В. А. Виткуп, О представлении S-блоков при реализации в блочных шифрах, *ПДМ. Приложение*, 2013, выпуск 6, 30–32

https://www.mathnet.ru/pdma120

Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

О ПРЕДСТАВЛЕНИИ S-БЛОКОВ ПРИ РЕАЛИЗАЦИИ В БЛОЧНЫХ ШИФРАХ

В. А. Виткуп

Рассматривается предложенный недавно способ разбиения S-блоков для защиты от атак по сторонним каналам. Известно, что для всех классов эквивалентности S-блоков, кроме одного, такое разбиение возможно. Доказано, что для этого одного класса не существует искомого разбиения.

Ключевые слова: *S-блок, векторные булевы функции, аффинная эквивалентность.*

Многие криптографические алгоритмы уязвимы к атакам по сторонним каналам, направленным на слабости в практической реализации алгоритма. В качестве мер противодействия используются методы, маскирующие входные данные так, чтобы вычисления не зависели от них в явном виде.

В [1] предложен следующий способ маскирующей реализации S-блока. Рассмотрим S-блок $n \times n$. Пусть $x = (x_1, \ldots, x_n)$, где $x_i \in \mathbb{Z}_2$. Рассмотрим векторную функцию $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $S = (f_1, \ldots, f_n)$, где $f_1, \ldots, f_n$ — булевы функции от n переменных. Разбиваем переменные x_i каждую на r булевых переменных: $x_i = \sum_{j=1}^{r} x_{ij}$. Пусть $v = (x_{11}, \ldots, x_{nr})$. Разбиваем функцию S на r векторных функций $S_i : \mathbb{Z}_2^{nr} \to \mathbb{Z}_2^n$ так, чтобы выполнялось $S(x) = \sum_i S_i(v)$. Такое разбиение векторной функции S обозначим $P(S)$.

Введём следующие условия для разбиения.

1. *Неполнота*: блок S_i не должен зависеть от переменных x_{ki}, $k = 1, \ldots, n$.

2. *Взаимная однозначность*: функция $S^* : \mathbb{Z}_2^{nr} \to \mathbb{Z}_2^{nr}$, $S^* = (S_1, \ldots, S_r)$, является взаимно однозначной.

Разбиение $P(S)$, удовлетворяющее этим двум условиям, называется *допустимым*.

Две векторных функции S и $\overline{S}$ называются *аффинно эквивалентными*, если существует пара невырожденных аффинных преобразований A и B, таких, что $S = B \circ \overline{S} \circ A$. Отношение аффинной эквивалентности разбивает множество всех взаимно однозначных S-блоков на непересекающиеся классы. Множество S-блоков 3×3 содержит 4 класса, $\mathcal{A}_1^3$, $\mathcal{Q}_1^3$, $\mathcal{Q}_2^3$, $\mathcal{Q}_3^3$. В таблице приведены их представители.

Класс	Представитель
$\mathcal{A}_1^3$	(x, y, z)
$\mathcal{Q}_1^3$	$(x, y, xy + z)$
$\mathcal{Q}_2^3$	$(x, y + xz, z + xy + xz)$
$\mathcal{Q}_3^3$	$(xy + xz + yz, x + y + xy + yz, x + z + yz)$

Теорема 1 [1]. Если для некоторой векторной функции существует допустимое разбиение, то для любой аффинно эквивалентной ей функции также существует допустимое разбиение.

Построить разбиение и добиться выполнения условия неполноты нетрудно; сложность представляет свойство взаимной однозначности, которое требует отдельной проверки для каждого полученного разбиения. Для классов $\mathcal{A}_1^3$, $\mathcal{Q}_1^3$ и $\mathcal{Q}_2^3$ допустимые разбиения найдены в работе [1]. Чтобы достигнуть взаимной однозначности, в функции из разбиения S-блока добавляются пары так называемых корректирующих слагаемых, комбинацией которых можно получить всевозможные разбиения $P(S)$, удовлетворяющие условию 1. Для S-блоков 3×3 существует всего 54 таких слагаемых.

