УДК 681.3.06

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА УМЕНЬШЕННОЙ ВЕРСИИ ШИФРА «КАЛИНА»

В.И. ДОЛГОВ, Р.В. ОЛЕЙНИКОВ, А.Ю. БОЛЬШАКОВ, А.В. ГРИГОРЬЕВ, Е.В. ДРОБАТЬКО

В первой части роботы приводится описание уменьшенной 16-битной версии шифра ″Калина″, а во второй – результаты исследования ряда криптографических показателей уменьшенной модели (циклические, дифференциальные, линейные и др. свойства).

Ключевые слова: симметричный блочный шифр, случайная перестановка.

ВВЕДЕНИЕ

В настоящее время в Украине проходит открытый конкурс по выдвижению и отбору кандидатов на национальный стандарт блочного симметричного шифрования. Одним из алгоритмов, представленных на данный конкурс, является алгоритм блочного симметричного шифрования ″Калина″.

На текущем этапе конкурса проходит изучение предложений экспертами и специалистами, а также ведется работа по проверке заявленных показателей стойкости и производительности.

Всесторонний анализ криптографических алгоритмов требует больших вычислительных мощностей, а некоторые его аспекты вообще неосуществимы на данный момент.

В широком спектре стоящих задач большое значение приобретает развитие и применение технологий, позволяющих ускорить процессы исследования и принятия решений. Одним из таких путей, направленных на создание и отработку эффективных методов сопоставления различных предложений, может стать, на наш взгляд, анализ криптографических показателей уменьшенных версий (моделей) шифров, в которых сохранены все принципиальные преобразования основного (большого) шифра. Естественно, здесь сразу возникает вопрос об адекватности перехода к версиям малых шифров (в смысле сохранения в модели всех свойств прототипа). Однако здесь можно положиться на достаточно очевидный принцип (назовем его постулатом): если хороши свойства модели, то свойства прототипа как минимум будут не хуже. Когда прототип поддается масштабируемости, то есть удается в модели сохранить структуру преобразований блоков данных и свойства основных операций, то результаты анализа свойств модели при определенных условиях, могут быть перенесены на прототип.

В этой работе предлагается уменьшенная модель шифра ″Калина″ [1] и изучаются ее ряд криптографических показателей.

При изложении материала мы в значительной степени будем опираться на описание шифров mini-AES [2] и большого шифра ″Калина″ [1].

1. ОПИСАНИЕ ШИФРА МИНИ-КАЛИНА

Алгоритм шифрования мини-Калина повторяет принципиальные решения, использованные при построении основной версии предложения [1], и практически является результатом масштабирования оригинальной разработки к размеру входного блока и ключа равному 16 битам. Как и в большом шифре, каждый 16-битный блок входных данных обрабатывается независимо от остальных. В процессе расшифрования используется тот же ключ, что и при шифровании. Шифртекст составляется из шифрованных блоков, последовательность которых соответствует очередности блоков открытого текста.

Нами были рассмотрены варианты построения алгоритма с десятью (как в оригинальной версии алгоритма) и с четырьмя циклами (для сравнения результатов с другими известными шестнадцати битными версиями БСШ [3,4]).

Рис. 1, заимствованный из описания mini-AES [2], иллюстрирует процесс шифрования сообщения с помощью нашей модели.

1.1. Компоненты шифра мини-Калина

Алгоритм ″Калина″ относится к Rijndael-подобным шифрам (как и AES, ADE), и поэтому для его описания удобно будет воспользоваться концепцией описания и терминологией, представленными в спецификации шифра mini-AES [2].

Для простоты описания процедуры шифрования входной 16-битный блок открытого текста P, состоящий из последовательности четырёх полубайтов $P=(p_0,p_1,p_2,p_3)$, представляется в виде матрицы размера 2×2, названной в соответствии с терминологией, использованной при описании шифра AES (и ADE), состоянием. Отмеченное представление иллюстрирует рис. 2.

