

А.А.КУЗНЕЦОВ, канд.техн.наук, **Ю.А.ИЗБЕНКО**, канд.техн.наук,
А.А.ЮКАЛЬЧУК (г.Харьков)

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ПОСТРОЕНИЯ ВЫСОКО НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

В статті наведено аналіз відомих методів побудови високо нелінійних булевих функцій. Проведено дослідження методів, що побудовані на основі різних підходів. Зроблено висновок щодо доцільності розробки комбінованого методу побудови високонелінійних булевих функцій.

Present analysis known methods construction of highly nonlinear Boolean functions in article. Perform to investigation of methods, that are construction by different approach. The conclusion is given to advisability development of combined method construction highly nonlinear Boolean functions.

Одной из базовых компонент симметричных криптосистем являются нелинейные преобразования, определяющие стойкость к методам криптоанализа. Как правило, нелинейные преобразования строятся на основе нелинейных булевых функций. Конструирование методов построения высоко нелинейных булевых функций в последние годы является областью широких исследований в теории защиты информации [1]. На сегодняшний день существует большое количество методов построения требуемых функций, позволяющих осуществлять построение функций с высокими показателями стойкости [2-13]. Существующее разнообразие методов построения, отличие используемых подходов и показателей делают задачу анализа известных методов построения нелинейных функций актуальной. Анализ данных методов позволит определить оптимальные пути построения нелинейных преобразований для формирования функций с высокими показателями стойкости.

Основными показателями стойкости нелинейных функций являются [2,3]:

1. Сбалансированность.
2. Нелинейность.
3. Корреляционный иммунитет.
4. Критерий распространения (строгий лавинный критерий).
5. Алгебраическая степень.

Введем основные понятия и определения.

Функция f над $GF(2^n)$ является сбалансированной, если ее выходные значения являются равновероятными:

$$|\{x | f(x) = 0\}| = |\{x | f(x) = 1\}| = 2^{n-1}.$$

Нелинейность функции N_f - минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над $GF(2^n)$ [3]:

$$N_f = \min \{d(f, \varphi)\},$$

где φ - множество аффинных функций. Для сбалансированной функции f над $GF(2^n)$ ($n \geq 3$) нелинейность N_f может достигать [3]:

$$N_f \leq \begin{cases} 2^{n-1} - 2^{n/2-1} - 2, & n = 2k, \\ \lfloor \lfloor 2^{n-1} - 2^{n/2-1} \rfloor \rfloor, & n = 2k + 1, \end{cases}$$

где $\lfloor \lfloor x \rfloor \rfloor$ - максимальное четное целое, меньше либо равно x .

Функция f обладает *корреляционным иммунитетом* порядка k , если выходная последовательность функции $y \in Y$ статистически не зависит от любого подмножества из k входных координат [4]:

$$\forall \{x_1, \dots, x_k\} \quad P(y \in Y | \{x_1, \dots, x_k\} \in X) = P(y \in Y).$$

Функция f над полем $GF(2^n)$ удовлетворяет [3]:

- критерию распространения относительно вектора α , $KP(\alpha)$, если функция $f(x) \oplus f(x \oplus \alpha)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, \dots, x_n)$:

$$P(f(x) \oplus f(x \oplus \alpha)) = \frac{1}{2};$$

- критерию распространения степени k , $KP(k)$, если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \leq W(\alpha) \leq k$:

$$P(f(x) \oplus f(x \oplus \alpha)) = \frac{1}{2} \quad \forall \alpha : 1 \leq W(\alpha) \leq k;$$

- строгому лавинному критерию, *СЛК*, если f удовлетворяет критерию распространения степени 1:

$$P(f(x) \oplus f(x \oplus \alpha)) = \frac{1}{2} \quad \forall \alpha : W(\alpha) = 1.$$

Алгебраическая степень $deg(f)$ является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Алгебраической нормальной формой называется выражение вида

$$f(x_1, \dots, x_n) = a_0 \oplus \bigoplus_{i=1}^n a_i x_i \oplus \bigoplus_{1 \leq i < j \leq 1} a_{ij} x_i x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n.$$

