7. *Collard B. and Standaert F.-X.* A statistical saturation attack against the block cipher PRESENT // LNCS. 2009. V. 5473. P. 195–210.
8. *Шнайер Б.* Прикладная криптография: протоколы, алгоритмы и исходный код. М.: Альфа-книга, 2019. 1024 с.
9. *Alda F., Aragona R., Nicolodi L., and Sala M.* Implementation and improvement of the partial sum attack on 6-round AES // Physical and Data-Link Security Techniques for Future Communication Systems. Lecture Notes in Electr. Eng. 2016. V. 358. P. 181–195.
10. *Сорокин М. А., Пудовкина М. А.* О почти совершенных нелинейных преобразованиях и разделяющем свойстве мультимножеств // Прикладная дискретная математика. Приложение. 2019. № 12. С. 237–239.
11. *ElSheikh M. and Youssef A. M.* Integral cryptanalysis of reduced-round tweakable TWINE // LNCS. 2020. V. 12579. P. 485–504.
12. *Hebborn P., Lambin B., Leander G., and Todo Y.* Strong and tight security guarantees against integral distinguishers // LNCS. 2021. V. 13090. P. 362–391.
13. *Knudsen L. R. and Wagner D.* Integral cryptanalysis (extended abstract) // LNCS. 2002. V. 2365. P. 112–127.
14. *Kiryukhin V. A.* Related-key attack on 5-round Kuznyechik // Математические вопросы криптографии. 2020. Т. 11. № 2. С. 53–67.
15. *Ferguson N., Kelsey J., Schneier B., et al.* Improved cryptanalysis of Rijndael // LNCS. 2000. V. 1978. P. 213–230.
16. *D'Halluin C., Bijnens G., Rijmen V., and Preneel B.* Attack on six rounds of Crypton // LNCS. 1999. V. 1636. P. 46–59.
17. *Лось А. Б., Нестеренко А. Ю., Рожков М. И.* Криптографические методы защиты информации. М.: Юрайт, 2018, 473 с.
18. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4(18). С. 14–30.
19. *Панков К. Н.* Уточнённые асимптотические оценки для числа (n, m, k)-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
20. *Бабенко Л. К., Ищукова Е. А.* Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.

УДК 519.7 + 004.056.55 DOI 10.17223/2226308X/15/16

СВОЙСТВА XS-СХЕМ, СВЯЗАННЫЕ С ГАРАНТИРОВАННЫМ ЧИСЛОМ АКТИВАЦИЙ[1]

Д. Р. Парфенов, А. О. Бахарев, А. В. Куценко, А. Р. Белов, Н. Д. Атутова

Гарантированное число активаций является важной криптографической характеристикой, позволяющей получить оценку стойкости блочного шифра к разностному криптоанализу. В работе исследован один из алгоритмов (Агиевич, 2020) поиска числа гарантированных активаций XS-схем. Предложен подход к оптимизации существующего решения с помощью метода ветвей и границ, а также анализа специальных матриц, характеризующих XS-схему. Для нескольких шифров проведены вычислительные эксперименты, которые демонстрируют существенное

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2022-281.

ускорение вычисления гарантированного числа активаций по сравнению с известными подходами. С помощью оптимизированной версии алгоритма проведены численные эксперименты. На основе полученных данных выдвинуто несколько гипотез, часть из которых доказана. Например, обнаружен класс XS-схем, обладающих наименьшими гарантированными числами активации, а также доказано равенство гарантированного числа линейных и разностных активаций.

Ключевые слова: *гарантированное число активаций, XS-схемы, разностный криптоанализ, линейный криптоанализ, метод ветвей и границ.*

Введение

На сегодняшний день разностный (дифференциальный) криптоанализ является одним из наиболее эффективных статистических методов анализа симметричных блочных шифров. Данный подход основывается на анализе разностей открытых текстов и разностей соответствующих им шифртекстов.

XS-схемы представляют собой конструкции блочных шифров, основанные на использовании двух операций: X (поразрядное сложение двоичных слов по модулю 2) и S (подстановка слов с помощью нелинейных взаимно-однозначных отображений). Известно, что модели XS-схем покрывают достаточно широкий спектр блочных шифров, включая SM4, Skipjack и схему Фейстеля.

В данной работе рассматривается задача оптимизации поиска гарантированного числа активаций в XS-схемах, что позволит получить оценку эффективности разностного криптоанализа таких шифров.

Рассмотрим поле $\mathbb{F}$ характеристики 2. Раундовое преобразование XS-схемы задаётся следующим образом:

$$(a, B, c)[S] : \mathbb{F}^n \to \mathbb{F}^n, (x_1, x_2, \ldots, x_n) \longmapsto (x_2, x_3, \ldots, x_n, x_{n+1}),$$
$$x_{n+1} = (x_1, x_2, \ldots, x_n)B + S((x_1, x_2, \ldots, x_n)a)c,$$

где $a, c \in \mathbb{F}_2^n$; B — булева матрица.

