© Yevseiev S., Ostapov S., Korolev R. Use of mini-versions to evaluate the security of block-symmetric ciphers // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p.100-108.

DOI: 10.18372/2225-5036.23.11796

ИСПОЛЬЗОВАНИЕ МИНИ-ВЕРСИЙ ДЛЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНО-СИММЕТРИЧНЫХ ШИФРОВ

Сергей Евсеев[1], Сергей Остапов[2], Роман Королев[3]

[1]Харьковский национальный экономический университет им. С. Кузнеца, Украина
[2] Черновицкого национального университета им. Ю. Федьковича, Украина
[3]Харьковский университет Воздушных Сил им. И. Кожедуба, Украина

ЕВСЕЕВ Сергей Петрович, к.т.н.

Дата и место рождения: 1969, Харцызск, Донецкая обл., Украина.
Образование: Харьковский военный университет, 2002.
Должность: доцент кафедры информационных систем с 2007.
Научные интересы: безопасность банковской информации в автоматизированных банковских системах.
Публикации: более 180 научных публикаций включая монографии, книги, статьи и патенты.
*E-mail***:** serhii.yevseiev@hneu.net

ОСТАПОВ Сергей Эдуардович, д.ф.-м.н.

Дата и место рождения: 1957, Черновцы, Черновицкая обл., Украина.
Образование: Черновицкий государственный университет, 1980.
Должность: заведующий кафедры программного обеспечения компьютерных систем Черновицкого национального университета имени Юрия Федьковича.
Научные интересы: информационная безопасность, моделирование динамических систем.
Публикации: более 150 публикаций, включая монографии, книги, статьи.
E-mail: s.ostapov@chnu.edu.ua

КОРОЛЕВ Роман Владимирович, к.т.н.

Дата и место рождения:.1974, Красный Луч, Луганская обл. Украина.
Образование: Харьковский военный университет, 1999.
Должность: старший преподаватель кафедры боевого использования и эксплуатации АСУ.
Научные интересы: безопасность банковской информации в автоматизированных банковских системах.
Публикации: более 20 научных публикаций включая, учебники, статьи и патенты.
E-mail: korolevrv01@ukr.net

Аннотация. *Развитие криптологии в эру высоких технологий тесно связано с формированием новых подходов и методологий, позволяющих оценить стойкость используемых блочных симметричных шифров (БСШ) к основным видам атак линейного и дифференциального криптоанализа, учитывая основные требования по быстродействию криптопреобразований и энергетические затраты на реализацию. Предложенная в 2010 году новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного анализа учеными кафедры БИТ ХНУРЭ под руководством профессора Горбенко И.Д. ориентирована на использование ожидаемых показателей стойкости больших шифров на основе анализа показателей уменьшенных их версий, с одной стороны, и развитую на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, с другой стороны, концепции определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа. Для преодоления трудностей анализа полномасштабных моделей (алгоритмов) шифрования предлагается разрабатывать и исследовать показатели уменьшенных моделей прототипов (используются 16-ти битовые мини-версии), для которых имеющихся*

вычислительных возможностей достаточно. Однако вопрос использования мини-версий для оценки криптостойкости полных шифров поддерживается не всеми учеными. В этой статье приводятся результаты исследований алгоритмов Rijndael, Лабиринт, Калина, Мухомор, ADE на основе 16-ти и 32-х битных мини-версий. Показано, что для сохранения всех свойств прототипов в упрощенных моделях необходимым условием их адекватности является использование mini-S-box с основными показателями эффективности нелинейных узлов замен (сбалансированность, нелинейность, автокорреляция) на уровне данных показателей полномасштабных шифров. Для оценки использования уменьшенных моделей на основе предложенной методологии в статье приводятся результаты исследований на основе мини-версий (16-ти бит и 32-х бит) алгоритмов Rijndael, шифров Лабиринт, Калина, Мухомор, ADE, используемых в качестве экспериментального подтверждения правильности предложенной методологии и концепции оценки, анализируются основные показатели S-блоков мини-версий.

Ключевые слова: *блочно-симметричные шифры, уменьшенные модели БСШ, криптостойкость.*

Введение

Развитие криптологии тесно связано с совершенствованием методологи оценки блочных шифров, получивших широкое распространение в протоколах обеспечения безопасности банковской информации и других коммуникационных системах, и сетях благодаря высокой производительности и низкой сложности реализации. Кроме обеспечения конфиденциальности (защиты данных при передаче от пассивных атак), симметричные алгоритмы используются для обеспечения целостности на основе кодов аутентичности сообщений (MAC-кодов) и хэш-функций, как компоненты электронной цифровой подписи, генерации псевдослучайных после-довательностей в составе протоколов подтверждения подлинности и т.п.

Предложенная и развиваемая в работах [1–15] новая методология оценки стойкости блочно-симметричных шифров к атакам дифференциального и линейного криптоанализа строится на установленном факте, что все современные блочные шифры после нескольких начальных циклов шифрования приобретают свойства случайных подстановок соответствующей степени [5, 7].

