УДК 621.391:519.2:519.7

А. А. Кастенко

ПОКАЗАТЕЛИ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ УКРАИНСКИХ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

В статье представлены результаты сравнения статистических свойств шифров, представленных на украинский конкурс по выбору стандарта блочного симметричного шифрования, а также дополнительно обоснована гипотеза о том, что малые модели блочных симметричных шифров повторяют свойства прототипов.

Ключевые слова: *блочный симметричный шифр, статистическая безопасность, корреляционные свойства, лавинный эффект, степень полноты, степень строгого лавинного критерия, степень лавинного эффекта.*

1. Введение

Исследования, о которых идет речь в данном докладе, относятся к области безопасности информационных технологий. Современный уровень развития и внедрения в жизнь общества информационных технологий делает очень актуальной задачу обеспечения конфиденциальности информации. На данный момент основным механизмом предоставления услуги конфиденциальности являются алгоритмы блочного симметричного шифрования и передовые в освоении информационных технологий страны перешли или развернули активную работу по переходу на новые стандарты шифрования с повышенными гарантиями стойкости. По этому пути пошла и Украина. В докладе приводятся результаты оценки показателей статистической безопасности шифров, представленных на украинский конкурс.

2. Постановка задачи

Исследование свойств полных версий блочных симметричных шифров является технически сложной задачей, в виду большой размерности блоков открытых текстов, шифртекстов и ключей. В связи с этим разработаны новые подходы, одним из которых является исследование шифров с помощью их малых моделей. Задачей является подтвердить целесообразность и допустимость исследования больших моделей шифров на основе их малых моделей, а также в целом определить свойства шифров, разработанных украинскими учеными и сравнить их с другими алгоритмами, являющимися общепризнанными лидерами в области блочного симметричного шифрования.

3. Основная часть

3.1. Анализ литературы по теме исследования. Как показывает анализ [1], в основе всех известных подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежит процедура определения максимума среднего значения дифференциальной вероятности (MADP) для всего шифра и максимума среднего значения вероятности линейного корпуса (MALHP), при этом полученные оценки этих показателей в разных работах отличаются в значительных пределах.

Однако проверить на практике достоверность приведенных утверждений не представлялось вычислительно возможным, в виду больших размерностей блоков и ключей в современных блочных симметричных шифрах.

Предложенный в работах [2—5 и др.] подход, основанный на изучении и исследовании криптографических свойств уменьшенных версий шифров, позволил преодолеть вычислительные ограничения, и оказалось, что результаты экспериментов не подтвердили доказанные положения и теоремы.

В работах [6, 7] было показано, что большие версии шифров при использовании их в режиме зашифрования укороченных (16-битных и 32-х битных) блоков данных, так же, как и их малые модели, повторяют законы распределения вероятностей переходов *XOR* таблиц и таблиц смешений линейных аппроксимаций, свойственные соответствующим законам распределения вероятностей случайных подстановок. В продолжение развития этого направления, в настоящей работе представлены материалы по дополнительному обоснованию справедливости гипотезы о том, что малые модели шифров повторяют свойства больших моделей, а так же то, что большие модели шифров тоже являются случайными подстановками. Теперь сравниваются между собой корреляционные характеристики ряда современных шифров и их уменьшенных моделей.

3.2. Результаты исследований. Приводятся результаты вычислительных экспериментов по оценке

показателей статистической безопасности, в качестве которых выступают:

— среднее число выходных битов, которые изменяются, когда изменяется один входной бит (лавинный эффект);

— степень полноты (d_c);

— степень лавинного эффекта (d_a);

— степень строгого лавинного критерия (d_{sa});

— для шифров, представленных на украинский конкурс: Лабиринт, Калина, Мухомор и ADE и ряда других современных шифров. Рассматриваются большие шифры и их малые модели.