Множество регулярных XS-схем распадается на классы эквивалентности относительно отношения подобия [1]. Выберем в качестве представителей классов XS-схемы, находящиеся в *первой канонической форме* [1]. Класс XS-схем однозначно определяется парой векторов a и b, где b — последний столбец матрицы B, которая является фробениусовой клеткой, когда XS-схема находится в первой канонической форме.

Для каждого шифра можно найти число активаций. Данная характеристика позволяет получить нижнюю оценку сложности разностного криптоанализа шифра.

Определение 1. *Активация* — получение на вход S-блока векторов с ненулевой разностью при различных входных векторах раунда.

Определение 2. *Гарантированное число активаций* — наименьшее число активаций по всем ненулевым разностям между входными векторами за заданное число раундов.

Отметим, что поиск связан с исследованием линейного кода определенного вида, который строится на основе рассматриваемого шифра. Для каждого шифра из класса XS-схем (схема находится в первой канонической форме) строится матрица $G = G(n, a, b, t)$ размерности $(t + n) \times 2t$ (подробнее см. в [1]).

Одним из подходов к поиску гарантированного числа активаций является алгоритм GNA [2]. Основная идея алгоритма — полный перебор разбиений матрицы G на G_0 и G_1 так, чтобы:

1) матрица G_0 содержала $k+1$ (k изначально известно) пар столбцов из G;
2) $\mathrm{rank}(G_0) < t+n-1$, где t — число раундов, n — размерность векторов a и b;
3) в матрице G_1 не было ни одного столбца, линейно зависимого от столбцов в G_0.

1. Оптимизация алгоритма вычисления гарантированного числа активаций

Существующий алгоритм при увеличении t и n работает весьма длительное время. Предложен способ оптимизации разбиения матрицы G, который существенно ускоряет алгоритм. Его основная идея строится на подходе, основанном на методе ветвей и границ, который является развитием метода полного перебора с отсечением подмножеств допустимых решений, заведомо не содержащих оптимальных решений.

Предлагается следующая интерпретация полного перебора. Рассмотрим двоичное дерево, в котором каждый лист соответствует некоторому разбиению пар столбцов матрицы G на матрицы G_0 и G_1. Корень дерева соответствует пустому множеству пар столбцов матрицы G. При переходе с i-го уровня на $(i+1)$-й переход к правому потомку соответствует добавлению $(i+1)$-й пары столбцов в матрицу G_0, а переход влево — в G_1. Таким образом, каждый узел дерева соответствует некоторому разбиению подмножества пар столбцов матрицы G на матрицы G_0 и G_1.

Если при обходе дерева обрабатываемый узел соответствует разбиению, которое не позволяет увеличить имеющуюся оценку k (в G_1 существует столбец, линейно зависимый от столбцов G_0), то все потомки данного узла также будут соответствовать разбиениям, в которых в G_1 существует столбец, линейно зависимый от столбцов G_0, и поэтому их можно не обрабатывать.

Кроме того, дополнительные критерии отсечения могут быть получены на основе следующего свойства матрицы G:

Лемма 1. Рассмотрим n подряд идущих пар столбцов из G, где n — размерность XS-схемы. Тогда первый столбец из $(n+1)$-й пары линейно зависим от столбцов из этих пар.

Для краткости формулировок введём следующее

Определение 3. Будем называть разбиение пар столбцов матрицы G на матрицы G_0 и G_1 «*неподходящим*», если в G_1 содержится столбец, линейно зависящий от столбцов матрицы G_0.

Сформулируем достаточные условия того, что разбиение является «неподходящим»:

Теорема 1. Пусть G_0 содержит n подряд идущих в G пар столбцов. Если выполнено одно из следующих условий, то такое разбиение является «неподходящим»:

1) в G_1 содержится пара с бóльшим порядковым номером, чем у последней из n подряд идущих пар;
2) a_1 и b_1 одновременно не равны 1.

Более того, возможно заранее обнаружить, что обрабатываемая ветвь неизбежно приведёт к «неподходящему» разбиению.

Следствие 1. Если для разбиения, заданного обрабатываемым узлом дерева, невозможно дополнить матрицу G_0 до $k+1$ пары столбцов без появления n подряд идущих в G пар столбцов, то все листья, являющиеся потомками этого узла, соответствуют «неподходящим» разбиениям.

Поскольку «неподходящее» разбиение не позволяет увеличить имеющуюся оценку k, все его потомки также заведомо не содержат оптимального решения. Это позволяет использовать теорему 1 и следствие из неё в качестве дополнительных критериев отсечения.

