УДК 681.3.06

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ БЛОЧНЫХ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ В ПОТОЧНЫХ ШИФРАХ

д.т.н., проф. Ю.В. Стасев, Ю.А. Избенко, к.т.н. Д.Е. Петрукович

Исследуется возможность применения блочных нелинейных преобразований в поточных шифрах, построенных над расширенным полем $GF(2^q)$.

Введение. Одной из составляющих схем симметричного шифрования являются поточные шифры (ПШ). В общем виде ПШ состоят из одного или нескольких линейных регистров сдвига (ЛРР) и нелинейной функции (НЛФ). Задачей НЛФ является внесение нелинейности в выходную последовательность ЛРР, поскольку сам по себе ЛРР является линейным устройством. В классической интерпретации ЛРР представляется в виде последовательности битовых ячеек, а в качестве нелинейных функций используют булевы функции; все арифметические операции выполняются в GF(2).

Анализируя последние разработки в области построения схем ПШ [1], можно констатировать отход от классической интерпретации их построения. Новая концепция построения ПШ подразумевает введение обобщенного регистра сдвига над полем $GF(2^q)$, где q – длина машинного слова, и использование в качестве НЛФ блочных нелинейных преобразований (блоков подстановок или S-блоков), более свойственных блочным шифрам, с выполнением всех арифметических операций в конечных полях. Очевидно, что немаловажным достоинством таких схем является увеличение производительности шифрования – если в классической интерпретации ПШ за один такт генерировал 1 бит шифрующей гаммы, то в новой интерпретации за тот же такт ПШ генерирует q бит.

Следует отметить, что применению нового подхода не предшествовал этап теоретического анализа и обоснования стойкости полученных конструкций. Повышение быстродействия схем спецпреобразований без обеспечения их стойкости делает нецелесообразным их применение. Поэтому **важным научным заданием** является исследование стойкости составных частей схем поточного шифрования, построенных над расширенным полем. **Целью данной статьи** является исследование возможности применения блочных нелинейных преобразований в ПШ, нахождение возможных путей повышения их стойкости.

Известно, что стойкость схем ПШ определяется, прежде всего, стойкостью нелинейных преобразований [2]. Поскольку основным ви-

дом атак на ПШ являются корреляционные атаки, является целесообразным рассмотрение корреляционных свойств нелинейных преобразований, основанных на использовании S-блоков.

При проведении корреляционных атак на схемы ПШ, выполненные в классической интерпретации, основываются на допущении, что выходная последовательность схемы {z} коррелирует с выходной последовательностью регистра {x}. Для описания и исследования корреляции данного рода моделируется поведение выходной последовательности регистра как последовательности, проходящей через некоторый канал. В качестве модели, имитирующей прохождение, рассматривается двоичный симметричный канал (ДСК) с некоторой вероятностью корреляции $p_к = 1 - p$, где $1 - p = P(x_i = z_i)$, p определено как вероятность перехода (вероятность ошибки) в ДСК, полагается $p = 1/ - \delta$, где $0 < \delta < 0{,}5$. Следовательно, вероятность корреляции $p_к$ для данных схем имеет вид

$$p_к = 1 - p = 1 - (1/2 - \delta) = 1/2 + \delta. \quad (1)$$

Как видно из (1), вероятность корреляции всегда меньше 1.

Рассмотрим блочные нелинейные преобразования. Пусть мы имеем некоторый S-блок, осуществляющий отображение $\{0,1\}^n \rightarrow \{0,1\}^q$

$$F(x) = (f_1(x), \ldots , f_q(x)),$$

где n – количество бит входа, q – количество бит выхода, каждая $f_i(x)$ является булевой функцией в $GF(2^n)$, $i = 1, \ldots , q$. Функция F(x) является аналитическим представлением S-блоков. Таблица истинности (последовательность) функции F(x) содержит $q2^n$ элементов.