Результаты, полученные в ходе исследований, свидетельствуют о том, что малые модели шифров, представленных на украинский конкурс, а также всемирно известных Rijndael, Serpent и ГОСТ 28147-89 практически повторяют корреляционные свойства своих прототипов. Таким образом, подтверждается гипотеза о том, что можно построить малые модели шифров, которые будут практически повторять показатели случайности полных версий шифров. Следовательно, выводы, полученные для малых моделей, можно переносить на большие версии шифров. В частности, это касается вывода о том, что и малые и большие шифры асимптотически приобретают свойства случайных подстановок.

Полученные результаты показывают, что корреляционные показатели являются еще одним из способов убедиться, что современные шифры после некоторого начального (как правило, небольшого) количества циклов зашифрования приобретают свойства случайных подстановок. Корреляционные показатели по зависимости их значений от количества циклов зашифрования практически повторяют результаты, полученные ранее при изучении дифференциальных и линейных свойств малых и больших моделей шифров [2—7].

Результаты исследований так же показывают, что три из четырех шифров, представленных на украинский конкурс, продемонстрировали более высокие криптографические показатели, чем признанный лидер блочного симметричного шифрования — шифр AES (Rijndael). Только шифр ADE не прошел тест по лавинным характеристикам из-за дефекта в его конструкции, хотя по остальным показателям случайности он не хуже AES.

Литература

1. Горбенко І. Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [Текст] / І. Д. Горбенко, **В. И. Долгов**, И. В. Лисицкая, Р. В. Олейников // Прикладная радиоэлектроника. — 2010. — Т. 9, № 3. — С. 212—320.
2. Долгов В. И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт [Текст] / **В. И. Долгов**, И. В. Лисицкая, А. В. Григорьев, А. В. Широков // Прикладная радиоэлектроника. — 2009. — Т. 8, № 3. — С. 283—289.
3. Долгов В. И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES [Текст] / **В. И. Долгов**, А. А. Кузнецов, Р. В. Сергиенко, О. И. Олешко // Прикладная радиоэлектроника. — 2009. — Т. 8, № 3. — С. 252—257.
4. Долгов В. И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс [Текст] / **В. И. Долгов**, А. А. Кузнецов, С. А. Исаев // Электронное моделирование. — 2011. — Т. 33, № 6. — С. 81—99.
5. Кузнецов А. А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс [Текст] / А. А. Кузнецов, И. В. Лисицкая, С. А. Исаев // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2. — С. 135—140.
6. Лисицкая И. В. Большие шифры — случайные подстановки [Текст] / И. В. Лисицкая, А. А. Настенко // Межведомственный научн. технический сборник «Радиотехника». — 2011. — Вып. 166. — С. 50—55.
7. Лисицкая И. В. Дифференциальные свойства шифра FOX [Текст] / И. В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2. — С. 122—126.

ПОКАЗНИКИ СТАТИСТИЧНОЇ БЕЗПЕКИ УКРАЇНСЬКИХ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

А. О. Настенко

У статті представлені результати порівняння статистичних властивостей шифрів, представлених на український конкурс з вибору стандарту блокового симетричного шифрування, а також додатково обґрунтована гіпотеза про те, що малі моделі блокових симетричних шифрів повторюють властивості прототипів.

Ключові слова: блочний симетричний шифр, статистична безпека, кореляційні властивості, лавинний ефект, ступінь повноти, ступінь суворого лавинного критерію, ступінь лавинного ефекту.

***Андрій Олександрович Настенко**, аспірант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, **тел.: (097) 398-22-45, e-mail: andreww7865@yandex.ru**.*

INDICATORS OF STATISTICAL SECURITY OF THE UKRAINIAN SYMMETRIC BLOCK CIPHERS

A. Nastenko

The paper presents the results of a comparison of the statistical properties of ciphers submitted to the Ukrainian competition for a new standard of symmetric block encryption. Also substantiated the hypothesis that small models of symmetric block ciphers repeat prototype properties.

Keywords: symmetric block cipher, the statistical security, correlation properties, avalanche effect, the degree of completeness, the degree of strict avalanche criterion, the degree of avalanche effect.

***Andrey Nastenko**, graduate student of Department of security of informational technologies, Kharkiv national university of radioelectronics, **tel.: (097) 398-22-45, e-mail: andreww7865@yandex.ru**.*