Основой развиваемого подхода является положение, в соответствии с которым большие шифры повторяют свойства своих уменьшенных моделей. В работах [3–10] было показано, что большие версии шифров при использовании их в режиме шифрования укороченных (16-битных и 32-битных) блоков данных повторяют законы распределения вероятностей переходов XOR таблиц и таблиц смещений линейных аппроксимаций, свойственные соответствующим законам распределения вероятностей своих уменьшенных версий. Последние, в свою очередь, после нескольких начальных циклов шифрования приходят к законам распределения вероятностей переходов XOR таблиц и смещений таблиц аппроксимаций случайных подстановок [5, 7].

Анализ существующих исследований

Для проведения исследований использования мини-версий БСШ (уменьшенных моделей) к оценке стойкости полных шифров воспользуемся методикой исследований, предложенной в работах Долгова В.И. и Лисицкой И.В. [2, 3, 5–7], позволяющей использовать большой шифр как малый для шифрования блоков уменьшенной длины (зашифрованные блоки данных тоже усекаются до необходимого размера), при этом сохраняются все преобразования и внутренние связи большого шифра. Кроме этого, появляется возможность применить весь наработанный аппарат изучения показателей случайности малых версий шифров для определения показателей случайности больших шифров [2, 5, 7]. Для подтверждения правомерности использования новой идеологии оценки стойкости БСШ, как правило, используются мини-версии больших шифров в режиме шифрования укороченных (16-ти битных) блоков данных, результаты исследований представлены в работах [3–15].

Подобные исследования мини-версий проводились и зарубежными авторами. Так, в работах F.-X. Standaert с коллегами [16–17] исследовалась разница между теоретической и практической стойкостью шифров, введенной Л. Кнудсеном [18], причем была подтверждена ее существенная зависимость от размера блока. Проверка гипотезы эквивалентности ключей на мини-версиях AES показала, что ее необходимо проводить на полноразмерных ключах, для которых данный шифр и был спроектирован. Вывод, который можно сделать из анализа указанных работ, заключается в том, что нужно с осторожностью распространять на полноразмерные версии шифров выводы, сделанные на основе экспериментов с их мини-версиями.

Целью статьи является исследование мини-версий (16-ти бит и 32-х бит) алгоритмов Rijndael, шифров Лабиринт, Калина, Мухомор, ADE. Для экспериментального подтверждения правильности предложенной методологии и концепции оценки стойкости полных шифров, анализируются основные показатели S-блоков мини-версий.

Основная часть. Экспериментальные исследования использования мини-версий для оценки стойкости полных шифров

Анализ публикаций [1-4] и проведенные исследования мини-версий (упрощенных версий) рассматриваемых БСШ для оценки доказуемой безопасности полномасштабных моделей блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [5-15] показали, что предлагаемый подход учеными кафедры БИТ ХНУРЭ основывается на методологии

изучения свойств и показателей случайных подстановок уменьшенных моделей шифров.

Такое масштабирование хорошо допускают большое число современных алгоритмов. Этот факт позволяет решить многие задачи анализа и сравнения по показателям стойкости больших версий шифров.

Схематично новая методология представлена на рис. 1.

Основная идея, заложенная в новый подход оценки стойкости полных шифров, состоит в том, что итоговые (асимптотические) показатели стойкости (максимумы полных дифференциалов таблиц XOR разностей последовательностей шифрующих преобразований также, как и максимумы линейных аппроксимационных таблиц этих же преобразований зависят только от числа циклов шифрующего преобразования и размера битового входа [1]. Таким образом, для каждого блочного симметричного шифра (из числа известных БСШ) существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.