2. Тестирование

Для проверки предложенного решения на практике было произведено несколько тестовых запусков. Референсная реализация GNA [3] выполнена на Python. Для корректности сравнения оптимизированный вариант также выполнен на Python и использует те же библиотеки, что и референсная реализация GNA. В таблице приведено время работы существующего и предложенного алгоритма на XS-схемах, описывающих блочные шифры SMS4 (стандарт КНР GB/T 32907-2016), skipjackg-4 (стандарт США FIPS 185 EES) и beltWBL-4 (стандарт Республики Беларусь СТБ 34.101.31-2020). Для старого алгоритма приведено время работы до 25 раундов, поскольку для большего числа раундов вычисления заняли бы существенно больше времени.

Время работы для SMS4, skipjackg-4 и beltWBL-4, с

Кол-во раундов	SMS4		skipjackg-4		beltWBL-4	
	Сущ. алг.	Предл. алг.	Сущ. алг.	Предл. алг.	Сущ. алг.	Предл. алг.
20	60,0129	1,2929	131,3367	0,2681	67,303	0,8394
21	89,1743	0,8057	231,5267	0,2155	176,574	2,5539
22	132,9802	0,4689	644,076	0,5805	391,1274	3,4973
23	197,0892	0,264	1589,793	1,4337	994,2484	6,6221
24	735,1466	1,4642	2916,3251	1,117	1677,1016	4,5253
25	2555,2445	7,1559	7348,0468	2,6989	3183,5355	2,9505
26	—	4,3972	—	2,1177	—	11,3771
29	—	8,0172	—	8,2899	—	26,1846
32	—	14,217	—	12,983	—	196,2868
35	—	169,632	—	37,8486	—	388,0823

3. Приложение к линейному криптоанализу

В [1] упомянуто, что алгоритм может быть применён к оценке стойкости к линейному криптоанализу. Для того чтобы вычислить гарантированное число линейных активаций, необходимо вычислить гарантированное число разностных активаций дуальной схемы. Матрица схемы, дуальной к заданной схеме (a, B, c), получается с помощью транспонирования матрицы B и обмена местами значений векторов a и c — $(c^{\mathrm{T}}, B^{\mathrm{T}}, a^{\mathrm{T}})$.

Интересно посмотреть, каким образом могут быть взаимосвязаны гарантированные числа разностных и линейных активаций. При анализе результатов численных экспериментов мы заметили, что они совпадают. В свою очередь, это означает, что совпадают и первые канонические формы XS-схем, что в конечном итоге было доказано.

Теорема 2. Пусть (a, B, c) — XS-схема в первой канонической форме. Тогда первая каноническая форма дуальной схемы $(c^{\mathrm{T}}, B^{\mathrm{T}}, a^{\mathrm{T}})$ совпадает с (a, B, c).

4. Схемы с экстремальным гарантированным числом активаций

С помощью усовершенствованной версии алгоритма вычисления гарантированного числа активаций осуществлён полный перебор представителей классов регулярных XS-схем для различных n и вычислены максимальные и минимальные гарантированные числа активаций для различного числа раундов. При анализе результатов выявлен

класс схем, которые обладают минимальными гарантированными числами активации. Для них установлена и доказана зависимость гарантированного числа активаций от размерности и числа раундов.

Утверждение 1. Пусть (a, B, c) — XS-схема в первой канонической форме размерности n и $a + b = (1, 0, \ldots, 0)$. Тогда k-я активация происходит на раунде kn.

Данные схемы образуют класс потенциально наименее стойких схем.

Кроме того, исходя из результатов численных экспериментов, можно выдвинуть следующие гипотезы:

Гипотеза 1. У всех схем размерности n, кроме схем с минимальным гарантированным числом активаций, число раундов, необходимое для k активаций, не превышает $kn - (k - 1)$.

Гипотеза 2. XS-схемы, которые задаются парами векторов (a, b) и (b, a), имеют одинаковые гарантированные числа активации.

Заключение

В работе проанализирован алгоритм GNA [2] и предложен подход к оптимизации существующего решения. Предлагаемые изменения позволяют существенно ускорить вычисление гарантированного числа активаций, а также вычислять гарантированное число активаций для большего количества раундов, чем референсная реализация. Проведены численные эксперименты, вычислены гарантированные числа активации для всех схем размерности 7 и меньше. На основе полученных данных выдвинуто несколько гипотез, часть из которых доказана, в том числе равенство гарантированного числа разностных и линейных активаций.

В дальнейшем планируется продолжать исследования с целью поиска принципов построения криптографических примитивов на основе XS-схем с оптимальными гарантированными числами активаций. Возможными применениями являются шифры, хэш-функции и генераторы псевдослучайных чисел. Авторы заинтересованы также в исследовании возможности использовать sponge-функции для построения примитивов с переменной размерностью.

ЛИТЕРАТУРА

1. *Агиевич С. В.* XS-circuits in block ciphers // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 7–30.
2. *Агиевич С. В.* On the guaranteed number of activations in XS-circuits // Матем. вопр. криптогр. 2021. Т. 12. № 2. С. 7–20.
3. Реализация алгоритмов поиска гарантированного числа активаций. `https://github.com/agievich/xs`.