Известные методы построения нелинейных функций с требуемыми показателями стойкости можно условно разделить на два класса: эвристические; систематические. К эвристическим методам [2,3] относятся методы, использующие некоторые интуитивные подходы к построению требуемых функций, основанные на манипуляции известными свойствами предмета исследования. Достоинства таких методов заключаются в достижении высоких показателей стойкости (для некоторого множества показателей). Недостатком данных методов является высокая вычислительная сложность построения требуемых примитивов.

К систематическим методам [4-13] относятся методы, использующие итеративные процедуры построения требуемых функций на основе модификации функций, удовлетворяющих определенным требованиям (например, бент-функций). Достоинством таких методов является низкая вычислительная сложность и возможность, при некоторых фиксированных показателях

стойкости, максимизации других показателей. Недостатком данных методов является то, что в процессе итерации процедур понижаются некоторые показатели стойкости, например, нелинейность.

Наибольшее распространение получили методы систематического конструирования. Они позволяют при фиксированных показателях стойкости (например, степени корреляционного иммунитета) максимизировать другие показатели стойкости (например, нелинейность, алгебраическую степень), а также целенаправленно (регулярно) получать функции с заданными показателями стойкости. Эвристические методы при некоторых высоких показателях стойкости (например, нелинейности) не позволяют обсуждать такие показатели, как критерий распространения, корреляционный иммунитет. На рис.1 представлена классификация методов построения высоко нелинейных булевых функций по способу их построения.

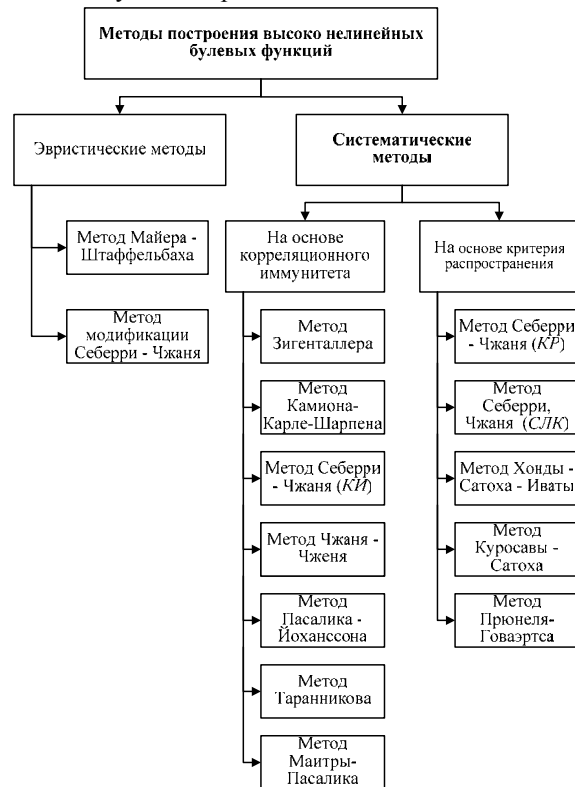


Рис.1 – Методы построения высоко нелинейных булевых функций

Проведенный анализ показал [14], что методы систематического конструирования используют два основных подхода к построению требуемых функций: подход, основанный на концепции корреляционного иммунитета и подход, основанный на концепции критерия распространения (строгого лавинного критерия). Оба подхода при общих фиксированных показателях стойкости (сбалансированность, нелинейность, алгебраическая степень) направлены на максимизацию порядка корреляционного иммунитета (первый подход) $k: \max KI, k \in KI$, и степени критерия распространения (второй подход) $k^*: \max KP, k^* \in KP$. Отметим, что в обоих случаях максимизация всех показателей невозможна вследствие взаимозависимости некоторых показателей, поэтому, разработчики, как правило, сами определяют, какие показатели являются в данном конкретном случае наиболее предпочтительными.

