УДК 681.3.06

В. И. Долгов, д-р техн. наук
Харьковский национальный университет радиоэлектроники
(Украина, 61166, Харьков, пр. Ленина, 14,
тел. (057) 3408460, E-mail: dolgovvi@mail.ru),
А. А. Кузнецов, д-р техн. наук, **С. А. Исаев**, аспирант
Харьковский национальный университет им. В. Н. Каразина
(Украина, 61077, Харьков, пл. Свободы, 4,
E-mail: kuznetsov_alex@rambler.ru)

Дифференциальные свойства блочных симметричных шифров

Предложен новый подход в теории и методах криптоанализа, основанный на использовании результатов анализа уменьшенных моделей больших шифров при определении показателей стойкости. Рассмотрены особенности построения уменьшенных моделей шифров, представленных на открытый конкурс по отбору кандидатов на национальный стандарт блочного симметричного шифрования Украины. Приведены результаты анализа дифференциальных свойств уменьшенных моделей, связанные с ожидаемыми показателями стойкости прототипов.

Запропоновано новий підхід в теорії та методах криптоаналізу, базований на використанні результатів аналізу зменшених моделей великих шифрів при визначенні показників стійкості. Розглянуто особливості побудови зменшених моделей шифрів, представлених на відкритий конкурс з відбору кандидатів на національний стандарт блокового симетричного шифрування України. Наведено результати аналізу диференціальних властивостей зменшених моделей, які пов'язані з очікуваними показниками стійкості прототипів.

Ключевые слова: блочный симметричный шифр, уменьшенная модель, значение максимума полного дифференциала, доказуемая стойкость.

Блочные симметричные шифры (БСШ), представленные на открытый конкурс в Украине. В настоящее время Украина не имеет БСШ собственной разработки. Действующим стандартом в Украине является ГОСТ 28147-89, разработанный в Советском Союзе. Однако этот стандарт, учитывая последние достижения современной криптографии, уже не является достаточно надежным. Страны-лидеры освоения современных информационных технологий приступили к замене действующих стандартов шифрования новыми. Международные конкурсы, проведенные в последние десятилетия — AES (Advanced Encryption Standard, США), NESSIE и

CRYPTREC — свидетельствуют об актуальности дальнейшего развития технологий БСШ.

Такой же путь наметился и в Украине. В 2006 г. в Украине был объявлен конкурс по выдвижению кандидатов на национальный стандарт БСШ. В конкурсе участвовало пять предложений, из которых к окончательному рассмотрению представлено четыре (шифры ADE (Algorithm of Dynamic Encryption), «Калина», «Мухомор» и «Лабиринт»). В отборе приняли участие ученые и разработчики шифров АОИИТ, Калина, Мухомор.

Материалы подобных конкурсов стали основой и ориентиром для украинской криптографической школы и повлияли на формирование условий проведения конкурса в Украине. К экспертизе заявленных предложений был привлечен коллектив украинских ученых и разработчиков. Для рассмотрения им было представлено пять проектов, а шестым претендентом был победитель конкурса AES — шифр Rijndael. Предпочтение сначала было отдано шифру Калина, однако на окончательное решение повлиял тот факт, что шифр Калина оказался подобен по построению шифру Rijndael. Динамическое управление состояниями цикловой функции с помощью ключевых битов в Rijndael, подобном шифру ADE, оказалось реализованным в шифре GrandCru (одном из участников конкурса Nessie). Окончательный выбор пал на победителя конкурса AES — шифр Rijndael, имеющий авторитетную поддержку на международном уровне. Украинские решения не имели заметных преимуществ перед шифром Rijndael.

Естественно, работа над экспертизой проектов потребовала освоения международного опыта и повлияла на разработку собственных подходов и методик, позволяющих ускорить процесс анализа и принятия решений. Новый подход в теории и методах криптоанализа, описанный в [1], ориентирован, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа их уменьшенных версий, а с другой, — на уточненную в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров концепцию (новую идеологию) определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [2].

Относительно применения уменьшенных моделей прототипов (для которых уже имеется вполне достаточно вычислительных ресурсов даже для проведения атаки полного перебора ключей) следует заметить, что большое число хорошо известных алгоритмов шифрования допускают масштабирование. Удалось построить уменьшенные модели, которые сохраняют все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения по показателям стойкости соответствующих

больших версий (хотя доказательства адекватности моделей нуждаются в доработке).

Главный и неожиданный результат изучения уменьшенных моделей состоит в том, что общепринятая точка зрения, представленная во многих работах, оказалась не совсем верной. Эта точка зрения заключается в том, что линейные и дифференциальные свойства шифров непосредственно связаны с соответствующими свойствами *S*-блоков, используемых при их построении. На самом деле получаемые в результате (при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются для большого числа *S*-блоков практически только размером битового входа в шифр. Свойства *S*-блоков сказываются (в незначительной степени) только на динамике перехода к показателям случайной подстановки. Поэтому оказалось целесообразным оценивать эффективность шифрующих преобразований в целом по числу циклов, необходимых шифру для прихода к асимптотическим значениям максимумов полных дифференциалов и линейных корпусов, свойственных случайным подстановкам.

Второй важный вывод из результатов выполненных исследований сводится к тому, что показатели стойкости больших шифров (полных реализаций) к атакам дифференциального и линейного криптоанализа (таких, как Rijndael, Лабиринт, Калина, Мухомор, ADE [3—6]) могут быть получены в результате расчетов по формулам для максимумов полных дифференциалов.

Несмотря на то, что украинские шифры не смогли выдержать конкуренции с Rijndael, результаты, полученные в ходе работы над проектами, и результаты экспертизы решений по построению БСШ, заслуживают дальнейшего изучения и развития. Попытаемся обобщить полученные результаты анализа дифференциальных свойств уменьшенных моделей шифров, представленных на украинский конкурс, и дополнить их некоторыми новыми результатами.

