УДК 621. 3.06

УТОЧНЁННЫЕ ПОКАЗАТЕЛИ ПРИХОДА ШИФРОВ К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ

И.Д. ГОРБЕНКО, В.И. ДОЛГОВ, К.Е. ЛИСИЦКИЙ

Представляются уточнённые данные по оценке динамических показателей перехода современных шифров к состоянию случайной подстановки за счёт учёта маловероятных активизаций входов.

Ключевые слова: подстановка, активный S-блок, состояние случайной подстановки, динамические показатели шифров.

ВВЕДЕНИЕ

В наших работах по изучению динамических показателей прихода шифров к состоянию случайной подстановки [1–3], мы искали минимальное число активных S-блоков, позволяющих осуществить этот переход. Анализ, однако, показал, что существует возможность активизации меньшего числа S-блоков, чем рассмотрено в работах [1–3]. Мы сосредоточили внимание в наших работах на наиболее вероятных переходах. В то же время существуют пускай даже маловероятные переходы, но, как оказалось, они позволяют шифрам прийти к случайной подстановке при большем числе циклов, чем те, которые были определены при использовании наиболее вероятных переходов. Они, конечно, должны быть учтены при оценке динамических показателей шифров.

В этой работе мы приводим дополнительные обоснования по оценке минимального числа циклов, после которых шифры приходят к состоянию случайной подстановки.

1. ПРИХОД ШИФРОВ К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ ПРИ МАЛОВЕРОЯТНЫХ АКТИВИЗАЦИЯХ ВХОДОВ

Мы начнём с лидера среди современных блочных симметричных шифров алгоритма **Rijndael**.

При оценке динамических свойств прихода к состоянию случайной подстановки шифра Rijndael в [1–3] мы определяли минимальное число S-блоков на первом цикле преобразования этого шифра в виде одного байта, позволявшего активизировать один S-блок первого цикла. В последующем после МДР преобразования (MixColumns), использованного при построении цикловой функции этого шифра, активизировалось сразу четыре S-блока, т.е. на два цикла приходилось пять активизированных S-блоков. Однако эти же пять S-блоков можно активизировать, используя не один активный байт входа, а сразу четыре. Как показано в [4], МДР преобразование позволяет при четырёх активных байтах входа получить на выходе с вероятностью $2^{-23,983}$ один активный байт. Тогда эти четыре байта будут делать активными все четыре S-блока первого цикла, которые за счёт МДР преобразования первого цикла (с коэффициентом ветвления 5) хоть и с весьма малой вероятностью будут активизировать только один S-блок второго цикла, так что на два цикла и в этом случае будет приходиться пять активных S-блоков. Тогда в первом случае четыре активных S-блока второго цикла с учетом преобразования ShiftRow и MixColumns, будут уже активизировать в следующем третьем цикле все шестнадцать его S-блоков (ShiftRow расставляет выходы S-блоков по одному в каждой колонке). В результате на трёх циклах, как и указывалось в наших работах, становится активным 1 + 4 + 16 = 21 S-блок. В это же время во втором случае в третьем цикле будет активизироваться (за счёт МДР преобразования с коэффициентом ветвления 5) только четыре S-блока третьего цикла. Получается, что во втором случае число активизируемых S-блоков меньше, чем при активизации одного входного байта (в этом случае получаем 4 + 1 + 4 = 9 S-блоков), а на четырёх циклах число активных S-блоков будет 25. В результате шифр приходит к состоянию случайной подстановки и по дифференциальным и по линейным показателям за четыре цикла, а не за три, как указано в работе [3]. Именно четыре цикла прихода шифра Rijndael к состоянию случайной подстановки определяют и сами разработчики шифра [5].

Шифр Калина-128. В этом случае необходимо было рассмотреть и активизацию входа шифра сразу восемью байтами. Тогда на первом цикле имеем восемь активных S-блоков, на втором – один (вероятность перехода восьми активных входов операции MixColumns в одноблочный активный выход равна $2^{-55,9}$ [4]), на третьем ещё восемь, на четвёртом – все шестнадцать. Шифр для этой ситуации приходит гарантировано к случайной подстановке как по дифференциальным, так и по линейным показателям тоже за четыре цикла (8 + 1 + 8 + 16 = 33).