Для представления полубайтов наряду с двоичной формой в дальнейшем будет использоваться и шестнадцатеричная форма представления, приведенная в табл. 1.

Итак, входной блок данных $p_0p_1p_2p_3$ представляется в виде матрицы-состояния $\begin{bmatrix} p_0 & p_2 \\ p_1 & p_3 \end{bmatrix}$.

Например, если входной блок 1000 1100 0111 0001 состоит из полубайтов $p_0=8$, $p_1=C$, $p_2=7$, $p_3=1$, то соответствующая матрица состояния будет иметь вид

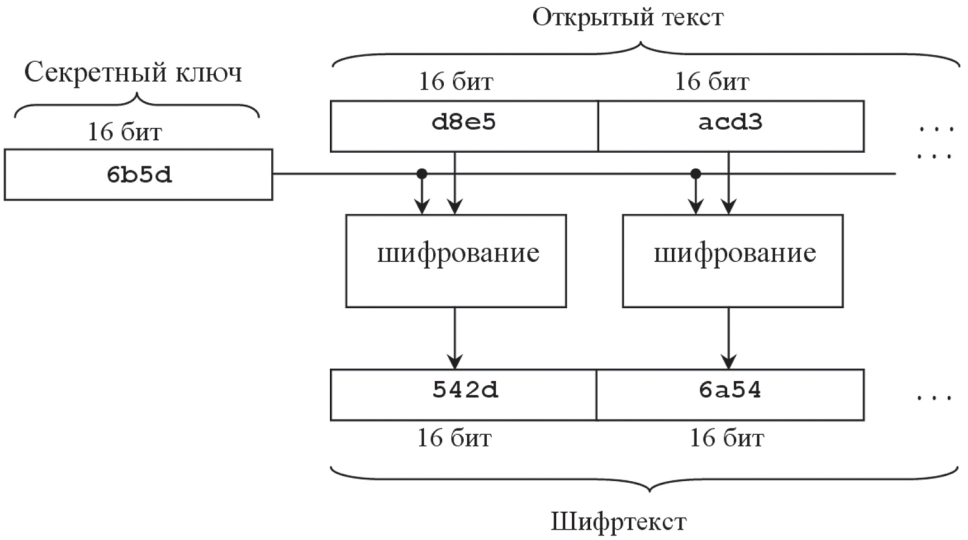


Рис. 1. Шифрование открытого сообщения БСШ с размером блока 16 бит

$$\begin{bmatrix} 8 & 7 \\ C & 1 \end{bmatrix}, \text{ или } \begin{bmatrix} 1000 & 0111 \\ 1100 & 0001 \end{bmatrix}.$$

Подобным же образом представляется и секретный ключ – как 4 полубайта $k_0k_1k_2k_3$ и соответствующее им состояние $\begin{bmatrix} k_0 & k_2 \\ k_1 & k_3 \end{bmatrix}$.

В процессе шифрования принимают участие пять основных компонент, а именно: операции *XORRoundKey, AddRoundKey, Sbox, ShiftRows* и *MixColumns,* многократное применение которых в определённом порядке и определяет процедуру шифрования. Еще одной важной частью шифра является алгоритм разворачивания ключа.

Цикл шифрования включает последовательное выполнение следующих преобразований:

– подстановка (Sbox);

– циклический сдвиг строк (ShiftRows);

– перемешивание в колонках (MixColumns);

– сложение с подключом по модулю 2^4 (AddRoundKey), если номер цикла четный и по модулю 2 (XORRoundKey), если номер цикла нечетный.

Перед повторением этих циклов производится сложение по модулю 2 с нулевым элементом массива подключей, а после цикловых преобразований – ещё одна подстановка (S-блок) и сложение по модулю 2^4 с последним элементом массива подключей. Количество циклов в оригинальной разработке равняется десяти, хотя в большинстве уменьшенных версий шифров оно равно четырём. Изменение этого параметра не составляет труда, поэтому в дальнейшем мы рассматриваем оба варианта реализации.