S-блок является структурой, комбинирующей выходы q нелинейных булевых функций, подобранных определенным образом. Очевидно, что для противостояния корреляционным атакам каждая функция должна иметь малую корреляцию со множеством линейных функций, другими словами, быть высоко нелинейной, и иметь равномерную минимизацию коэффициентов корреляции. Т.к. последовательность {z} является комбинацией выходных бит булевых функций, необходимо рассмотрение корреляции всех булевых функций (линейных и нелинейных) над $GF(2^q)$ со множеством всех линейных функций над $GF(2^n)$. Известно, что над $GF(2^q)$ существует 2^{2^q} булевых функций.

Задача определения корреляции может быть формализована следующим образом. Пусть имеется функция F(x) над $GF(2^n)$, осуществляющая отображение $\{0,1\}^n \rightarrow \{0,1\}^q$, и произвольная булева функция g над $GF(2^q)$, осуществляющая отображение $\{0,1\}^q \rightarrow \{0,1\}$. Выходная последовательность F(x) может рассматриваться как последовательность булевой функции g(F(x)) над $GF(2^q)$, осуществляющей отображение $\{0,1\}^n \rightarrow \{0,1\}$. Необходимо найти корреляцию между заданной функцией g, $g \in GF(2^q)$, и линейной функцией L_w, $L_w \in GF(2^n)$. В терминах корреляции можем записать, что

$$\min c(g, A) \le c(g, L_w) = c\,(g(F(x)), L_w) \le \max c(g, A),$$

где c – коэффициент корреляции, A – множество всех аффинных функ-

ций над $GF(2^n)$.

Поскольку при рассмотрении корреляции необходимо определение спектральных свойств преобразований, по аналогии с [3] преобразование Уолша для функции F(x) можем представить как

$$\hat{F}_u(w) = \sum_{x \in GF(2^n)} (-1)^{g(F(x))} (-1)^{wx}, \quad (2)$$

где $g(F(x)) = u_1 f_1 \oplus u_2 f_2 \oplus \ldots \oplus u_q f_q$ рассматривается как булева функция, осуществляющая отображение $\{0,1\}^n \to \{0,1\}$ для любого произвольного вектора и $\in GF(2^q)$, либо как

$$\hat{F}_u(w) = \#\{x \mid w \cdot x = u \cdot F(x)\} - \#\{x \mid w \cdot x \neq u \cdot F(x)\} = 2^n - 2d(g(F(x)), L_w), \quad (3)$$

где $d(g(F(x)), L_w)$ – расстояние Хэмминга между функциями $g(F(x))$ и L_w; $w, x \in GF(2^n)$.

Аналогично [3], для блочного нелинейного преобразования имеем

$$\sum_{w \in GF(2^n)} \hat{F}_u^2(w) = 2^{2n}. \quad (4)$$

Коэффициент корреляции в терминах преобразования Уолша для блочного нелинейного преобразования будет иметь вид

$$c(g(F(x)), L_w) = \frac{1}{2^m} \sum_{u \in GF(2^q)} |\hat{F}_u(w)| (-1)^{\langle u,w \rangle}. \quad (5)$$

Кроме того, поскольку блок подстановки состоит из q булевых функций $f_i(x)$ над $GF(2^n)$, $i = 1, \ldots, q$, вероятности корреляции будут иметь вид:

$$1 - p_1 = 1/2 + \delta_1; \quad 1 - p_2 = 1/2 + \delta_2; \quad \cdots \quad 1 - p_q = 1/2 + \delta_q.$$

Следовательно, для блочных нелинейных преобразований выражение (1) принимает вид

$$p_к = 1 - \prod_{i=1}^{q} (1 - p_i) = 1 - \prod_{i=1}^{q} \left(\frac{1}{2} - \delta_i \right), \quad (6)$$

где $p_i = 1/2 + \delta_i$, $i = 1, \ldots, q$. Поскольку для $\forall \delta_i$ справедливо $0 < \delta_i < 0{,}5$, $i = 1, \ldots, q$, анализируя выражение (6) можно сделать вывод, что возможны случаи, когда будет справедливо равенство $p_к = 1$.