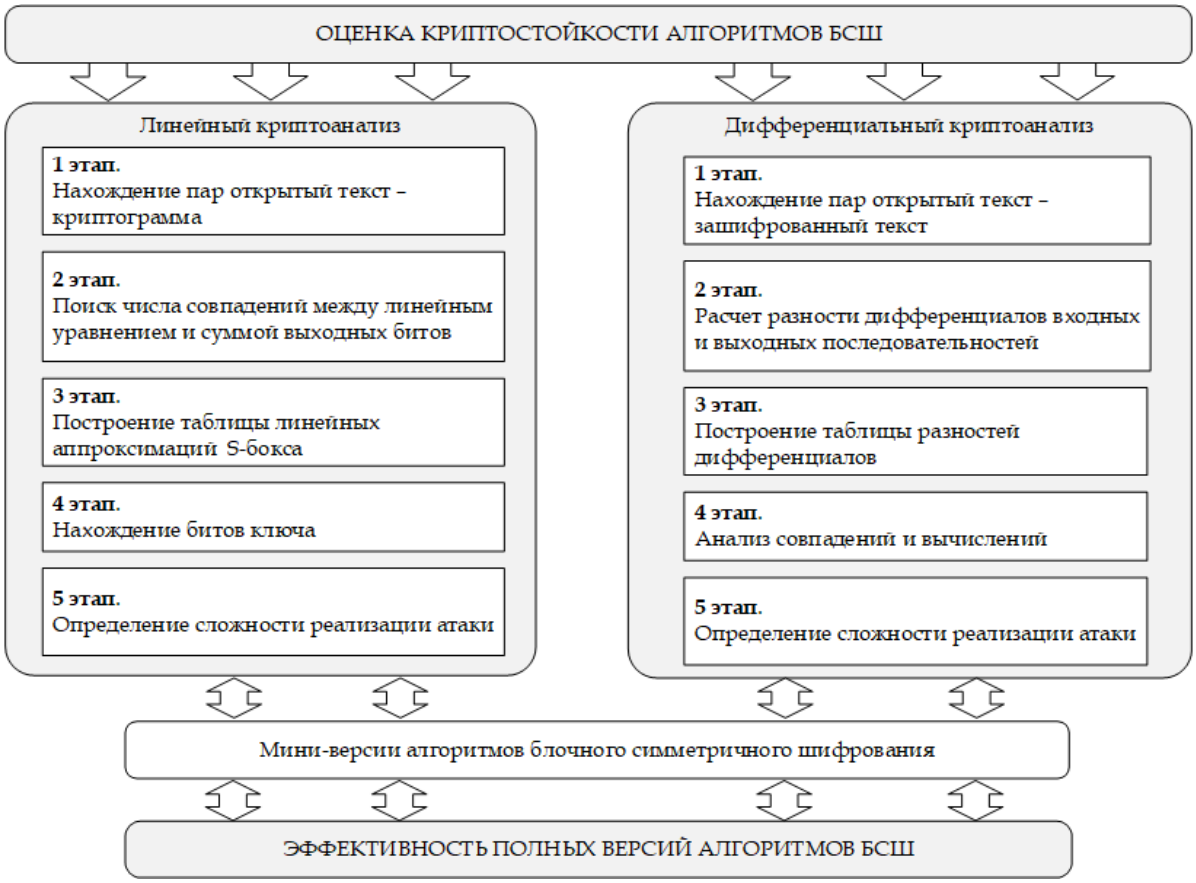

Рис. 1. Структурная схема методологии оценки стойкости блочных симметричных шифров

На основе анализа методологии оценки стойкости БСШ, рассмотренных в работах [1-7] определены основные этапы линейного и дифференциального криптоанализов, в соответствии с методикой оценки стойкости полных шифров [1, 3, 5, 6] (рис. 2).

Для проведения экспериментальных исследований были реализованы уменьшенные модели полных шифров *Rijndael, шифров Лабиринт, Калина, Мухомор, ADE*, участников всеукраинского конкурса на стандарт симметричного шифрования. На основе описания полных шифров [11–13] были реализованы мини-версии шифров с различными коэффициентами уменьшения (koef). В табл. 1 приведена информация о реализованных мини-версиях алгоритмов, коэффициент уменьшения, и количество операций для соответствующего алгоритма.

При построении мини-версий использовались два подхода для построения мини-S-блоков. Первый подход основан на работах Долгова В.И., Кузнецова А.А. [8, 11, 13], где для построения уменьшенного S-блока предлагается использовать отдельные строки S-box шифра Хейса.

При этом учитывается отдельные частные показатели S-box. Второй поход основан на работах Лисицкой И.В. [5, 6, 10, 22, 23], где для построения уменьшенного S-блока предлагается использовать случайную выборку строки S-блока полного шифра, как правило, выбирается 1 и/или 2 строка. На основании предложенной методики [3] ниже представлены результаты исследований.

Энергетические затраты на программную реализацию криптоалгоритмов Таблица 1

Алгоритм, koef	Операция	Полная версия	Мини-версия (16 бит)	Мини-версия (32 бит)
Лабиринт, koef=8	Сумма	264	24	28
	Умножение	264	24	28
Калина koef=8	Сумма	232	24	28
	Умножение	264	24	28
Мухомор koef=4	Сумма	232	24	28
	Умножение	264	24	28
AES koef=4	Сумма	232	24	28
	Умножение	232	24	28
ADE koef=4	Сумма	232	24	28
	Умножение	232	24	28

Рис. 2. Основные этапы линейного и дифференциального криптоанализов

В табл. 2 и на рис. 3 представлены результаты исследований стойкости мини-версий (16-ти бит и 32-х бит) шифров к дифференциальному криптоанализу (количество элементарных операций).

В табл. 3 и на рис. 4 представлены результаты исследований стойкости мини-версий (16-ти бит и 32-х бит) шифров к линейному криптоанализу (количество элементарных операций).

Результаты исследований стойкости мини-версий (16-ти бит и 32-х бит) шифров к дифференциальному криптоанализу (количество элементарных операций) Таблица 2

Алгоритм	16-ти битная мини-версия (теор)		16-ти битная мини-версия (практ)		32-ти битная мини-версия (теор)		32-ти битная мини-версия (практ)	
	S-box Хейса	Random S-box	S-box Хейса	Random S-box	S-box Хейса	Random S-box	S-box Хейса	Random S-box
Лабиринт	2^{40}	2^{29}	2^{38}	2^{29}	2^{43}	2^{35}	2^{42}	2^{34}
Калина	2^{33}	2^{23}	2^{30}	2^{22}	2^{37}	2^{30}	2^{37}	2^{29}
Мухомор	2^{28}	2^{22}	2^{27}	2^{21}	2^{33}	2^{30}	2^{33}	2^{30}
AES	2^{44}	2^{32}	2^{43}	2^{30}	2^{48}	2^{37}	2^{48}	2^{36}
ADE	2^{37}	2^{25}	2^{36}	2^{24}	2^{43}	2^{30}	2^{43}	2^{29}

Рис. 3. Результаты оценки стойкости мини-версий шифров к дифференциальному анализу

Изучение уменьшенных моделей БСШ показали, что линейные и дифференциальные свойства шифров непосредственно не связаны со свойствами S-блоков, т.е. получающиеся при использовании полного набора цикловых преобразований показатели стойкости шифров определяются практически только размером битового входа в шифр и могут быть получены расчетным путем. Полученные результаты (мини-версии 16-ти битные шифров) соответствуют результатам в работах [5, 6, 8, 10, 11, 13, 22, 23], что подтверждает правильность основных положений предлагаемой методологии.