1.1.1. Сложение с ключом

Функции AddRoundKey и XORRoundKey достаточно просты, и полностью аналогичны тем, что использованы в оригинальной версии шифра.

1.1.2. Таблицы подстановок (Sbox)

В уменьшенной версии шифра Калина используются подстановки 16-го порядка. Они взяты из работы [3]:

10	12	9	7		10	2	0	6
13	4	1	2		15	1	12	4
1	6	11	8		14	11	7	13
3	14	0	15		9	5	3	8

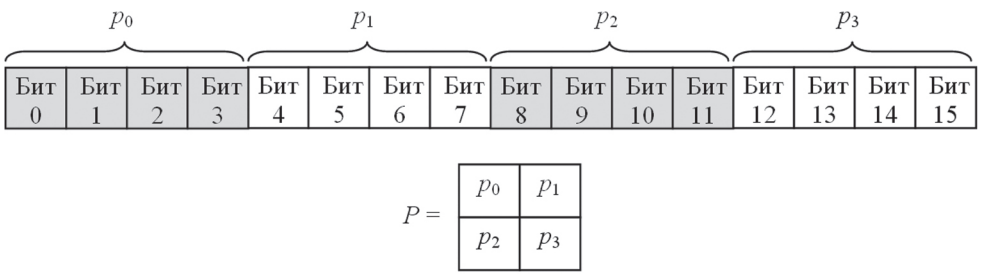


Рис. 2. Представление 16-битного блока в виде матрицы 2×2

Таблица 1

Представление 4-битных массивов в шестнадцатеричном виде

p-дв.	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
p-шестн.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Текущее состояние, как и в других функциях, представляется в виде массива полубайт размера 2×2.

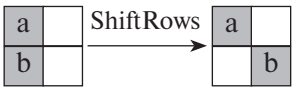
К первой строке массива применяется одна подстановка, ко второй – вторая.

Подстановка определяется как замена полубайта состояния на полубайт из таблицы, такой, что номер его столбца определяется двумя младшими, а строки – двумя старшими битами полубайта состояния. Достаточно очевидно, что если развернуть массив 4×4 по строкам в одномерный массив из шестнадцати полубайт, то подстановка определяется значительно проще: полубайт берётся просто по номеру в строке.

1.1.3. Циклический сдвиг строк (ShiftRows)

Ввиду того, что текущее состояние представлено в виде матрицы размером 2×2 полубайта, эта функция сильно вырождается относительно аналогичной в большом шифре.

Собственно при этом происходит только циклический сдвиг 2-й строки:



Из этого следует, что функция ShiftRows для уменьшенной версии будет обратной к самой себе, и создание отдельной функции invShiftRows не требуется.

1.1.4. Перемешивание в колонках (MixColumns)

Выполнение данной процедуры сводится к умножению матричного представления текущего состояния на константную матрицу над полем GF(2^4). В качестве константной использована матрица

10	7
7	15

Поле GF(2^4) задается полиномом $x^4 + x + 1$.

1.2. Инверсный шифр

Процедура расшифрования является обратной к процедуре зашифрования. Её код достаточно очевиден и пояснений не требует.

Функции XORRoundKey и ShiftRows являются инверсными в отношении самих себя, поэтому используются и при расшифровании.

Функции InvSbox и InvMixColumns аналогичны прямым, но используют другие встроенные данные, а именно:

S-блоки:

2	5	1	14		14	8	7	12
7	13	3	10		6	5	9	3
15	12	0	9		11	2	0	10
6	11	8	4		2	4	13	15

и матрицу:

3	5
5	2

Функция SubRoundKey, отличается от AddRoundKey знаком (выполняется модульное вычитание).