Уменьшенные модели шифров и особенности их реализации. Во всех представленных далее разработках за основу взят размер битового входа в шифры, равный 16 битам. Это максимально возможный размер, позволяющий вычислительно реализовать большинство известных в настоящее время атак (методов) криптоанализа.

Шифр Mini-AES. В [7] приведено описание уменьшенной модели этого шифра, которая представляет собой уменьшенную четырехцикловую версию шифра AES [8]. Для получения 16-битной модели 128-битный AES следует уменьшить в восемь раз. В модели реализованы все операции прототипа, но при масштабировании размер *S*-блоков взят равным четырем битам (восьмикратное уменьшение байтового *S*-блока приводит к

однобитному вырожденному преобразованию) и соответственно число *S*-блоков в уменьшенной модели взято равным четырем. Линейное преобразование (операции MixColomn и ShiftRow), которое в оригинальной разработке осуществляет перестановку (сдвиг) строк и перемешивание столбцов, в уменьшенной версии заменено умножением выходов двух смежных полубайтовых *S*-блоков на уменьшенную в два раза матрицу (МДР кода с максимально достижимым расстоянием) над полем $GF(2^4)$.

В шифре Mini-AES в качестве *S*-блоков использована одна и та же таблица подстановок, значения которой задаются первой строкой первого *S*-блока шифра DES. В [9] рассмотрены варианты построения уменьшенных (полубайтовых) *S*-блоков по идеологии, использованной разработчиками AES [10]. В [11] реализованы программы, позволяющие менять число циклов шифрования от одного до восьми. Схема разворачивания ключей повторяет идеи, реализованные в прототипе.

Шифр Mini-ADE. Алгоритм ADE [6] разработан на основе шифра AES. Для повышения стойкости шифра AES к алгебраическим атакам в шифрующее преобразование были введены механизмы динамического управления промежуточными преобразованиями. С этой целью в структуру цикловых преобразований, включающих в AES операции рассеивания, сдвига и нелинейной побайтовой замены, введены (без изменения принципиальной основы использованных в AES решений), ключезависимые параметры, позволяющие реализовать динамическое изменение результатов каждой из операций в зависимости от текущего значения ключевых бит.

Например, в шифре ADE используются изменяемые таблицы блоков замены, формируемые с помощью дополнительно введенного параметра $\gamma \in GF(2^8)$, который определяется битами расширенного мастер-ключа. Идея этого преобразования реализована и в шифре Baby-ADE [11], но оно масштабировано соответственно размеру 16-битного состояния. Поэтому в качестве *S*-блоков (операции SubByte) используется изменяемая матрица подстановок, которая реализуется с помощью вычисления мультипликативно обратного элемента $(a\gamma)^{-1} \in GF(2^4)$ с последующим выполнением аффинного преобразования $b = \beta^T = (M(a\gamma))^{-1} + \beta$, где $a = \{a_0, a_1, a_2, a_3\}$ и $b = \{b_0, b_1, b_2, b_3\}$ — четырехбитные векторы (полубайты матрицы состояний); M — квадратная невырожденная матрица 4×4,

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix};$$

β — четырехбитный вектор, $\beta \in GF(2^4)$; $\beta^T = (1 \quad 0 \quad 1 \quad 0)$.

Каждое значение выхода подстановки $b=\{b_0, b_1, b_2, b_3\}$ зависит как от входного состояния $a=\{a_0, a_1, a_2, a_3\}$, так и от случайного вектора $\gamma=\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$, который задается значением циклового ключа. В результате осуществляется криптографическое преобразование данных, при котором происходит динамическое изменение *S*-блоков (блоков нелинейных замен), с сохранением показателей их нелинейности. Управляемыми с помощью битов подключа являются и операции MixColumn и ShiftRow [12].

Шифр Мини-Калина [13]. В этом алгоритме шифрования использованы те же принципиальные решения, что и при построении основной версии предложения [5]. Практически он является результатом масштабирования оригинальной разработки к размерам входного блока и ключа, равным 16 битам. Отличия шифра Калина от шифра Rijndael состоят в следующем:

- используемые *S*-блоки построены на основе отбора из множества случайных подстановок и поэтому не допускают простого алгебраического описания, как это удается сделать для *S*-блоков шифра Rijndael;
- цикловый подключ вводится не однообразным сложением состояний шифра с ключевыми состояниями по mod2, а используется попеременное (через цикл) сложение с подключами по модулю два (XORRoundKey) для нечетных циклов и сложение с подключами по модулю 2^{32} (Add32RoundKey) для четных циклов;
- использована иная схема разворачивания ключей.

Эти особенности учтены при построении малой версии шифра Калина, т.е. в ней практически полностью повторяются решения по построению функций ShiftRows и MixColumns шифра Baby-Rijndael. При этом, как и в шифре Baby-Rijndael, слой нелинейного преобразования реализован с помощью четырех *S*-блоков 16-й степени, а вместо функции Add32RoundKey использовано сложение с битами подключа по модулю 2^4.

Для получения цикловых подключей из исходного мастер-ключа используется процедура разворачивания ключей, повторяющая в уменьшенной версии оригинальную разработку [13]. Для 10-цикловой миниверсии требуется 12 подключей, каждый длиной 4×4 бита (размер подключа совпадает с размером открытого (шифрованного) текста и текущего состояния шифра).

Шифр Мини-Мухомор. В большом шифре Калина [5] используется восемь различных подстановок «байт-в-байт», причем для байтов одной строки текущего состояния шифра используется одна и та же подстановка. В описании шифра готовые таблицы подстановок приведены в приложении и об их построении ничего не сказано. В [3] указано, что для шифра Мухомор таблицы подстановок совпадают с первыми четырьмя *S*-блоками алгоритма Калина. Поэтому при построении уменьшенной модели

этого шифра предложено использовать набор малых *S*-блоков с различными (или одинаковыми) параметрами γ шифра Baby-ADE или малые *S*-блоки шифра Fox, обладающие высокими дифференциальными и линейными характеристиками переходов [14]. Следует, однако, заметить, что в исследованиях, описанных в [14], они не применялись.