Результаты абсолютных значений максимумов линейных свойств приведены в табл. 4 и на рис. 5.

Результаты исследований стойкости мини-версий (16-ти бит и 32-х бит) шифров к линейному криптоанализу (количество элементарных операций) Таблица 3

Алгоритм	16-ти битная мини-версия (теор)		16-ти битная мини-версия (практ)		32-ти битная мини-версия (теор)		32-ти битная мини-версия (практ)	
	S-box Хейса	Random S-box	S-box Хейса	Random S-box	S-box Хейса	Random S-box	S-box Хейса	Random S-box
Лабиринт	2^{43}	2^{32}	2^{42}	2^{32}	2^{47}	2^{35}	2^{47}	2^{34}
Калина	2^{35}	2^{26}	2^{33}	2^{24}	2^{38}	2^{28}	2^{38}	2^{27}
Мухомор	2^{31}	2^{25}	2^{30}	2^{24}	2^{35}	2^{27}	2^{35}	2^{26}
AES	2^{50}	2^{34}	2^{50}	2^{34}	2^{55}	2^{40}	2^{54}	2^{39}
ADE	2^{46}	2^{29}	2^{43}	2^{28}	2^{52}	2^{32}	2^{51}	2^{31}

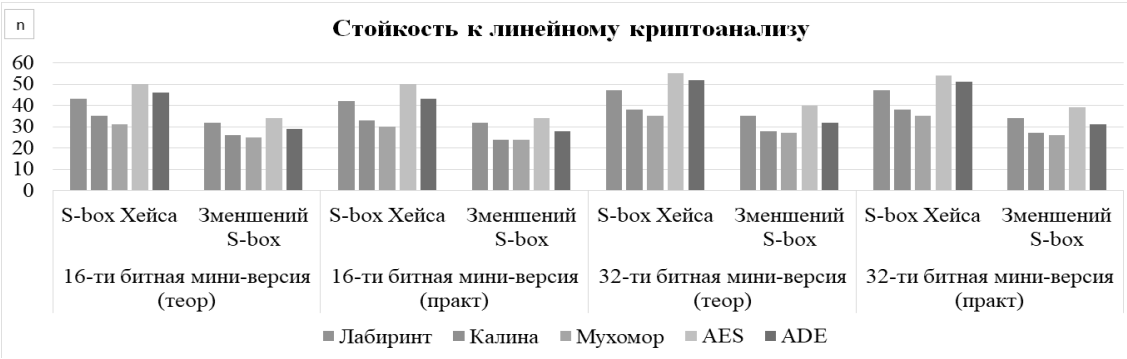

Рис. 4. Результаты оценки стойкости мини-версий шифров к линейному анализу

Результаты абсолютных значений максимумов линейных свойств шифров Таблица 4

Шифр/r	AES	ADE	Лабиринт	Калина	Мухомор
1	25722,88	25722,88	–	19292,16	19292,16
2	16076,8	19292,16	–	7033,6	15272,96
3	6832,64	6832,64	2267,08	1469,52	13181,72
4	1475,8	1463,24	1434,98	1431,84	13266,5
5	1413	1406,72	1416,14	1413	13607,19
6	1447,54	1381,6	1422,42	1431,84	13652,72

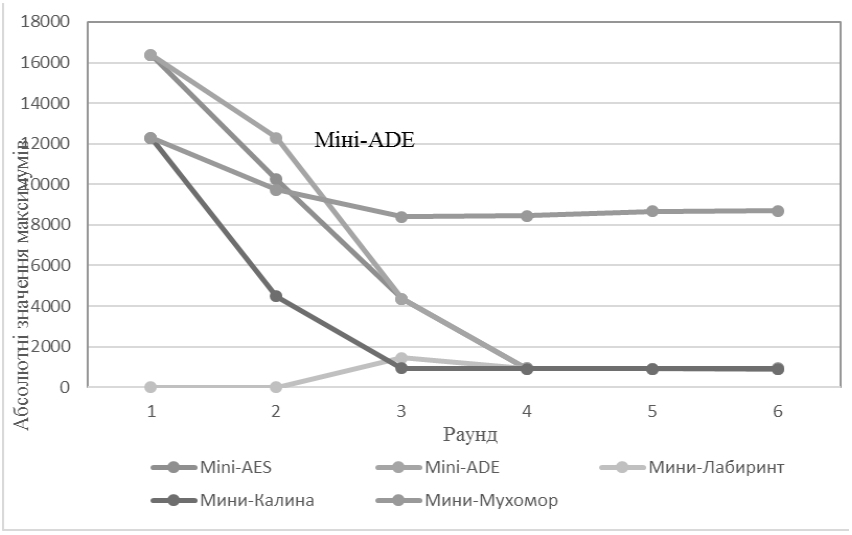

Рис. 5. Результаты абсолютных значений максимумов линейных свойств

Математическое ожидание максимумов и результаты предыдущей таблицы подтверждают, что БСШ после определенного числа циклов приобретает свойство случайной подстановки. В табл. 5 и на рис. 6 приведено математическое ожидание максимумов.