Последовательность применения данных функций представляет собой последовательность функций зашифрования, развёрнутую в обратном порядке с заменой функций зашифрования на обратные им (такой шифр называется инволютивным).

1.3. Схема разворачивания ключей

Для получения цикловых подключей из исходного мастер-ключа используется процедура разворачивания ключей. Для шифрования алгоритмом «мини-калина» необходимо 12 подключей, каждый длиной 4×4 бита (размер подключа совпадает с размером открытого/шифрованого текста и текущего состояния шифра).

Алгоритм разворачивания ключа работает по схеме, которая включает в себя два этапа:

1) На основе мастер-ключа и константы вырабатывается три ключевых состояния KS_{len}^{j}, где j – порядковый номер ключевого состояния, len – длина ключевого состояния в битах.

При этом константа складывается с мастер-ключом по модулю 2, а потом проходит два цикла шифрования (в первом она шифруется побитовой инверсией мастер-ключа, во второй – собственно мастер-ключом).

Для каждого ключевого состояния берётся своя константа.

Константы имеют вид:

$c_1 = \{1,1,1,1\}$;

$c_2 = \{2,2,2,1\}$;

$c_3 = \{3,3,3,1\}$;

2) на основе каждого из трёх KS_{len}^{j} с помощью циклических сдвигов вправо формируются цикловые подключи K_i.

Таблица 2 иллюстрирует процесс формирования цикловых подключей с помощью циклических сдвигов.

Таблица 2

Формирование подключей на основе циклических сдвигов

1	0	0	1	0	1	1	1	0	1	0	0	1	1	0	1	KS_{len}^{j}
0	1	1	0	1	1	0	0	1	0	1	1	1	0	1	0	>>5
1	0	0	1	1	0	1	1	0	0	1	0	1	1	1	0	>>7
1	1	1	0	1	0	0	1	1	0	1	1	0	0	1	0	>>11

Таким образом, мы получаем массив из шестнадцати цикловых подключей.

2. ИССЛЕДОВАНИЯ ЦИКЛИЧЕСКИХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

При исследовании циклических свойств использована методика, изложенная в работе [6].

Если рассматривать шифр при заданном ключе как подстановку, определяющую переход от

исходного блока данных к зашифрованному (биективное отображение), то циклические свойства можно определить на основе результатов анализа последовательных зашифрований исходного текста на каждом ключе.

Здесь определяется закон распределения числа циклов для множества ключей зашифрования (подстановочных преобразований). Известно, что для случайных подстановок справедлива теорема [8].

Теорема. Если ξ_n – *число циклов равновероятно выбранной подстановки степени n, то случайная величина* $\xi_n' = \frac{\xi_n - \ln n}{\sqrt{\ln n}}$ *имеет в пределе нормальное распределение с параметрами* (0,1).

Мы сначала и поставили задачу оценки соответствия (близости) закона распределения числа циклов для множества ключей зашифрования шифра мини-Калина асимптотическому распределению.

2.1. Особенности программной реализации

Алгоритм работы программы такой: для каждого ключа из полного множества ключей мы производим поиск циклов и запоминаем получившееся их число. Поиск циклов производится так: мы создаём массив всех возможных вариантов пар исходный текст/зашифрованный текст и, начиная с нулевого элемента массива из заготовленных открытых тестов, применяем функцию шифрования, пока не обнаружим цикл (пока не придем снова к нулю). Таким образом, мы нашли цикл с нулевым образующим элементом, и в процессе пометили все элементы в него входящие. После этого мы выбираем наименьший элемент, не попавший в этот цикл, и строим новый цикл от него, также запоминая пройденные значения. Это мы повторяем до тех пор, пока все элементы массива исходных/зашифрованных текстов не попадут в один из циклов.