Некоторые *S*-блоки, использованные при построении уменьшенных моделей рассматриваемых шифров, представлены в табл. 1, а также в работе [9], где приведены результаты детального изучения криптографических показателей указанного семейства малых *S*-блоков (подстановок 16-го порядка).

При построении уменьшенной версии шифра Мухомор возникла ситуация, когда шифр содержит преобразование, не допускающее прямого масштабирования. К такой операции относится *SL*-преобразование. В эту операцию оригинальной конструкции входят слой нелинейных преобразований, реализуемый с помощью четырехбайтовых *S*-блоков, и последующее МДР преобразование, с помощью которого осуществляется матричное умножение байтовых выходов четырех *S*-блоков (над полем $GF\ (2^8)$) на квадратную матрицу размера 4×4. (По существу, аналогичное преобразование выполняется в шифре Rijndael с помощью операции MixColumns, но там при умножении используется другой полином.) При масштабировании этой операции к 16-битной модели она получается четырехбитной (в оригинале она 32-битная). Поэтому было принято решение заменить ее подстановочной, эквивалентной по эффективности.

В работе [15] выполнена оценка дифференциальных свойств (закон распределения переходов таблицы XOR разностей) *SL*-преобразования 16-битной версии, повторяющей оригинальную. В рассматриваемом слу-

Таблица 1. ***S*-блоки для уменьшенных версий шифров**

Шифр	Выход *S*-блока (вторая строка подстановки)															
Mini*A*	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
Baby*R*	10	4	3	11	8	14	2	12	5	7	6	15	0	1	9	13
ADE6	10	2	0	6	15	1	12	4	14	11	7	13	9	5	3	8
ADE7	10	3	8	2	5	6	0	9	11	4	12	14	15	7	13	1
ADE3	10	11	2	14	0	13	6	7	15	5	1	9	12	8	4	3
Лабиринт	*B*	8	6	4	*A*	0	*D*	2	*C*	5	1	*E*	3	*F*	9	7
Случаайный S_1	11	8	6	4	10	0	13	2	12	5	1	14	3	15	9	7
Случайный S_2	10	2	0	6	15	1	12	4	14	11	7	13	9	5	3	8

чае для построения *SL*-преобразования были использованы четыре *S*-блока уменьшенной версии шифра Baby-Rijndael [5]. Результаты вычислительного эксперимента по выполнению операции MixColumns над четырьмя такими *S*-блоками (одинаковыми) привели к выводу, что для полубайтовых *S*-блоков выбрать соответствующий разумно обоснованный эквивалент не удается (слишком мало степеней свободы в выборе подстановки 16-й степени). Поэтому было принято решение в качестве *SL*-преобразований в малой версии шифра использовать *S*-блоки случайного типа. Все остальные операции масштабирования прототипа, в том числе и операция разворачивания мастер-ключа, затруднений не вызвали.

Шифр Мини-Лабиринт. Как и все другие алгоритмы, шифр Лабиринт [3] построен по итеративной схеме, т.е. его основу составляет цикловое преобразование, повторяемое заданное число раз. Каждый цикл состоит из двух абсолютно идентичных итераций, осуществляющих преобразование (зашифрование) двух полублоков, на которые разбивается блок данных на входе каждого цикла. Однако, поскольку для обновления обоих полублоков, составляющих один блок, в предлагаемом решении требуется, как минимум, две итерации, в работе [3] понятие цикла отделено от понятия итерации (т.е. цикл состоит из двух итераций).

Кроме повторяющегося циклового преобразования процедура зашифрования включает начальное *IT* и конечное *FT* преобразования. Свойство инволютивности шифра достигается с помощью классической конструкции полублоковой цепи Фейстеля. Все эти решения, естественно, сохранены в уменьшенной модели алгоритма Лабиринт. Подобная структура процедуры зашифрования с учетом уменьшенного размера входного блока данных представлена на рис. 1 [16]. Число циклов в уменьшенной версии может меняться от одного до 16. Поскольку шифр построен по достаточно оригинальной схеме, приведем более детальное его описание.

Процедура зашифрования *EF* состоит из трех этапов.

1. Исходный блок данных $P_{<16>}$ (длиной 16 бит, что подчеркивается индексом <16> у символа исходного блока данных P) обрабатывается начальным *IT* преобразованием на ключе K^{IT} (здесь и далее будем сохранять обозначения, использованные в оригинальной разработке).

2. Результат первого этапа разбивается на два полублока длиной по восемь бит каждый: левый $L^0_{\langle 8\rangle}$ («старший») и правый $R^0_{\langle 8\rangle}$ («младший»). Полученная пара полублоков преобразуется на восьми итерациях (четырех циклах) цепи Фейстеля. Все итерации полностью идентичны и построены на основе общего нелинейного преобразования — *F*-функции, управляемой ключами итерации $K(i)$, $i = 1, 2, ..., 2r$;

3. Два полублока, $L^{2r}_{\langle 8\rangle}$ и $R^0_{\langle 8\rangle}$, полученные в результате четырехциклового итеративного преобразования, меняются местами и обрабатываются

