

**ОПТИМИЗАЦИЯ АЛГОРИТМА ВЫЧИСЛЕНИЯ
ГАРАНТИРОВАННОГО ЧИСЛА АКТИВАЦИЙ
В XS-СХЕМАХ
С ПОМОЩЬЮ МЕТОДА ВЕТВЕЙ И ГРАНИЦ**

**Д. Р. Парфенов, А. О. Бахарев,
А. В. Куценко (Новосибирск),
А. Р. Белов (Ярославль), Н. Д. Атутова (Новосибирск)**

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, схему Фейстеля.

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

Раундовое преобразование XS-схемы задаётся следующим образом:

$$(a, B, c)[S] : \mathbb{F}^n \rightarrow \mathbb{F}^n, (x_1, x_2, \dots, x_n) \mapsto (x_2, x_3, \dots, x_n, x_{n+1}),$$
$$x_{n+1} = (x_1, x_2, \dots, x_n)b + S((x_1, x_2, \dots, x_n)a).$$

Для каждого шифра можно найти число активаций — количество ненулевых разностей, попавших на вход S -блоков. Гарантированное число активаций шифра — наименьшее из всех минимальных чисел активаций. Данная характеристика позволяет получить нижнюю оценку сложности разностного криптоанализа шифра — метода, основанного на анализе разностей между парами открытых текстов и соответствующих им пар шифртекстов.

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 в [1]). Основная идея существующего алгоритма — полный перебор разбиений матрицы G на G_0 и G_1 , так чтобы:

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

Существующий алгоритм [2] при увеличении t и n работает весьма длительное время. Основная идея предлагаемой нами оптимизации 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.

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 $(i + 1)$ -ый, переход к правому потомку соответствует добавлению $(i + 1)$ -ой 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 .

Для краткости формулировок введём следующее определение.

Определение. 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 .

Если при обходе дерева обрабатываемый узел соответствует «неподходящему» разбиению, которое не позволяет увеличить имеющуюся оценку k , то все потомки данного узла также будут соответствовать «неподходящим» разбиениям, и поэтому их можно не обрабатывать.

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

Лемма. Рассмотрим n подряд идущие пары столбцов из G , где n — размерность XS-схемы. Тогда первый столбец из $(n + 1)$ -ой пары будет линейно зависящим от столбцов из предыдущих n подряд идущих пар.

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

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

- 1) Существует пара с большим порядковым номером, лежащая в G_1 ;
- 2) a_1 и b_1 одновременно не равны 1.

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

Утверждение. 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.

Для проверки предложенного решения на практике было произведено несколько тестовых запусков. Референсная реализация алгоритма выполнена на Python. Для корректности сравнения оптимизированный вариант также выполнен на Python и использует те же библиотеки, что и референсная реализация (<https://github.com/agievich/xs>). В таблице приведено время работы существующего и предложенного алгоритма на XS-схемах, описывающих блочные шифры SMS4 (стандарт КНР GB/T 32907-2016) и skipjackg-4 (стандарт США FIPS 185 EES).

Кол-во раундов	SMS4		skipjackg-4	
	Сущ. алг.	Предл. алг.	Сущ. алг.	Предл. алг.
20	60,0129	1,2929	131,3367	0,2681
21	89,1743	0,8057	231,5267	0,2155
22	132,9802	0,4689	644,076	0,5805
23	197,0892	0,264	1589,793	1,4337
24	735,1466	1,4642	2916,3251	1,117
25	2555,2445	7,1559	7348,0468	2,6989
26	-	4,3972	-	2,1177
29	-	8,0172	-	8,2899
32	-	14,217	-	12,983
35	-	169,632	-	37,8486

Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации номер 075-15-2022-281.

Список литературы

1. Агиевич С. В. XS-circuits in block ciphers // Матем. вопр. криптогр. — 2019. — 10:2. — С. 7—30
2. Агиевич С. В. On the Guaranteed Number of Activations in XS-circuits // Матем. вопр. криптогр. — 2021. — 12:2. — С. 7—20

DOI: 10.20948/dms-2022-87