Математические ожидания максимумов шифров Таблица 5

Шифр/r	AES	ADE	Лабиринт	Калина	Мухомор
1	16384	16384	–	9349,15±237,02	11602±5424,45
2	9164,8±120,75	9093,10±94,3	–	3545,8±83,93	8499,2±622,48
3	3658,2±65,8	3509,8±62,37	1069,8±38,41	830,55±83,93	7928,7±6134,3
4	827,24±7,25	828,56±7,58	826,36±6,6	820,14±6,96	7605,4±6180,14
5	821,34±6,16	820,52±5,48	820,8±5,44	823,28±4	7660,65±6234,62
6	821,68±7	819,92±5,81	822,88±7,25	825,04±6,34	7738,65±6215,21

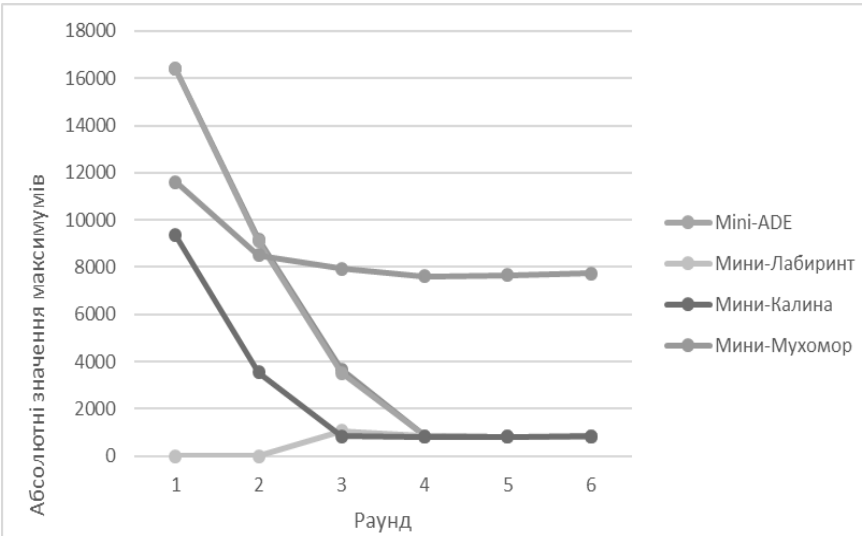

Рис. 6. Математическое ожидание максимум

Поцикловые значения максимумов полных дифференциалов для 16-битных сегментов приведены в табл. 6. Поцикловые значения максимумов смещений таблиц линейных аппроксимаций мини-шифров со значениями среднеквадратических отклонений представлены в табл. 7.

Поцикловые значения максимумов полных дифференциалов для 16-битных сегментов Таблица 6

Число циклов, r	Мини-Лабиринт	Мини-Калина	Мини-Мухомор	Мини-AES	Мини-ADE
1	37,5	3732,48	65536	16384	16384
2	**19,04**	382,4	5770,24	8904,25	3353,6
3	19,24	**19,36**	1802,24	1911.47	307,2
4	19,04	19,14	125,53	**19,24**	20,54
5	19,14	19,2	29,7	20,31	**19,08**
6	19,24	19,36	**18,88**	18,83	19,24
7	19,33	18,93	18,67	19,21	18,87
8	18,67	19,27	19	19,4	19,27
9	19	18,93	18	18,33	19,20
10	18	18,87	18,67	19,17	18,73

Поцикловые значения максимумов смещений таблиц линейных аппроксимаций мини-шифров со значениями среднеквадратических отклонений Таблица 7

Число циклов, r	Мини-Лабиринт	Мини-Калина	Мини-Мухомор	Мини-AES	Мини-ADE
1	3178±777	9671,1±867	32768±0	16384	16384
2	980±193	3370,6±301	12839,3±1031	9284.27±657,454	9093,10±94,37
3	825,4±14	836,8±15	6400±697	818.467±26,8809	3509,8±62,37
4	825,6±23	832,2±21	1797,6±347	815±28,204	828,56±7,58
5	817,2±11	838,6±21	837,8±47	818.5±18,536	820,52±5,48
6	824±21	835,5±33	815,6±24	815.967±20,18	819,92±5,81
7	823,4±30	821,5±22	817,2±20	832.1±33,1887	818,55±5,35
8	833,6±35	827,3±18	815,8±15	823.133±23,5722	837,34±5,91
9	824,8±24	813,3±21	815,5±15	829.9±33,5741	814,95±6,21
10	819±17	834±28	810±17	827.4±25,2885	822,54±7,13

Расчет полных дифференциалов позволяет теоретически определить количество циклов после, которых шифр приобретает свойства случайной подстановки.