Шифр FOX-64. Здесь, как отмечено в [3], функция f32 внутреннего уровня включает в себя два слоя из четвёрок байтовых S-блоков с промежуточной рассеивающей частью, представляющей собой линейную 4×4-мультиперестановку в поле $GF(2^8)$, и три промежуточных сложения с цикловыми подключами [13]. В результате в

первом цикле активизируется минимум пять S-блоков (один S-блок первого слоя и четыре второго или четыре S-блока первого слоя и один второго).

Далее в первом случае продолжением может быть снова пять S-блоков (вероятность двух переходов в один цикл получается равной $2^{-47,966}$), так что в этом случае имеем 5 + 5 + 5 = 15 активных S-блоков на три цикла.

Во втором случае вероятность на трёх циклах получить третий переход в один активный S-блок уже равна $2^{-71,949}$ – это уже невероятное событие). Но зато хоть и с малой вероятностью возможны переходы в два и более активных S-блоков, так что здесь имеем на три цикла 5 + 5 + 6 = 16 активных S-блоков.

Если считать, что внешний уровень конструкции шифра (схема Лэя Мэсси) позволяет удвоить результат для активных S-блоков (для трёх циклов имеем минимум 30 активных S-блоков), приходим к выводу, что для прихода шифра Шифр FOX-64 к случайной подстановке достаточно трёх циклов и по дифференциальным и по линейным показателям: $2^{58} = 2^{-4k}$ и, следовательно, $k_{\min} = 14{,}5$ (2^{-4} – показатель δ-равномерности S-блоков шифра FOX [10]); $2^{58} = 2^{k-1}\,(2^{-4})^k$ имеем $k_{\min} = 19{,}3$ (2^{-4} – показатель нелинейности S-блоков шифра FOX [10]).

Шифр FOX-128. В 128-битном шифре FOX **в** функции f64 внутреннего уровня применяется матричное умножение на МДР матрицу 8×8 и опять двухслойное нелинейное преобразование. Поэтому на первом цикле имеем девять активных S-блоков (1 + 8 или 8 + 1). На втором цикле и в первом и во втором случае будет снова девять активных S-блоков (вероятность перехода в МДР преобразовании восьми активных байтов входа в один, как и в Калине, здесь равна $2^{-55,9}$, а дважды такое событие может произойти с вероятностью $2^{-111,8}$). На третьем цикле в первом случае имеем снова девять активных S-блоков (ещё один переход $1 \to 8$), а во втором – переход $8 \to 1$ уже невероятен, и здесь можно ожидать, скорее всего, в МДР преобразовании переходы в четыре и более активных байтов. Итак, на трёх циклах минимальным числом S-блоков будет 9 + 9 + 9 = 27, и, следовательно, в этом случае с учётом удвоения за счёт преобразования внешнего уровня на двух циклах имеем 54-е активных S-блока. Здесь $2^{120} = 2^{-4k}$ и $k_{\min} = 30$; $2^{120} = 2^{k-1}\,(2^{-4})^k$ и $k_{\min} = 40$. Следовательно, для шифра FOX-128 $r_{\min} = 3$ и по дифференциальным и по линейным показателям.

Шифр Мухомор-128. Конструкция функции усложнения M-64 шифра Мухомор-128 содержит три SL преобразования, в каждое из которых входит слой нелинейных преобразований, реализуемый с помощью 4-байтовых S-блоков, и МДР преобразование, осуществляющее матричное умножение байтовых выходов четырех S-блоков (над полем) на квадратную матрицу, размера 4×4 (аналогичное преобразование выполняется в шифре Rijndael с помощью операции MixColumns, только там при умножении используется другой полином). На входе функции усложнения M-64 выполняется сложение 32-битных блоков данных по модулю 2^{32}. В предыдущей работе [3] отмечалось, что схема включения SL преобразований обеспечивает активизацию всех двенадцати S-блоков цикловой функции. Однако это не так. Все 12 S-блоков активизируются первым активным байтом или 4-байтовым сегментом, поступающим на вход левого первого по порядку следования SL преобразования. Но, если рассматривать ситуацию, когда активизируется второе по порядку SL преобразование, то один или более активных байтов, поступающих на вход этого SL преобразования активизируют от одного до четырёх его S-блоков, а также третье SL преобразование (первое по порядку прохождения преобразований SL преобразование не активизируется).