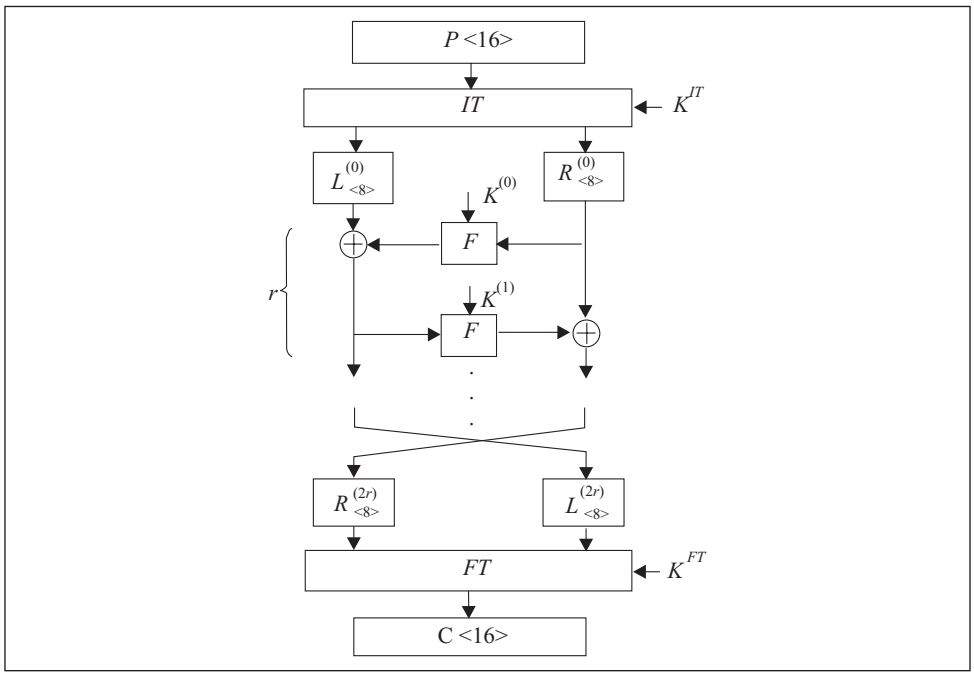

Рис. 1. Схема процедуры шифрования

конечным *FT* преобразованием на ключе K^F. Полученный после *FT* преобразования двоичный вектор $C_{<16>}$ (длиной 16 бит) является зашифрованным блоком (криптограммой).

На каждой итерации *F*-функция использует восьмибитный подключ $K^{(i)}$. Длина ключей начального K^{IT} и конечного K^{FT} преобразований составляет по 16 бит.

***F*-функция.** В уменьшенной модели повторена конструкция *F*-функции большого шифра, но операции в ней выполняются не над байтами, а над двумя полубайтами. Сложение двух полубайтов циклового ключа с полублоками из полубайтов входного блока данных выполняется в этом случае по модулю 2^8. Кроме того, фиксированная перестановка *P* (как и в большом шифре для длительности блока данных 128 бит) в уменьшенной версии шифра не применяется. Таким образом, *F*-функция, использующая в процессе преобразований подключ из восьми бит, может быть представлена такой же схемой, как и *F*-функция большого шифра (рис. 2).

Начальное и конечное преобразования представляют собой, по сути, два дополнительных цикловых преобразования шифра [16].

Начальное *IT* преобразование уменьшенной версии шифра Лабиринт (рис. 3), повторяя структуру оригинальной разработки, включает сложе-

ние по модулю 2^8 полублоков входного блока данных (по восемь бит) с восемьюбитными рабочими подключами (левый полублок ключа суммируется с левым полублоком входного блока данных, а правый полублок ключа — соответственно с правым полублоком входного блока данных).

На следующем шаге 16 результирующих бит разбиваются на блоки по четыре бита, которые подаются на нелинейные преобразования (*S*-блоки). Затем 16 бит снова разбиваются на два полублока, где выполняются циклические сдвиги: левый полублок сдвигается на два бита влево, а правый — на два бита вправо. В заключение над полученным 16-битным блоком выполняется операция инволютивного линейного смешивания IMix.

В уменьшенной версии шифра операция IMix, так же как и в оригинальном алгоритме, реализует сложение по модулю два восьмибитных полублоков входного блока данных и, после циклического сдвига результата влево на пять бит, его сложение по модулю два с полублоками входного блока данных, поступающими на вход преобразования IMix.

Конечное *FT* преобразование выполняет те же операции, что и начальное, но в обратном порядке. Как и в большом шифре, после выполнения последней итерации цепи Фейстеля левый и правый полублоки меняются местами, и только после этого результирующий блок поступает на вход *FT* преобразования.

Преобразование SL определяет фиксированное биективное отображение слов и представляет собой объединение нелинейного преобразования байтов (с помощью байтовых *S*-блоков) с последующим линейным «смешиванием» результатов нелинейного преобразования.

В уменьшенной модели операции выполняются над полубайтами. Поэтому сначала над каждыми двумя полубайтами, объединенными в полублок, выполняется нелинейное преобразование с помощью уменьшенных (полубайтовых) *S*-блоков, над выходными полубайтами которых выполняется CMBN (Cyclic Maximum Branch Number) преобразование. Это преобразование осуществляет биективное линейное отображение слов, составляющих полублок (для уменьшенной модели полублок имеет размерность байта).

В уменьшенной версии шифра полностью сохранена идея построения CMBN преобразования. Оно реализовано в виде умножения квадратной матрицы размерностью 2×2 полубайта, образованной циклическим CMBN кодом, справа на вектор-столбец длиной один байт (два полубайта, соответствующих слову-аргументу). Элементы матрицы и элементы векторов аргумента (результата), интерпретируются как элементы поля $GF(2^4)$ (полубайты), образованного выбранным неприводимым (над полем $GF(2)$) полиномом четвертой степени $f_{\mathrm{CMBN}}(x) = x^4 + x^3 + 1$. В данной мини-вер-

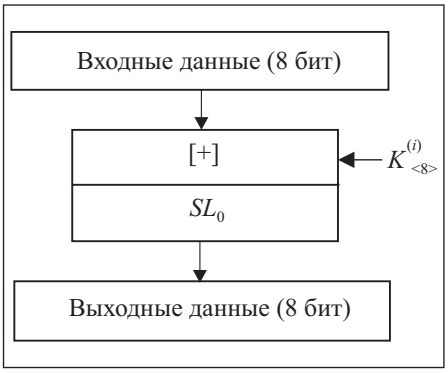

Рис. 2. Схема восьмибитной *F*-функции

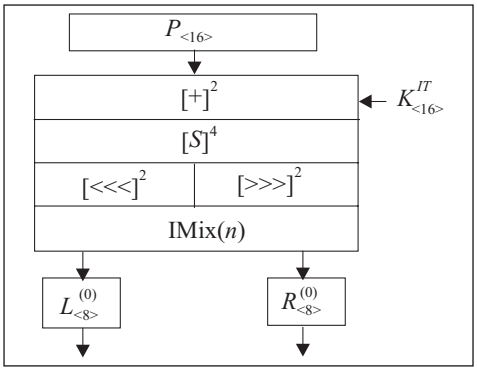

Рис. 3. Начальное преобразование *IT*

сии БСШ Лабиринт использован следующий полином второй степени, порождающий CMBN код: $g(x) = 11x + 01$.