Оценка случайности выходной последовательности (криптограммы) с помощью пакета NIST STS-822

Пакет тестов NIST STS для тестирования генераторов случайных или псевдослучайных чисел является одним из подходов реализации задачи оценки статистической безопасности криптографических примитивов. Таким образом, пакет NIST STS с высокой долей вероятности позволяет оценить, насколько сгенерируемая последовательность статистически безопасна.

В табл. 8 представлены результаты исследований.

Общие результаты тестов пакета NIST STS-822 Таблица 8

Алгоритм	Версия алгоритма	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96% последовательностей	Количество тестов, в которых тестирование прошли менее 96% последовательностей
Лабиринт	Полная версия	145 (76,72%)	189 (100%)	0 (0%)
	рандом (16-бит)	124 (65,61%)	189 (100%)	0 (0%)
	S-блок Хейса (16 бит)	139 (73,54%)	189 (100%)	0 (0%)
	рандом (32-бита)	133 (70,1%)	189 (100%)	0 (0%)
	S-блок Хейса (32 бит)	143 (75,66%)	189 (100%)	0 (0%)
ADE	Полная версия	122 (64,55%)	188 (99,45%)	1 (0,55%)
	рандом (16-бит)	86 (45,5%)	185 (98%)	4 (2%)
	S-блок Хейса (16 бит)	120 (63,49%)	187 (98,9%)	2 (1,1%)
	рандом (32-бита)	104 (55,02%)	187 (98,9%)	2 (1,1%)
	S-блок Хейса (32 бит)	122 (64,55%)	188 (99,45%)	1 (0,55%)
AES	Полная версия	133 (70,37%)	187 (98,9%)	2 (1,1%)
	рандом (16-бит)	101 (53,43%)	181 (95,76%)	8 (4,2%)
	S-блок Хейса (16 бит)	132 (69,48%)	186 (98,35%)	3 (1,65%)
	рандом (32-бита)	114 (60,04%)	187 (98,9%)	2 (1,1%)
	S-блок Хейса (32 бит)	133 (70,37%)	187 (98,9%)	2 (1,1%)
Калина	Полная версия	135 (71,43%)	186 (98,4%)	3 (1,65%)
	рандом (16-бит)	107 (56,6%)	179 (94,7%)	10 (5,3%)
	S-блок Хейса (16 бит)	130 (68,78%)	186 (98,35%)	3 (1,65%)
	рандом (32-бита)	122 (64,55%)	182 (96,3%)	7 (3,7%)
	S-блок Хейса (32 бит)	136 (71,95%)	187 (98,9%)	2 (1,1%)
Мухомор	Полная версия	123 (65,08%)	185 (97,9%)	4 (2,2%)
	рандом (16-бит)	87 (46,03%)	174 (92%)	15 (7,9%)
	S-блок Хейса (16 бит)	123 (65,08%)	174 (98,35%)	3 (1,65%)
	рандом (32-бита)	98 (51,85%)	183 (96,8%)	6 (3,2%)
	S-блок Хейса (32 бит)	126 (66,7%)	188 (99,45%)	1 (0,55%)

Результаты анализа табл. 8 показали прямую зависимость уровня «случайности» выходной последовательности при использовании *S-box*-ов на основе предварительной оценки основных критериев к формируемым нелинейным узлам замены уменьшенных моделей полных шифров.

С этой целью в работе представлены результаты исследований основных критериев оценки [24, 25]: сбалансированности $S_{СБ}$, нелинейности S_N, алгебраическая степень S_{DEG}, степень корреляционного иммунитета/критерия распространения S_{CIPC}, значение автокорреляции S_{AC} (см. табл. 9, 10). Таким образом, в математической форме основные требования к нелинейным узлам замены для симметричных криптографических средств защиты информации запишется в виде:

$$\left\{\begin{matrix}\{S_{СБ}, max(S_N), max(S_{DEG}), max(S_{CIPC}), min(S_{AC})\},\\ \{S_{СБ\_Л}, max(S_{N\_Л}), max(S_{DEG\_Л}),\}\\ \{max(S_{CIPC\_Л}), min(S_{AC\_Л})\}\end{matrix}\right\}.$$

Представленные результаты исследований основных показателей нелинейных узлов замен выдвигают предположение о необходимости дополнительной оценки выбранных строк из S-блока полного шифра для формирования нелинейного узла замены уменьшенной модели исследуемых алгоритмов симметричного шифрования.

S-box 16-битные последовательности Таблица 9

Название алгоритма	Сбалансированность	Нелинейность	Алгебраическая степень	Критерий распространения	Автокорреляция
AES(rand)	Нет	48	6	0	56
AES	Нет	32	6	0	**24**
ADE(rand)	Нет	28	5	0	16
ADE	Нет	32	6	0	22
Лабиринт(rand)	Нет	49	7	0	50
Лабиринт	Нет	32	6	0	**22**
Калина(rand)	Нет	45	7	0	44
Калина	Нет	32	6	0	**24**
Мухомор(rand)	Нет	28	5	0	16
Мухомор	Нет	32	6	0	22