2.2. Результаты исследований циклических свойств и их анализ

Результат работы данной программы представляет собой файл достаточно большого размера, поэтому в табл. 3 представлена только его финальная часть. В таблице показаны также взятые из работ [3,4] результаты исследований уменьшенных моделей других шифров. Рассмотрены две версии уменьшенной модели шифра Калина: десятицикловый алгоритм (как в оригинальной версии) и четырёхцикловый (для сравнения с другими известными моделями). Из приведенных данных можно сделать вывод о том, что миниверсия шифра "Калина" практически повторяет циклические свойства других известных моделей шифров и, в частности, совпадает со свойствами шифра mini-AES. Соответственно процедуру шифрования данного шифра можно считать близкой к свойствам случайной подстановки. Из сравнения показателей десяти и четырехцикловой версий шифра видно, что появление ключа, порождающего 28 циклов, скорее является фактором случайности чем несовершенства алгоритма или реализации.

3. ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

В процессе исследований были изучены также дифференциальные свойства подстановочных преобразований, формируемых мини шифром Калина. Некоторые результаты в этом направлении иллюстрирует табл. 4 (расчеты для шифра мини "Калина" выполнены по выборке из 10 ключей). В этой же таблице для сравнения представлены результаты изучения дифференциальных свойств малых версий блочных шифров Baby ADE и Mini AES, взятые из нашей работы [6] (данные получены по 1000-е ключам зашифрования).

Таблица 3

Сравнение циклических свойств уменьшенных моделей БСШ

Количество циклов	Количество подстановок Baby-Camellia	Количество подстановок Baby-Rijndael	Количество подстановок babyADE	Количество подстановок mini-Kalina (4 цикла)	Количество подстановок mini-Kalina (10 циклов)
2	28	18	32	2	27
4	496	499	521	549	507
6	3147	3255	3322	3167	3234
8	9373	9436	9415	9528	9482
10	15567	15429	15366	15256	15317
12	15903	15963	16124	15988	16054
14	11530	11580	11400	11760	11524
16	6168	5956	5952	5935	6052
18	2406	2411	2397	2384	2407
20	713	774	778	733	706
22	160	174	188	166	186
24	36	35	34	39	34
26	9	6	5	7	5
28	0	0	1	0	1
30	0	0	1	0	0

Таблица 4

Дифференциальные свойства мини шифра «Калина» при различном числе циклов шифрования

Шифр	Число циклов *r*						
	2	3	4	5	6	7	8
Baby ADE	3254±59	301,3±7,3	20,064±0,35	19,170±0,124	19,120±0,092	19,166±0,093	19,106±0,091
Mini AES	4955±24	640,6±4,6	43,066±0,99	20,538±0,202	19,082±0,093	19,122±0,092	19,122±0,096
Mini Калина	301±70	36,6±11,3	19,06 ±1	18,6±0,81	19,06±1,075	20±0,1	19,0±1

И в этом случае шифр рассматривается для каждого ключа зашифрования как подстановка порядка 2^{16} и таблица XOR разностей фактически представляет собой таблицу распределения полных дифференциалов шифра. Результаты свидетельствуют, что шифр ″Калина″ имеет показатели, не уступающие другим алгоритмам шифрования, представленным на Украинский конкурс.

Считаем важным также отметить, что полученные для малых моделей шифров (с числом циклов большим четырех) максимальные значения полных дифференциалов совпадают с ожидаемыми средними значениями максимумов таблиц XOR разностей случайных подстановок соответствующего порядка.

4. ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

При исследовании линейных свойств мини версии шифра ″Калина″ была построена таблица линейных аппроксимаций размером $2^m \times 2^m$ для всего шифра, рассматриваемого как подстановка.

По принятой терминологии в этом случае значения такой таблицы называются линейным корпусом [7]. Полученные результаты вместе с данными аналогичного исследования, выполненного для шифра Лабиринт, представлены в табл. 3.