Как указано в [3], *S*-блок шифра Лабиринт выбран из множества так называемых предельно-нелинейных биективных преобразований, в основе которых лежит конструкция Ниберга—Динга, т.е. преобразование, аффинно-эквивалентное функции вычисления обратного элемента в поле. В малой версии шифра Лабиринт эта конструкция использована для полубайтовых подстановок. Детальное ее описание можно найти в [9]. Следует заметить, что свойства *S*-блоков шифра Лабиринт подобны свойствам *S*-блоков шифра Rijndael.

В малой версии шифра предусмотрена и процедура разворачивания мастер-ключа. Она отмасштабирована под длину исходного (пользовательского) ключа 16 бит и в уменьшенной версии полностью повторяет оригинальную разработку [3].

Шифр Baby-Rijndael. Еще одна уменьшенная до нужных размеров модель шифра AES (Baby-Rijndael) описана в [17]. Если ранее [7] предлагалось в качестве элементов нелинейной замены использовать первую строку подстановки первого *S*-блока шифра DES, то в данной версии при построении *S*-блоков использованы идеи, предложенные в [10] (см. табл. 1, *S*-блок Baby*R*). Следует заметить, что линейное преобразование в этом шифре при умножении на матрицу отличается от линейного преобразования шифра Rijndael.

Шифрование в Baby-Rijndael начинается с того, что входной 16-битный блок данных в полубайтовом представлении $\gamma_0\ \gamma_1\ \gamma_2\ \gamma_3$ преобразуется в матрицу состояния $\begin{bmatrix} \gamma_0 & \gamma_2 \\ \gamma_1 & \gamma_3 \end{bmatrix}$. Общая структура процедуры зашифрова-

ния представляется в виде $E(a) = r_4 \circ r_3 \circ r_2 \circ r_1(a \oplus k_0)$, где a — состояние; k_0, k_1, k_2, k_3, k_4 — цикловые подключи; $r_i(a) = (t\hat{\sigma}(S(a))) \oplus k_i$. При этом в r_4 умножение на t отсутствует (для четвертого цикла). В конце зашифрования состояние преобразуется в 16-битный блок в таком же порядке, как это было сделано при загрузке.

Описание индивидуальных компонент шифра:

S-operation является табличным преобразованием замены каждой шестнадцатеричной цифры состояния:

$$\begin{bmatrix} \gamma_0 & \gamma_2 \\ \gamma_1 & \gamma_3 \end{bmatrix} \to \begin{bmatrix} s(\gamma_0) & s(\gamma_2) \\ s(\gamma_1) & s(\gamma_3) \end{bmatrix},$$

где s — таблично заданная функция (см. табл. 1, Baby*R*);

$\hat{\sigma}$ — операция обмена входов во второй строке состояния:

$$\begin{bmatrix} \gamma_0 & \gamma_2 \\ \gamma_1 & \gamma_3 \end{bmatrix} \xrightarrow{\hat{\sigma}} \begin{bmatrix} \gamma_0 & \gamma_2 \\ \gamma_3 & \gamma_1 \end{bmatrix}.$$

Матрица t линейного преобразования является 8×8 битовой матрицей вида

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Для этого преобразования состояние рассматривается как 8×8 битовая матрица и умножается слева с использованием матричного умножения на матрицу t по модулю 2: $a \to ta$. При этом верхняя левая 4×4 подматрица матрицы t равна нижней правой подматрице, и верхняя правая и нижняя левая подматрицы также равны.

В начале шифра и в конце каждого цикла состояние побитно складывается по модулю два с цикловыми подключами. Они задаются массивами 2×2, подобными состоянию. Колонки цикловых подключей определяются рекурсивно по следующему правилу:

$$w_0 = \begin{pmatrix} k_0 \\ k_1 \end{pmatrix} w_1 = \begin{pmatrix} k_2 \\ k_3 \end{pmatrix},$$

$$w_{2i} = w_{2i-2} \oplus S\,(\text{reverse}\,(w_{2i-1})) \oplus r_i\ ,$$

$$w_{2i+1} = w_{2i-1} \oplus w_{2i},\ \ i = 1, 2, 3, 4.$$

Константы определяются по правилу $r_i = \begin{pmatrix} 2^{i-1} \\ 0 \end{pmatrix}$, а обратные функции меняют местами два входа в колонке, S-функция остается прежней. Все сложения выполняются побитно по модулю два. Цикловые подключи k_i при $i = 0, 1, 2, 3, 4$ — матрица, колонками которой являются w_{2i} и w_{2i+1}. Еще одной особенностью этой уменьшенной модели является отличие реализации процедуры линейного преобразования от примененной в шифре Rijndael: в уменьшенной модели шифра Baby-Rijndael умножение на матрицу осуществляется одновременно для всех четырех полубайтовых выходов S-блоков. При этом матрица имеет битовые значения и операция умножения выполняется по модулю два.