S-box 32-битные последовательности Таблица 10

Название алгоритма	Сбалансированность	Нелинейность	Алгебраическая степень	Критерий распространения	Автокорреляция
AES(rand)	да	105	8	0	92
AES	да	64	7	0	**40**
ADE(rand)	да	56	7	0	34
ADE	да	64	7	0	42
Лабиринт(rand)	да	103	8	0	94
Лабиринт	да	64	7	0	**40**
Калина(rand)	да	105	8	0	90
Калина	да	64	7	0	**40**
Мухомор(rand)	да	56	7	0	28
Мухомор	да	64	7	0	42

Выводы

Полученные результаты в ходе исследования упрощенных версий БСШ для оценки доказуемой безопасности полномасштабных моделей шифров к атакам дифференциального и линейного криптоанализа на основе увеличения размера входа в шифр подтверждают возможность их использования. Адекватность результатов оценки свойств упрощенной модели БСШ зависит от выбора коэффициента масштабирования, который определяет свойства своих прототипов полных шифров. Выбор значения коэффициента должен быть пропорционален максимальному ресурсу вычислительных средств, используемых для проведения исследований. Для каждого блочного симметричного шифра (из числа известных итеративных БСШ) существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подста-новки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра, что дает возможность «сократить» количество итераций и увеличить скорость криптопреобразований. Вместе с тем, для сохранения всех свойств прототипов в упрощенных моделях необходимым условием их адекватности является использование mini-S-box с основными показателями эффективности нелинейных узлов замен (сбалансированность, нелинейность, автокорреляция) на уровне данных показателей полномасштабных шифров.

Литература

[1] И. Горбенко, «Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа», *Прикладная радиоэлектроника*, том 9, № 3, с. 312 – 320, 2010.

[2] В. Долгов, И. Лисицкая, «Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа», *монография*, Х., Издательство «Форт», 420 с., 2013.

[3] И. Лисицкая, «О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа», *Системи обробки інформації*, вип. 4 (94), с. 167-173, 2011.

[4] И. Лисицкая, «Методология оценки стойкости блочных симметричных шифров». [Электронный ресурс]. Режим доступа : https://cyberleninka-.ru/article/n/metodologiya-otsenki-stoykosti-blochnyh-simmetrichnyh-shifrov.

[5] И. Лисицкая, «Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс, и их уменьшенных моделей». [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/bolshie-shifry-sluchaynyepodstanovki-sravnenie-differentsialnyh-i-lineynyh-svoystv-shifrov-predstavlennyh-na-ukrainskiy-konkurs-i-ih.

[6] И. Лисицкая, К. Лисицкий, М. Родинко, И. Головко, И. Жариков, М. Корниенко, М. Кулеба, «Эксперементальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайности», *Радіоелектроніка, інформатика, управління*, № 1, с. 129 – 141, 2017.

[7] И. Лисицкая, А. Настенко, «Большие шифры – случайные подстановки», *Межведомственный научн. технический сборник «Радиотехника»*, вып. 166, с. 50–55, 2011.

[8] Л. Сорока, А. Кузнецов, И. Московченко, С. Исаев, «Исследование дифференциальных свойств блочно-симметричных шифров», *Системи обробки інформації*, вип. 6 (87), с. 286-295, 2010.

[9] И. Лисицкая, А. Кузнецов, С. Исаев, «Линейные свойства блочных симметричных шифров, представленных на украинский конкурс», *Прикладная радиоэлектроника: научно-техн. журнал*, том 10, № 2, с. 135-140, 2011.

[10] И. Лисицкая, Т. Гриненко, С. Бессонов, «Анализ дифференциальных и линейных свойств шифров rijndael, serpent, threefish при 16-битных входах и выходах», *Восточно-Европейский журнал передовых технологий*, с. 50-54, 2015.

[11] В. Долгов, Р. Олейников, А. Большаков, «Криптографические свойства уменьшенной версии шифра «Калина»», *Прикладная радиоэлектроника*, том 9, № 3, с. 349-354, 2010.

[12] И. Лисицкая, О. Олешко, С. Руденко, Е. Дроботько, А. Григорьев, «Криптографические свойства уменьшенной версии шифра Мухомор», *Збірник наукових праць*, К., с. 31-42, 2010.

[13] А. Кузнецов, Р. Сергиенко, А. Наумко, «Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption)», *Прикладная радиоэлектроника*, том 6, № 2, с. 241-249, 2007.

[14] R. Oliynykov, I. Gorbenko, V. Dolgov, V. Ruzhentsev, «Results of Ukrainian national public cryptographic competition», *Tatra Mt. Math*, Publ. 47, pp. 99–113, 2010.

[15] В. Долгов, Р. Олейников, А. Большаков, А. Григорьев, Е. Дробатько, «Криптографичекие свой-

ства уменьшенной версии шифра Калина», *Прикладная радиоэлектроника,* том 9, № 3, с. 349–354, 2010.

[16] G. Piret, F.-X. Standaert, «Provable security of block ciphers against linear cryptanalysis: a mission impossible?», *Designs, Codes and Cryptography*, v. 50, N 3, p. 325 – 338, 2009.

[17] B. Collard, F.-X. Standaert, «Experimenting linear cryptanalysis», *Advanced Linear Cryptanalysis,* v.116, p. 90-117, 2011.

[18] L. Knudsen, «Practically Secure Feistel Ciphers», *Proc. Fast Software Encryption*, Cambridge, V. 809, p. 211-221, 1994.