Если активизируются четыре байта на входе самого правого (второго по порядку прохождения) SL преобразования, то в этом SL преобразовании активизируются четыре S-блока, которые после МДР преобразования дают один активный байт и, следовательно, в третьем (по порядку прохождения) SL преобразовании активизируется один S-блок. Этот один S-блок формирует четыре активных байта левого 32-битного выходного блока данных цикловой функции, и они же, складываясь с одноблочным выходом правого SL преобразования, формируют четыре активных байта правого 32-битного выходного блока данных цикловой функции. Получается, что в формировании выхода левого полублока цикловой функции принимают участие пять S-блоков, а в формировании правого полублока цикловой функции принимают участие шесть S-блоков.

В результате для прихода к случайной подстановке функции усложнения M-64 одного цикла не хватает.

Второй цикл в рассматриваемом случае позволяет активизировать SL преобразования второго цикла по схеме 1 + 4 + 2 активных S-блока (можно ориентироваться на два маловероятных перехода МДР преобразований), что для левого и правого полублоков цикловой функции второго цикла даёт семь активных S-блоков. На два цикла в рассматриваемом случае приходиться минимум двенадцать активных S-блоков. Это два цикла прихода к состоянию случайной подстановки по дифференциальным показателям и три по линейным.

Если опять удваивать результат прохождения функции усложнения M-64 для того, чтобы оценить число активных S-блоков для всей цикловой функции шифра Мухомор, то приходим к результату: для одного цикла – 10 S-блоков, для двух циклов – 24 S-блока.

Для шифра Мухомор: $2^{-120} = 2^{-5k}$ и $k_{\min} = 24$; $2^{-120} = 2^{k-1}\,(2^{-5})^k$ и $k_{\min} = 30$ (2^{-5} – показатель

δ-равномерности и показатель нелинейности S-блоков шифра Мухомор). Это означает, что шифр Мухомор-128 приходит к случайной подстановке по линейным показателям за три цикла ($r_{\min}$.= 3).

Шифр Мухомор-256. Конструкция функции усложнения М-128 шифра Мухомор-256 (вход в шифр 256 битов) состоит из восьми SL преобразований [16].

Опять рассмотрим активизацию самого правого 4-байтового блока данных, поступающих на правое SL преобразования первой линейки SL преобразований. Сразу рассмотрим все четыре байта входа этого SL преобразования активными. Как и в предыдущем случае имеем все четыре S-блока этого преобразования активными. На выходе SL преобразования один активный байт. В результате этот активный байт активизирует один S-блок первого SL преобразования второй линейки SL преобразований и далее идёт цепочка 4 + 1 + 4 + 4 (событие более двух переходов $4 \to 1$, или второй переход $4 \to 1$ или второй переход $4 \to 3$ это практически невозможные события). Это, если не учитывать дополнительных обратных связей. Дополнительные обратные связи позволяют для первого 32-битного выхода получить оценку для числа активных S-блоков, участвующих в его формировании в виде 4 + 1+ 4 + 4 + 4 = 17. Для второго 32-битного блока – 4 + 1 + 4 + 9 + 13 = 31 и т.д. Минимальным значением является 17. С учётом удвоения (за счёт преобразований внешнего уровня) получается 34 S-блока. Будем считать, что второй цикл даёт 33 активных S-блока, а с учётом удвоения – 66 активных S-блоков.

Для шифра Мухомор-256: $2^{-248} = 2^{-5k}$ и $k_{\min} = 49{,}6$; $2^{-248} = 2^{k-1}(2^{-5})^k$ и $k_{\min} = 62$ (2^{-5} – показатель δ-равномерности и показатель нелинейности S-блоков шифра Мухомор).

В результате шифр будет выходить к показателям случайной подстановки за два цикла и с показателями δ-равномерности равным 8-ми, 10-ти, 12-ти, 16-ти и даже 20-ти (при δ = 16 минимально необходимое число S-блоков есть 30).

Белорусский шифр имеет в цикловой функции 28 блоков, из которых активизируется на первом цикле минимум 10–18 S-блоков, и, как отмечено в [3], шифр приходит к состоянию случайной подстановки за два цикла.

С данными по остальным шифрам можно согласиться.

2. СВОДКА УТОЧНЁННЫХ РЕЗУЛЬТАТОВ

С учетом уточнённых данных мы теперь снова приведём сводку полученных результатов. Она оформлена в виде табл. 1 и табл. 2.