Общий подход к оценке дифференциальных свойств шифров. Выражение для числа $\Lambda_{m,2k}$ переходов XOR (таблицы дифференциальных разностей) случайной подстановки порядка 2^m (среднего значения числа ненулевых характеристик $\Delta X \to \Delta Y$ таких, что $\Lambda_\pi(\Delta X, \Delta Y) = 2k$), имеет вид [18, 19]

$$\Lambda_{m,2k} = \frac{(2^m - 1)^2}{2^m!} \begin{pmatrix} 2^{m-1} \\ k \end{pmatrix}^2 k!2^k\, \Phi\,(2^{m-1} - k), \tag{1}$$

где функция $\Phi\,(d)$ определяется соотношением

$$\Phi\,(d) = \sum_{i=0}^{d} (-1)^i \begin{pmatrix} d \\ i \end{pmatrix}^2 2^i\, i!(2d - 2i)! \tag{2}$$

Если выражение (1) разделить на число всех ненулевых входов (ячеек) дифференциальной таблицы, то оно, по существу, описывает закон распределения переходов XOR таблицы случайной подстановки.

В работе [18] среднее значение максимума таблицы XOR разностей найдено из соотношений (1), (2) после определения значения k, при котором можно получить наименьшее целое значение k, близкое к единице. Это и будет максимально возможное значение k^*, определяемое из уравнения

$$\frac{(2^m - 1)^2}{2^m!} \begin{pmatrix} 2^{m-1} \\ k^* \end{pmatrix}^2 k^*!2^{k^*}\, \Phi\,(2^{m-1} - k^*) \approx 1. \tag{3}$$

Результаты решения уравнения (3) для различных значений m приведены в работе [19, табл. 1], где предложена оценка среднего значения максимума XOR таблицы случайной подстановки степени 2^m в виде $k^* \le (m+4)$. Предложенная оценка позволяет с достаточно высокой для практического применения точностью вычислить среднее значение максимума XOR таблицы случайной подстановки без использования формулы (3). Эффективность предложенной аппроксимации заключается в том, что сложность вычислений по формулам (1) и (2), вместо (1), (2) и (3), при увеличении значения m быстро возрастает, становясь непреодолимой. До настоящего времени удалось выполнить вычисления для значения $m = 16$.

С помощью формул (1), (2) можно сформулировать закон распределения парных разностей (переходов дифференциальной таблицы) для случайной подстановки. Результаты расчетов по формулам (1), (2) описаны, например, в работе [19, табл. 3], где сопоставлены законы распределения парных разностей для уменьшенной 16-битной модели шифра Rijndael и случайной подстановки степени 2^{16}. Представленные результаты свидетельствуют о практическом совпадении этих законов, и, следовательно, для оценки показателей стойкости малых моделей можно воспользоваться результатами расчетов максимумов переходов таблиц XOR разностей случайной подстановки.

В общепринятых обозначениях, например [7], выражение для максимальной дифференциальной вероятности подстановочного преобразования f имеет вид $DP^f_{\max} = \max\limits_{\Delta x \neq 0,\, \Delta y \neq 0} DP^f(\Delta x \to \Delta y)$, где f — функция преобразования входной разности Δx в выходную разность Δy. Очевидна связь этого выражения с выражением (1):

$$DP^f_{\max} = \frac{\Lambda_{m,\,2k^*}}{(2^m - 1)^2}, \tag{4}$$

где k^* — среднее значение максимума дифференциальной таблицы подстановки. Следует заметить, что значение $DP^f_{\max}$ для многоциклового шифрующего преобразования определяется таким утверждением.

Утверждение [2]. Для шифрующих преобразований, определяемых многоцикловыми процедурами перестановочно-подстановочных биективных отображений, свойственных современным блочным симметричным шифрам, ожидаемая вероятность самой правдоподобной ненулевой дифференциальной характеристики ограничена значением $(m+4)/2^m$.

Результаты оценки дифференциальных свойств уменьшенных моделей шифров. Методика выполнения исследований дифференциальных свойств мини-шифров достаточно подробно изложена в [12]. Шифр можно рассматривать как подстановочное преобразование при каждом фиксированном значении ключа. Поэтому сначала была изучена зави-

симость максимумов полных дифференциалов (таблиц XOR разностей для всего многоциклового шифрующего преобразования) от ключевых значений. Для мини-версии шифра Калина построены дифференциальные таблицы с частичным и полным перебором ключей для числа циклов шифрования от одного до четырех с использованием *S*-блоков с минимально возможными значениями δ-равномерности [20, *S*-блоки Baby*R*]. Результаты исследований приведены в табл. 2.

Как следует из полученных результатов, среднее (по множеству ключей) значение максимума после трех циклов шифрования принимает асимптотическое (установившееся) значение, не превышающее числа $m + 4 = 20$. Практически среднее значение максимума полного дифференциала рассматриваемого шифрующего преобразования оказывается близким к максимуму по всему множеству ключей зашифрования, т.е. оценку среднего значения максимума XOR таблицы (полного дифференциала) для произвольного ключа зашифрования можно рассматривать как значение, позволяющее согласно (4) определить стойкость к атакам дифференциального криптоанализа (требуемую безопасность).

Экспериментально были проверены результаты исследований, полученные в других работах для уменьшенных моделей шифров AES и ADE при выборке 1000 ключей (остальные шифры проверены на отдельных ключах зашифрования). Для каждого шифра построено 100 дифференциальных таблиц с использованием нелинейных узлов замены из табл. 1. Исследования проводили в двух направлениях по множеству из 100 случайно выбранных ключей шифрования:

1. Определяли абсолютные значения максимумов таблиц разностей мини-шифров.

2. Определяли средние значения максимумов таблиц разностей мини-шифров.

При выполнении этих исследований в шифрах Мини-AES, Мини-ADE и Мини-Лабиринт использовали уменьшенные полубайтовые *S*-блоки, повторяющие конструкции *S*-блоков больших версий шифров (с мини-

Таблица 2. **Результаты полного перебора ключей для шифра Мини-Калина**

Число циклов	Число экспериментов	Максимальное значение δ-равномерности	
		Абсолютное	Среднее
1	11 279	5120	3295,16
2	48 535	672	361,316
3	65 536	28	19,2439
4	65 536	26	19,1112

мально возможными значениями $\delta = 4$). В других шифрах со случайными *S*-блоками (Калина и Мухомор) были использованы два типа *S*-блоков: со значениями $\delta = 4$ и случайно порожденные *S*-блоки с большими значениями δ-равномерности. Кроме того, список уменьшенных моделей был дополнен 16-битным шифром из работы [21], в которой использованы идеи построения SPN шифра, изложенные в [22]. Результаты исследований первого и второго направлений приведены в табл. 3.