Следует здесь заметить, что объём вычислений при построении линейной аппроксимационной таблицы оказывается существенно большим, чем при определении максимума полного дифференциала. Он связан с битовым размером входа в шифр n как 2^{2n}, и выполнение полного объема расчетов даже для одного ключа и для 16-битных блоков данных оказывается вычислительно трудной задачей. Поэтому в табл. 5 иллюстрируются результаты вычислений для ограниченных наборов масок входа и выхода. В последнем случае объем выборки взят более, существенно меньшим, чем для первого шифра.

ЗАКЛЮЧЕНИЕ

Представленные результаты свидетельствуют, что шифр ″Калина″ обладает криптографическими показателями (из числа проверенных) не уступающими шифру Rijndael и другим шифрам, представленным на украинский конкурс по выбору кандидата на национальный стандарт симметричного блочного шифра.

Литература.

[1] *Горбенко І. Д, Долгов В.І., Олейніков Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцкій О.С., Казьміна С.В.* Перспективний блоковий симетричний шифр “Калина” – основні положення та специфікації // Прикладна радіоелектроніка: наук.-техн. журнал. – 2007. Т.6. № 2. – С. 195-208.

[2] Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Tested for Cryptanalysis Students, Cryptologia, XXVI (4), 2002.

[3] *Долгов В.И., Кузнецов А.А., Сергеенко Р.В., Белоковаленко А.Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-Ade) // Прикладная радиоэлектроника: научн.-техн. журнал. – 2008. Т. 7. № 3. – С. 215-224.

[4] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра «Лабиринт». Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. Т. 8. № 3. – С. 283-289.

[5] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Т.6, № 2. – С. 257-263.

[6] *Олейников Р.В., Лисицкая И.В., Широков А.В., Лисицкий К.Е.* Исследование дифференциальных свойств подстановок. Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. I, С. 59-63.

[7] *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p. 189-221.

[8] *Сачков В.Н.* Комбинаторные методы дискретной математики. – М.: Наука ,1977. – 319 с.

Поступила в редколлегию 7.07.2010.

Таблица 5

Линейные свойства шифров ″Лабиринт″ и ″Калина″

смещение	0	2	100	200	300	400	500	600	720
Линейный корпус шифра ″Лабиринт″									
количество	81839	163317	120328	48060	10378	1232	82	1	1
Линейный корпус шифра ″Калина″									
количество	29282	28825	21332	8522	1879	225	15	1	0

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

Большаков Андрей Юрьевич, студент кафедры БИТ ХНУРЭ. Область научных интересов: анализ БСШ, статистические методы исследования стойкости.

Григорьев Андрей Владимирович, студент кафедры БИТ ХНУРЭ. Область научных интересов: анализ криптографических свойств блочных симметричных и потоковых шифров, и их схем разворачивания ключей.

Дроботько Екатерина Викторовна, магистр кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров, анализ структурных элементов БСШ.

УДК 681.3.06

Криптографічні властивості зменшеної версії шифра «Калина» / В.І. Долгов, Р.В. Олійников, А.Ю. Большаков, А.В. Григорьєв, Е.В. Дроботько // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 349-354.

У роботі наведений опис зменшеної 16-бітової версії шифру «Калина» і результати дослідження декількох криптографічних показників зменшеної моделі (циклічні, диференційні, лінійні та інші властивості).

Ключові слова: симетричний блоковий шифр, випадкова перестановка.

Табл. 04. Іл.02. Бібліогр.: 08 найм.

UDC 681.3.06

Cryptographic properties of reduced version of «Kalina» cipher / V.I. Dolgov, R.V. Oleinikov, A.Yu. Bolshakov, A.V. Grigor'iev, E.V. Drobotko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 349-354.

The first part of the paper provides a description of the reduced cipher «Kalina» 16-bit version and the second one gives the results of researching a number of cryptographic indices of the reduced model (cyclic, differential, linear and other properties).

Key words: symmetric block cipher, random substitution.

Tab. 04. Fig. 02. Ref.: 08 items.