Рассмотрим, например, S-блок $(x, y + xz, z + xy + xz)$ из класса $\mathcal{Q}_2^3$ и его разбиение $P(S)$, удовлетворяющее условию неполноты:

$$S_1(v) = (x_2, y_2 + x_2z_2 + x_2z_3 + x_3z_2, z_2 + x_2y_2 + x_2y_3 + x_3y_2 + x_2z_2 + x_2z_3 + x_3z_2);$$
$$S_2(v) = (x_3, y_3 + x_3z_3 + x_1z_3 + x_3z_1, z_3 + x_3y_3 + x_1y_3 + x_3y_1 + x_3z_3 + x_1z_3 + x_3z_1);$$
$$S_3(v) = (x_1, y_1 + x_1z_1 + x_1z_2 + x_2z_1, z_1 + x_1y_1 + x_1y_2 + x_2y_1 + x_1z_1 + x_1z_2 + x_2z_1).$$

Условие 2 не выполняется. Однако при добавлении следующей комбинации корректирующих слагаемых (выделены подчеркиванием) разбиение становится допустимым:

$$S_1(v)=(x_2,\ y_2+x_2z_2+x_2z_3+x_3z_2+\underline{z_2},\ z_2+x_2y_2+x_2y_3+x_3y_2+x_2z_2+x_2z_3+x_3z_2+\underline{y_3}+\underline{z_2});$$
$$S_2(v)=(x_3,\ y_3+x_3z_3+x_1z_3+x_3z_1+\underline{z_1},\ z_3+x_3y_3+x_1y_3+x_3y_1+x_3z_3+x_1z_3+x_3z_1+\underline{y_3}+\underline{z_1});$$
$$S_3(v)=(x_1,\ y_1+x_1z_1+x_1z_2+x_2z_1+\underline{z_1}+\underline{z_2},\ z_1+x_1y_1+x_1y_2+x_2y_1+x_1z_1+x_1z_2+x_2z_1+\underline{z_1}+\underline{z_2}).$$

Для класса $\mathcal{Q}_3^3$ допустимое разбиение так и не было найдено, а большой перебор комбинаций корректирующих переменных делает поиск трудным, поэтому в [1] авторы обозначили открытый вопрос: существует ли для S-блоков из класса $\mathcal{Q}_3^3$ допустимое разбиение?

Пусть $S = (f_1, \ldots, f_n)$, $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ и $P(S)$ — непосредственное разбиение S-блока S на r частей $S_i = (f_{1i}, \ldots, f_{ni})$. Рассмотрим векторную функцию $F = (f_{11}, \ldots, f_{n1}, \ldots, f_{1r}, \ldots, f_{nr})$. Будем говорить, что функция $C_F = (c_{11}, \ldots, c_{n1}, \ldots, c_{1r}, \ldots, c_{nr})$, $c_{ij} : \mathbb{Z}_2^{nr} \to \mathbb{Z}_2$ — *корректирующая функция* для F, если функция $F + C_F$ обладает следующими свойствами:

1) $f_i = \sum\limits_{j=1}^{r} (f_{ij} + c_{ij})$ для каждого $i = 1, \ldots, n$;
2) $f_{ij} + c_{ij}$ не зависит от переменных $x_{1j}, \ldots, x_{nj}$ для каждого $i = 1, \ldots, n$, $j = 1, \ldots, r$.

Пусть $k \in \{1, \ldots, nr\}$, $(i_1j_1, \ldots, i_kj_k)$ — набор индексов длины k из множества $\{11, \ldots, n1, \ldots, 1r, \ldots, nr\}$. Определим множество $C^k_{i_1j_1,\ldots,i_kj_k} = \{C_F : (f_{i_1j_1} + c_{i_1j_1}, \ldots, f_{i_kj_k} + c_{i_kj_k})$ — сбалансированная функция из $\mathbb{Z}_2^{nr}$ в $\mathbb{Z}_2^k\}$. Пусть $C = \bigcap\limits_{k} \bigcap\limits_{i_1j_1,\ldots,i_kj_k} C^k_{i_1j_1,\ldots,i_kj_k}$.

Теорема 2. Функция $F + C_F$ взаимно однозначна, если и только если $C_F \in C$.