Для 16-битного шифра Хейса в первом случае в качестве *S*-блока использован *S*-блок шифра Mini*A* (первая строка первого *S*-блока шифра DES), а во втором — случайный *S*-блок (см. табл. 1, S_1), который по дифференциальным характеристикам не уступает *S*-блоку Baby*R*.

Таблица 3. **Абсолютные и средние значения максимумов таблиц разностей различных шифров**

Число циклов	Шифр Хейса		Мини-AES	Мини-ADE	Мини-Лабиринт	Мини-Мухомор		Мини-Калина	
	$\delta = 8$	$\delta = 4$	$\delta = 4$	$\delta = 4$	$\delta = 4$	$\delta = 8$	$\delta = 4$	$\delta = 8$	$\delta = 4$
Абсолютные значения									
1	32 768	16 384	16 384	16 384	—	65 536	65 536	7 168	6 144
2	12 288	4 096	4 096	5 120	—	16 384	6 144	1 376	640
3	2 490	488	352	1 024	128	4 608	3 072	38	24
4	286	98	22	38	22	2 304	224	22	22
5	92	46	22	24	24	156	60	22	22
6	36	22	20	22	24	36	20	24	24
7	22	22	—	—	26	—	—	—	—
8	22	22	—	—	22	—	—	—	—
Средние значения									
1	32 768	16 384	16 384	16 384	—	65 536	65 536	6082,56	3732,48
2	12 288	4 096	3036,16	3353,6	—	14187,5	5770,24	826,88	382,4
3	2326,81	439	274,24	307,2	37,5	2496,32	1802,24	24,8	**19,36**
4	216,803	56,964	**19,326**	20,54	**19,04**	542,72	125,53	**19,04**	19,14
5	65,38	26,18	19,02	**19,08**	19,24	46,28	29,7	19,14	19,2
6	24,108	**19,108**	18,812	19,24	19,04	**19,48**	**18,88**	19,14	19,36
7	**19,021**	19,086	—	—	19,14	—	—	—	—
8	19,16	19,1	—	—	19,24	—	—	—	—

Таблица 4. **Распределение переходов XOR таблиц шифра Мини-Мухомор**

Число циклов для одного ключа			
5		10	
#2	1 302 443 900	#2	1 302 455 754
#4	325 634 132	#4	325 627 300
#6	54 278 584	#6	54 284 259
#8	6 783 190	#8	6 781 258
#10	679 866	#10	678 321
#12	56 522	#12	56 731
#14	4 196	#14	4 086
#16	267	#16	245
#18	19	#18	16
#20	4	#20	2
#22	1		
#24	1		

Как было указано ранее, в шифре Мини-Мухомор таблицы подстановок, участвующие в *SL*-преобразованиях, сформированы случайным образом. Текущее состояние на входе функции усложнения *M*-8 представляется в виде двух полубайт, к каждому из которых применяется определенная подстановка. При реализации шифра Мини-Калина также использованы *S*-блоки двух типов: с высокими (*S*-блоки шифра ADE) и низкими (*S*-блоки шифра DES) дифференциальными показателями. Поскольку для шифра Мини-Лабиринт преобразования *IT* и *FT* считались отдельными циклами, данные для этого шифра в табл. 3 приведены начиная с третьего цикла. Полученные результаты свидетельствуют о том, что все рассмотренные шифры после выполнения соответствующего числа циклов пришли к установившемуся (асимптотическому) значению для данного порядка подстановок, весьма близкому к теоретически обоснованному значению $\Lambda_{m,2k^*} = 20$. В табл. 3 значения, соответствующие асимптотическим, выделены полужирным шрифтом.

Как видно из табл. 3, вычисленные абсолютные (для выборки рассматриваемого объема) значения максимумов полных дифференциалов для всех рассмотренных шифров весьма близки к соответствующим средним значениям максимумов полных дифференциалов. Разница между числом циклов, требуемых для выхода к асимптотическим значениям, у рассмотренных шифров составляет один-два цикла. Следует заметить, что близким по рассматриваемым показателям к уменьшенным версиям современных

шифров оказался и шифр Хейса с простейшей конструкцией линейного преобразования. Рассматриваемые шифры выходят на асимптотические значения максимумов полных дифференциалов в таком порядке: 1) Калина; 2) Лабиринт; 3) AES; 4) ADE; 5) Мухомор; 6) шифр Хейса.

Для более полной информации приведем распределение переходов XOR таблиц шифра Мини-Мухомор в зависимости от числа циклов зашифрования (табл. 4). Аналогичные результаты получены и для других версий уменьшенных шифров. Из табл. 4 видно, что дифференциальные свойства шифра Мухомор и других шифров с высокой степенью точности совпадают с дифференциальными свойствами случайной подстановки соответствующего порядка. Следует заметить, что представленные результаты полностью согласуются с ранее полученными в работах [12, 13, 15, 16].

Выводы

Если считать правомерным перенос свойств уменьшенных моделей шифров на их прототипы, то полученные результаты свидетельствуют о том, что дифференциальные свойства представленных на украинский конкурс шифров Калина, ADE, Мухомор и Лабиринт после четырех-пяти циклов зашифрования становятся близкими случайным подстановкам. В связи с этим можно сделать вывод о том, что современные БСШ (при полном наборе цикловых преобразований) действительно являются случайными подстановками.

Свойства шифрующих преобразований современных блочных симметричных шифров являются результатом случайных подстановок, и, следовательно, шифр Rijndael и шифры, представленные на украинский конкурс, являются эквивалентными (неразличимыми). Все они реализуют наибольшую вероятность максимума полного дифференциала (для 128 битных версий), близкую к 2^{-120}. Этот результат следует считать обоснованным теоретически и практически.

