решений были исследованы алгоритмы PRESENT [2] и CLEFIA [3], включенные в 2012 г. в международный стандарт «легковесного» шифрования ISO/IEC 291922: 2012, а также ряд новых алгоритмов, представленных в 2015–2016 гг.: LILLIPUT [4], MIDORI [5] и SKINNY [6].

2. Экспериментальное исследование криптографических свойств

Показатель сильной нелинейности итеративного блочного алгоритма шифрования определим через минимальное число раундов, необходимое для того, чтобы каждая координатная функция выходного блока являлась нелинейной. Была проведена экспериментальная оценка показателя сильной нелинейности.

Если преобразование является нелинейным [7], то существуют $x, x', a \in V_n, a \neq 0$, такие, что

$$f(x) + f(x+a) \neq f(x') + f(x'+a). \tag{1}$$

В ходе эксперимента для случайно выбранной тройки x, x', a шифруются векторы $x, x', x+a, x'+a$ при некотором значении числа раундов шифрования. Если найдётся тройка, при которой каждая координатная функция удовлетворяет (1), то показатель сильной нелинейности не превосходит текущего числа раундов шифрования.

Заметим, что суперпозиция нелинейных функций может дать систему, содержащую линейные уравнения. Например, рассмотрим следущую систему:

$$\begin{cases} f_1(x,y) = x \oplus y \oplus xy, \\ f_2(x,y) = x \oplus xy. \end{cases}$$

Выполнив подстановку функций f_1, f_2 вместо аргументов x, y, получим

$$\begin{cases} f_1(f_1(x,y), f_2(x,y)) = x \oplus y \oplus xy, \\ f_2(f_1(x,y), f_2(x,y)) = y. \end{cases}$$

Экспериментально проверено, что для всех рассмотренных алгоритмов нелинейность координатных функций выходного блока сохраняется в течение 500 раундов. Это свойство является важным, поскольку легковесные алгоритмы используются при построении ключевого расписания или хеш-функций, например DM-PRESENT [8].

Для оценки перемешивающих свойств применён матрично-графовый подход [9], при котором существенная зависимость координат выходных векторов от координат входных векторов кодируется перемешивающей матрицей порядка n: элемент матрицы m_{ij} равен 1, где $i, j \in \{1, \ldots, n\}$, если имеется существенная зависимость j-й координатной функции выхода от i-й координаты входа, и 0 — в противном случае. Матрица называется перемешивающей матрицей или матрицей существенной зависимости (МСЗ). Для итеративных преобразований оценка перемешивающих свойств состоит в изучении примитивности МСЗ и определении их экспонентов. Матрица примитивная, если некоторая её степень не содержит нулевых элементов. Наименьшая из таких степеней называется экспонентом матрицы.

Проведено экспериментальное исследование перемешивающих свойств алгоритмов PRESENT, CLEFIA, LILLIPUT, MIDORI, SKINNY. Для них получены значения экспонентов перемешивающих матриц, построенных для раундовых функций. С помощью специального ПО осуществлено последовательное возведение МСЗ в степень и получены значения их экспонентов.

Перемешивающие свойства были оценены также экспериментальным способом, то есть получена оценка сверху показателя совершенности, который равен наименьшему числу раундов, при котором каждая координатная функция существенно зависит от каждой входной координаты. В ходе эксперимента для каждой входной координаты были выбраны 20 пар соседних по ней случайных векторов (x_1, x'_1), $\ldots$,(x_{20}, x'_{20}). Выбранные векторы шифруются при некотором значении числа раундов шифрования. Если выполняется условие $(f(x_1) \oplus f(x'_1)) \vee \ldots \vee (f(x_{20}) \oplus f(x'_{20})) = \mathbf{e}$, где $\mathbf{e}$ — вектор из единиц соответствующей длины, то показатель совершенности не превосходит текущего числа раундов. Результаты приведены в таблице.

Алгоритм	Число раундов	Размер МСЗ	Экспонент МСЗ	Показатель совершенности	Показатель сильной нелинейности
PRESENT	32	64×64	3	4	1
MIDORI	16, 20	64×64	3	3	1
SKINNY	32, 36, 40, 48, 56	64×64	6	6	1
CLEFIA	36, 44, 52	128×128	5	5	2
LILLIPUT	30	64×64	5	5	2

Выводы

Дан краткий обзор современных подходов к разработке «легковесных» алгоритмов блочного шифрования. Экспериментально определены показатели сильной нелинейности раундовых преобразований выбранных алгоритмов шифрования, показатели совершенности и экспоненты матриц существенной зависимости. Полученные значения существенно меньше числа раундов шифрования, что указывает на потенциал для возможной оптимизации алгоритмов путём сокращения числа раундов шифрования. Экспериментально проверено, что во всех рассмотренных алгоритмах нелинейность каждой координатной функции выходного блока сохраняется в течение большого числа раундов шифрования (500), что указывает на возможность использования этих алгоритмов при построении ключевого расписания и хеш-функций.

Авторы благодарят В. М. Фомичева и А. М. Кореневу за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Жуков А. Е.* Легковесная криптография. Ч. 1 // Вопросы кибербезопасности. 2015. № 1. С. 26–43.
2. *Bogdanov A., Knudsen L., Leander G., et al.* PRESENT: An ultra-lightweight block cipher // CHES 2007. LNCS. 2007. V. 4727. P. 450–466.
3. *Shirai T., Shibutani T., Akishita K., et al.* The 128-bit blockcipher CLEFIA // FSE 2007. LNCS. 2007. V. 4593. P. 181–195.
4. *Thierry P., Julien F., Marine M., and Gaël T.* Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput // IEEE Trans. Computers. 2015. V. 65. Iss. 7. P. 99.
5. *Banik S., Bogdanov A., Isobe T., et al.* Midori: a block cipher for low energy // ASIACRYPT 2015. LNCS. 2015. V. 9453. P. 411–436.
6. *Beierle C., Jean J., Kolbl S., et al.* The SKINNY family of block ciphers and its low-latency variant MANTIS // CRYPTO 2016. LNCS. 2016. V. 9815. P. 123–153.
7. *Фомичев В. М.* Методы дискретной математики в криптологии: учеб. пособие. М.:Диалог-МИФИ, 2010.
8. *Poschmann A.* Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. Ph.D. Thesis. Ruhr University Bochum, 2009.
9. *Коренева А. М., Мартышин В. Н.* Экспериментальное исследование экспонентов раундовых перемешивающих матриц обобщённых сетей Фейстеля // Прикладная дискретная математика. Приложение. 2016. № 9. С.48–51.