[19] І. Горбенко, В. Долгов, Р. Олійников, «Перспективний блоковий симетричний шифр «КАЛИНА». Основні положення та специфікація», *Прикладная радиоэлектроника*, том 6, № 2, с. 195-208, 2007.

[20] І. Горбенко, В. Долгов, Р. Олійников, «Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація», *Прикладная радиоэлектроника*, том 6, № 2, с. 147-157, 2007.

[21] С. Головашич, «Спецификация алгоритма блочного симметричного шифрования «Лабиринт»», *Прикладная радиоэлектроника,* том 6, № 2, с. 230-240, 2007.

[22] И. Лисицкая, «Сравнение по эффективности суперблоков некоторых современных шифров», *Радіоелектроніка, інформатика, управління*, № 1, с. 37-44, 2012.

[23] И. Лисицкая, И. Ставицкий, «32-х битная мини-версия блочного симметричного алгоритма криптографического преобразования информации «Мухомор». Оценка максимального значения полного дифференциала», *Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика,* № 7 (102), вып.18/1, с. 177-186, 2011.

[24] І. Горбенко, О. Потій, Ю. Ізбенко, «Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму Rijndael (FIPS 197)», *Радиотехника. Всеукраинский межведомственный научно-технический сборник*, № 126, с. 132-138, 2004.

[25] А. Потий, Ю. Избенко, «Обоснование выбора метода построения криптографически стойких булевых функций», *Всеукр. начно-тех. сборник «Радио-техника»*, Харьков, вып. 126, с. 132 – 137, 2002.

УДК 681.3.06 (045)

Євсеєв С. П., Остапов С.Е., Корольов Р.В. Використання міні-версій для оцінки стійкості блоково-симетричних шифрів

Анотація. *Розвиток криптології в еру високих технологій тісно пов'язаний з формуванням нових підходів і методологій, що дозволяють оцінити стійкість використовуваних блокових симетричних шифрів (БСШ) до основних видів атак лінійного і диференціального криптоаналізу, з огляду на основні вимоги щодо швидкодії криптоперетворень і енергетичні витрати на реалізацію. Запропонована в 2010 році нова ідеологія оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного аналізу науковцями кафедри БІТ ХНУРЕ під керівництвом професора Горбенка І.Д. орієнтована на використанні очікуваних показників стійкості великих шифрів на основі аналізу показників зменшених їх версій з одного боку, і розвинену на основі вивчення властивостей і показників випадкових підстановок і зменшених моделей шифрів, що розглядаються як підстановчі перетворення, з іншого боку, концепції визначення показників стійкості БСШ до атак диференціального та лінійного криптоаналізу. Для подолання труднощів аналізу повномасштабних моделей (алгоритмів) шифрування пропонується розробляти і досліджувати показники зменшених моделей прототипів (використовуються міні-версії 16-ти біт), для яких наявних обчислювальних можливостей достатньо. Однак питання використання міні-версій для оцінки криптостійкості повних шифрів підтримується не всіма вченими. Для оцінки використання зменшених моделей на основі запропонованої методології в статті наводяться результати досліджень на основі міні-версій (16-ти біт і 32-х біт) алгоритмів Rijndael, шифрів Лабіринт, Калина, Мухомор, ADE, використовуваних в якості експериментального підтвердження правильності запропонованої методології і концепції оцінки, аналізуються основні показники S-блоків міні-версій.*

Ключові слова: *блоково-симетричні шифри, зменшені моделі БСШ, криптостійкість.*

Yevseiev S., Ostapov S., Korolev R. Use of mini-versions to evaluate the security of block-symmetric ciphers

Abstract. *Development of cryptology in the era of high technologies is closely connected with the formation of new approaches and methodologies that allow us to evaluate the security of the used block symmetric ciphers (BSC) to the main types of attacks of linear and differential cryptanalysis, taking into account the basic requirements for the speed of crypto-transformations and energy costs for implementation. Proposed in 2010 a new ideology of assessing the durability of block symmetric ciphers to attacks of differential and linear analysis by the scientists of the Department of BIT KhNURE under the guidance of Professor I. Gorbenka. Is oriented on the use of expected indicators of the durability of large ciphers based on the analysis of the indicators of their reduced versions on the one hand and developed on the basis of studying the properties and indicators of random substitutions and reduced models of ciphers considered as substitution transformations, on the other hand, differential and linear cryptanalysis. To overcome the difficulties of analyzing full-scale cryptographic models (algorithms), it is proposed to develop and study indicators of reduced prototype models (16-bit mini versions are used), for which the available computing capabilities are sufficient. However, the issue of using mini-versions to assess the cryptographic strength of full ciphers is not supported by all scientists. To assess the use of reduced models on the basis of the proposed methodology, the article presents the results of studies based on the mini versions (16 bit and 32 bits) of the Rijndael algorithms, Labirint, Kalina, Mukhomor cipher, ADE, used as experimental confirmation of the correctness of the proposed methodology And evaluation concepts, the main indicators of S-blocks of mini versions.*

Key words: *block-symmetric ciphers, reduced BSC models, cryptographic security.*

Отримано *18 червня 2017 року*, затверджено редколегією *6 липня 2017 року*