A new approach is proposed in theory and methods of cryptanalysis based on the use of analysis results of reduced models of large codes when determining the stability indices. The features of construction of reduced models of codes submitted to open tender for selection of candidates for the national standard of symmetric siphering block of Ukraine have been considered. The summarized data of analysis of differential properties of reduced models, and additional new results on the study of their differential characteristics are shown. The analysis models are associated with expected indices of prototypes stability.

1. *Долгов В. И., Лисицкая И. В., Олейников Р. В.* Подход к криптоанализу современных шифров // Материалы второй международной конференции «Современные информационные системы. Проблемы и тенденции развития».— Украина, Харьков—Туапсе, 2—5 октября. — 2007. — С. 435 — 436.

2. *Горбенко И. Д., Долгов В. И., Лисицкая И. В., Олейников Р. В.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа // Прикладная радиоэлектроника. — 2010. — **9**, № 3. — С. 312 — 320.
3. *Головашич С. А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Там же. — 2007. — **6**, № 2. — С. 230 — 240.
4. *Горбенко І. Д., Долгов В. І., Олійников Р. В. та ін.* Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація // Там же. — 2007. — **6**, № 2. — С. 147 — 157.
5. *Горбенко І. Д., Долгов В. І., Олійников Р. В.* Перспективний блоковий симетричний шифр «Калина». Основні положення та специфікація // Там же. — 2007. — **6**, № 2. — С. 195 — 208.
6. *Кузнецов А. А., Сергиенко Р. В., Наумко А. А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) // Там же. — 2007. — **6**, № 2. — С. 241— 249.
7. *Chung-Wei Phan R.* Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students // Cryptologia. — October, 2002. — XXVI (4). — P. 283—306.
8. *Final report* of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity and Encryption. — Version 0.15 (beta). — Springer-Verlag, 2004.
9. *Долгов В. И., Кузнецов А. А., Лисицкая И. В., Сергиенко Р. В., Олешко О. И.* Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров // Прикладная радиоэлектроника. — 2009. — **8**, №3. — С. 268 — 277.
10. *Daemen J. , Rijmen V.* AES proposal: Rijndael. — 1998. — http://www.nist.gov/aes.
11. *Долгов В. И., Кузнецов А. А., Сергиенко Р. В., Белоковаленко А. Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) // Прикладная радиоэлектроника. — 2008. — **7**, № 3. — С. 215 — 224.
12. *Долгов В. И., Кузнецов А. А., Сергиенко Р. В., Олешко О. И.* Исследование дифференциальных свойств мини-шифра Baby-ADE и Baby-AES // Там же. — 2009. — **8**, № 3. — С. 252 — 257.
13. *Долгов В. И., Олейников Р. В., Большаков А. Ю. и др.* Криптографические свойства уменьшенной версии шифра «Калина» // Там же. — 2010. — **9**, № 3. — С. 349 — 354.
14. *Junod P., Vaudenay S.* FOX specifications version 1.1. Technical Report EPFL/IC/2004/75. Ecole Polytechnique F ′ed′erale, Lausanne, Switzerland, 2004.
15. *Лисицкая И. В., Ставицкий И. А.* 32-битная мини версия блочного симметричного алгоритма криптографического преобразования информации «Мухомор». Оценка максимального значения полного дифференциала шифра. // Науч. ведомости Белгородского госуниверситета. — 2011. — №7 (102). Вып. 18/1. — С. 177—185.
16. *Долгов В. И., Лисицкая И. В., Григорьев А. В., Широков А. В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра «Лабиринт» // Прикладная радиоэлектроника. — 2009. — **8**, № 3 — С. 283—289.
17. *A Description* of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003.
18. *O'Connor L. J.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology // EUROCRIPT 93, Lecture Notes in Computer Science, T. Helleseth ed.— Springer-Verlag, 1994. — Vol. 795. — P. 360—370.
19. *Олейников Р. В., Лисицкая И. В., Широков А. В., Лисицкий К. Е.* Исследование дифференциальных свойств подстановок // Сб. науч. тр. Первой международной научно-технической конференции. «Компьютерные науки и технологии.». Ч. I. — Белгород, 2009. — С. 59 — 61.
20. *Seberry J., Zhang X. S., Zheng Y.* Relationships among nonlinearity criteria. Presented at EUROCRYPT-94, 1994.

21. *Heys H. M.* A Tutorial on Linear and Differential Cryptanalysis// CRYPTOLOGIA.— 2002. —Vol. 26, N 3.— P. 189—221.
22. *Feistel H.* Cryptography and computer privacy// Scientific American. — 1973.— 228 (5). — P. 15—23.
23. *Головашич С. А.* Анализ эффективности проектирования алгоритмов — участников конкурса БСШ Украины. — Харьков : ООО КРИПТОМАШ, 2009. — С. 70. http:// www.cryptomach.com/upload/ru/files/bc_design_effectiveness.pdf.

Поступила 10.12.10;
после доработки 27.10.11

ДОЛГОВ Виктор Иванович, д-р техн. наук, профессор кафедры БИТ Харьковского национального университета радиоэлектроники. В 1961 г. окончил Харьковское высшее военное командно- инженерное училище, а в 1965 г. — Харьковский госуниверситет. Область научных исследований — технологии блочного симметричного шифрования (разработка шифров и методы их криптоанализа).

КУЗНЕЦОВ Александр Александрович, д-р техн. наук, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета им. В. Н. Каразина. В 1966 г. окончил Харьковский военный университет. Область научных исследований — криптография, теория обработки и передачи данных, стеганографические методы защиты информации.

ИСАЕВ Сергей Александрович, аспирант факультета компьютерных наук Харьковского национального университета им. В. Н. Каразина, который окончил в 2009 г. Область научных исследований — теория защиты информации.