В качестве примера рассмотрим один из блоков подстановки, используемый в DES: {0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8}. По имеющимся последовательностям были восстановлены булевы функции, последовательности которых сформировали данный блок подстановки:

$$f_1(x) = x_1x_2x_3 + x_2x_3x_4 + x_1x_2 + x_3x_4 + x_1 + x_2 + x_4;$$
$$f_2(x) = x_1x_3x_4 + x_2x_3x_4 + x_1x_2 + x_2x_3 + x_3x_4 + x_2 + x_3 + x_4;$$
$$f_3(x) = x_1x_2x_4 + x_1x_3x_4 + x_1x_4 + x_2x_4 + x_1 + x_2 + x_3 + x_4;$$
$$f_4(x) = x_1x_2x_4 + x_1x_3x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3 + x_4.$$

В табл. 1 приведены расчетные данные коэффициентов корреляции, из которых видно, что блочным нелинейным преобразованиям присуща высокая корреляция выходной последовательности с линейными функциями. Это со-

здает потенциальную угрозу успешного применения корреляционных атак.

Таблица 1

Расчетные данные коэффициентов корреляции

	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	L_{16}
f_1	0	0,25	0	0,25	0	0,25	0	0,25	0,25	0	0,25	0,5	0,25	0,5	0,25	0
f_2	0	0	0	0,5	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0	0,5	0	0
f_3	0	0	0,25	0,25	0,25	0,25	0	0	0	0	0,25	0,25	0,25	0,25	0,5	0,5
f_4	0	0	0,25	0,25	0,25	0,25	0	0	0	0	0,25	0,25	0,25	0,25	0,5	0,5

Таким образом, можно констатировать, что использование в ПШ, построенных над расширенным полем, в качестве нелинейных преобразований только лишь блочных преобразований является потенциально опасным. Для минимизации просачивания информации в таких схемах, на наш взгляд, целесообразно придерживаться следующих правил: осуществлять подбор составляющих блоков подстановок – нелинейных булевых функций таким образом, чтобы они имели низкие значения вероятности корреляции $p_к$; выходная последовательность блока подстановки не должна быть выходной последовательностью схемы преобразования: необходимо последующее преобразование данной последовательности; в качестве последующих преобразований использовать технику "забеливания": выходная последовательность должна быть преобразована с помощью последующих труднообратимых операций.

ЛИТЕРАТУРА

1. *Горбенко И., Потий А., Избенко Ю., Орлова С. Анализ схем поточного шифрования, представленных на европейский конкурс NESSIE // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – НТУ "КПІ", ДСТСЗІ СБУ. – 2002. – Вип. 5. – С. 92 – 110.*
2. *Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. – Oct. 1984. – Vol. IT-30. – P. 776 – 780.*
3. *Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // In Advances in Cryptology – EUROCRYPT'89. – 1990. – Vol. 434, Lecture Notes in Computer Science, Springer-Verlag. – P. 549 – 562.*

Поступила 23.11.2004

***СТАСЕВ Юрий Владимирович**, доктор техн. наук, профессор, начальник факультета ХВУ. В 1981 году окончил Харьковское ВВКИУ РВ. Области научных интересов – помехоустойчивые системы связи, криптографическая защита информации.*

***ИЗБЕНКО Юрий Анатолиевич**, научный сотрудник НИЛ кафедры ХВУ. В 1998 году окончил ХВУ. Область научных интересов – криптографическая защита информации.*

***ПЕТРУКОВИЧ Дмитрий Евгеньевич**, канд. техн. наук, нач. отделения лаборатории ХВУ. В 1992 году окончил ХВВКИУ РВ. Области научных интересов – компактное*

представление видеоданных, криптографическая защита информации.