Практически изменения коснулись только шифров Rijndael, Калина, и функций усложнения шифров Мухомор-128 и Мухомор-256. Новые данные отличаются от старых увеличением числа циклов выхода шифров к состоянию случайной подстановки на один цикл. Для нас важно, что известные современные шифры, претендующие на лидерство, как, оказалось, требуют для выхода к случайной подстановке трёх и более циклов.

Таблица 1

Минимальное число циклов для выхода шифра по дифференциальным показателям к стационарному состоянию случайной подстановки

Шифр	$r_{\min}$
Rijndael-128	4
Калина-128	4
FOX-64	3
FOX-128	3
ГОСТ 28147-89	9
Мухомор-128	2
Мухомор-256	2
Serpent	3
Лабиринт	i
Шифр с цикловой функцией М-64	2
Шифр с цикловой функцией М-128	2

Таблица 2

Минимальное число циклов для выхода шифра по линейным показателям к стационарному состоянию случайной подстановки

Шифр	$r_{\min}$
Rijndael-128	4
Калина-128	4
FOX-64	3
FOX-128	3
ГОСТ 28147-89	9
Мухомор-128	3
Белорусский шифр	2
Serpent	3
Лабиринт	i
Шифр с цикловой функцией М-64	2
Шифр с цикловой функцией М-128	2

ВЫВОДЫ

Общим выводом можно отметить, что все известные современные шифры имеют число циклов выхода к состоянию случайной подстановки 3 и более.

Как показывает анализ, все известные конструкции цикловых функций не ориентированы на активизацию всех S-блоков первого цикла.

Отдельно можно выделить блочный шифр из белорусского стандарта и разработки шифров Мухомор. Они позволяют по нашим данным осуществить переход к состоянию случайной подстановки за два цикла.

Возникает интересный вопрос. А можно ли построить шифр, который становился бы случайной подстановкой уже с первого цикла? Чего это будет стоить? По видимому, нужно строить первый цикл не привязываясь к подобию всех цикловых преобразований. Мы на него постараемся ответить в нашей следующей работе.

Литература

[1] *Gorbenko I.D., Lisitskiy K.E., Denisov D.S.* (2014). On Ciphers Coming to a Stationary State of Random Substitution. Universal Journal of Electrical and Electronic Engineering, 2, 206–215. doi: 10.13189/ujeee.2014.020409.

[2] *Горбенко И.Д.* О динамике прихода блочных симметричных шифров к случайной подстановке / И.Д. Горбенко, Е.К. Лисицкий // Радиотехника. Всеукр. межвед. научн.-техн. сб. – 2014. – Вип.176. – С. 27–39.

[3] *Лисицкий К.Е.* Динамические показатели прихода блочных шифров к состоянию случайной подстановки / К.Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014. – 60 с.

[4] *Руженцев В.И.* О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов / В.И. Руженцев // Прикладная радиоэлектроника. – 2013. – Т. 12. – № 2. – С. 215–219.

[5] *J. Daemen and V. Rijmen.* AES Proposal: Rijndael. 1st AES Conference, California, USA, 1998. http://www.nist.gov/aes.

Поступила в редколлегию 8.07.2014

Горбенко Иван Дмитриевич, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета имени В.Н. Каразина, Главный конструктор ПАТ «ИИТ». Научные интересы: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.

Долгов Виктор Иванович, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета имени В.Н. Каразина. Научные интересы: методы криптоанализа, технологии блочного симметричного шифрования.

Лисицкий Константин Евгеньевич, фото и сведения об авторе см. на с. 212.

УДК 621. 391:519.2:519.7

Уточнені показники приходу шифрів до стану випадкової підстановки / І.Д. Горбенко, В.І. Долгов, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 213–216.

Надано уточнені дані щодо оцінки динамічних показників переходу сучасних шифрів до стану випадкової підстановки за рахунок обліку малоймовірних активізацій входів.

Ключові слова: підстановка, активний S-блок, стан випадкової підстановки, динамічні показники шифрів.

Табл.: 2. Бібліогр. 5 найм.

UDC 621. 391: 519. 2: 519.7

Ascertained indicators of ciphers coming to the state of random substitution / I.D. Gorbenko, V.I. Dolgov, K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 213–216.

The paper presents ascertained data on the evaluation of dynamic indicators of the transition of present-day ciphers to the state of random substitution with due account of unlikely input activation.

Keywords: substitution, active S-box, state of random substitution, dynamic indicators of ciphers.

Tab.: 2. Ref.: 5 items.