Теорема 2 даёт алгоритм отыскания возможного допустимого разбиения, так как для любой функции $C_F \in C$ разбиение $S'_1 = (f_{11} + c_{11}, \ldots, f_{n1} + c_{n1}), \ldots, S'_r = (f_{1r} + c_{1r}, \ldots, f_{nr} + c_{nr})$ по теореме 2 является допустимым. Для S-блока из $\mathcal{Q}_3^3$ доказано, что множество C пусто. Следовательно, не существует допустимого разбиения данного S-блока, и доказана следующая

Теорема 3. Для S-блоков из класса $\mathcal{Q}_3^3$ не существует допустимого разбиения.

ЛИТЕРАТУРА

1. *Bilgin B., Nikova S., Nikov V., et al.*Threshold implementations of all 3x3 and 4x4 S-boxes // CHES 2012. LNCS. 2012. V. 7428. P. 76–91.

УДК 056.55

АЛГОРИТМ ВОССТАНОВЛЕНИЯ ОТКРЫТОГО ТЕКСТА ПО ШИФРТЕКСТУ В КРИПТОСИСТЕМЕ МАК-ЭЛИСА

А. К. Калужин, И. В. Чижов

Предлагается алгоритм неструктурной атаки на кодовую криптосистему Мак-Элиса с целью дешифрования сообщения, основывающийся на алгоритме Бернштейна — Ланг — Петерса и работающий быстрее любого другого существующего алгоритма неструктурной атаки. Тем самым сделан ещё один шаг в приближении к нижней оценке сложности таких алгоритмов, доказанной М. Финиазом и Н. Сендрие.

Ключевые слова: *криптосистема Мак-Элиса, неструктурные атаки, алгоритм Бернштейна — Ланг —Петерса, алгоритм Шабо — Канто.*

Рассматриваются неструктурые атаки на криптосистему с открытым ключом Мак-Элиса [1] с целью дешифрования сообщения. По сути, решается уравнение $m \cdot G + e = c$, где m и e неизвестны, а $\mathrm{wt}(e) = t$. При этом m — исходное сообщение, G — порождающая матрица кода (открытый ключ), e — вектор ошибки, c — вектор, который подвергается дешифрованию. Найдя вектор ошибки e, мы решим систему полностью, так как вектор m находится из системы линейных уравнений. Все наилучшие алгоритмы неструктурной атаки на систему Мак-Элиса (Штерна, Шабо — Канто и Бернштейна — Ланг — Петерса) основываются на одной идее: итеративно генерируются различные базисы кода и решается задача в предположении, что вектор ошибки e можно выразить через $2p$ (p — параметр алгоритмов) некоторых из зафиксированных векторов базиса.

В 2009 г. М. Финиаз и Н. Синдреир в работе [2] доказали нижнюю теоретическую оценку ожидаемого количества битовых операций, необходимых для дешифрования сообщения в криптосистеме Мак-Элиса. Для кодов Гоппы $(1024, 524, 50)$ (стандартные параметры криптосистемы Мак-Элиса) эта оценка равна $2^{59,9}$. Оценка идеальна и недостижима (в силу предположений при доказательстве). В то же время ожидаемое количество битовых операций, необходимых для дешифрования сообщения, закодированного с помощью этого кода, составляет:

1) для алгоритма Штерна – $2^{66,21}$;
2) для алгоритма Шабо — Канто – $2^{64,1}$;
3) для алгоритма Бернштейна — Ланг — Петерса – $2^{60,55}$.

То есть существующие алгоритмы уже вплотную приблизились к идеальной оценке ожидаемого количества битовых операций.

В работе представляется модификация алгоритма Бернштейна — Ланг — Петерса [3], которая уменьшает как ожидаемое количество итераций, так и ожидаемое количество битовых операций, выполняемых на одной итерации. Достигается это посредством следующих двух оптимизаций.

1) В алгоритме Бернштейна — Ланг — Петерса на каждой итерации фиксируется некоторый базис кода. Он получается из базиса кода, зафиксированного на предыдущей итерации, путём обмена местами c из первых k столбцов матрицы с c столбцами среди оставшихся, с дальнейшим применением модифицированного преобразования