Основным недостатком известных методов построения функций на основе критерия распространения является сравнительно низкая алгебраическая степень [2,3,9,12,13]. Строго говоря, она равна $n/2$, в то время как для корреляционно - иммунных функций она может достигать $n - 1$ [4-8,10,11]. Корреляционно-иммунные функции, так же как и функции, удовлетворяющие критерию распространения, уступают по нелинейности функциям, построенным на основе эвристических методов. В таблице 1 приведены граничные показатели стойкости функций, построенных в соответствии с наиболее перспективными методами – эвристическим методом модификации Себерри-Чжэня (метод, дающий функции с высокой нелинейностью)[3], и систематическими методами на основе критерия распространения (методы, потенциально более стойкие относительно методов на основе корреляционного иммунитета[14]).

Таблица 1

Граничные показатели стойкости функций

	Нелинейность, N_f	Степень критерия распространения, $KP(k)$	Алгебраическая степень, $deg(f)$
Верхняя граница	$2^{n-1} - 2^{n/2-1} - 2$	$KP(n - 2)$	$n - 1$
Метод модификации Себерри - Чжэня	$N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$, $n=4t$	не обсуждается	не обсуждается
Метод Себерри-Чжэня (КР)	$N_f \geq 2^{n-1} - 2^{n/2}$	$KP(\leq 2n/3)$	$n/2-1$
Метод Себерри-Чжэня (СЛК)	$N_f \geq 2^{n-1} - 2^{n/2}$	$KP(1)$	$n/2-1$
Метод Хонды -Сатоха - Иваты	не обсуждается	$KP(2)$	$n - \log_2 n$
Метод Куросавы - Сатоха	$N_f \geq 2^{n-1} - 2^{n/2}$	$KP(1)$	$n - 1$

В таблицах 2, 3, 4 приведены расчетные показатели нелинейности, степени критерия распространения и алгебраической степени соответственно для данных методов и для различных векторных пространств. Подразумевается, что все функции являются сбалансированными и построены над четным векторным пространством V_n .

Таблица 2

Расчетные показатели нелинейности функций

	V_4	V_6	V_8	V_{10}	V_{12}	V_{14}	V_{16}
Верхняя граница	4	26	118	494	2014	8126	32638
Метод модификации Себерри -Чжэня	4	26	116	492	2010	8120	32624
Методы Себерри-Чжэня, Куросавы -Сатоха	4	24	112	480	1984	8064	32512

Таблица 3

Расчетные показатели степени критерия распространения функций

	V_4	V_6	V_8	V_{10}	V_{12}	V_{14}	V_{16}
Верхняя граница	≤ 2	≤ 4	≤ 5	≤ 6	≤ 8	≤ 9	≤ 10
Метод модификации Себерри -Чжэня	не обсуждается						
Метод Себерри-Чжэня (КР)	≤ 2	≤ 4	≤ 5	≤ 6	≤ 8	≤ 9	≤ 10
Метод Себерри-Чжэня (СЛК)	1	1	1	1	1	1	1
Метод Хонды -Сатоха - Иваты	2	2	2	2	2	2	2
Метод Куросавы -Сатоха	1	1	1	1	1	1	1

Таблица 4

Граничные показатели алгебраической степени функций

	V_4	V_6	V_8	V_{10}	V_{12}	V_{14}	V_{16}
Верхняя граница	3	5	7	9	11	13	15
Метод модификации Себерри -Чжэня	не обсуждается						
Методы Себерри-Чжэня	2	2	3	4	5	6	7
Метод Хонды -Сатоха - Иваты	2	4	5	7	9	11	13
Метод Куросавы -Сатоха	3	5	7	9	11	13	15

Выводы. Приведенные исследования показали, что неоспоримым преимуществом эвристических методов является достижение высокой нелинейности. Практически, удается достичь верхней границы нелинейности. Однако, как правило, не обсуждаются другие показатели стойкости. Систематические методы, уступая эвристическим в нелинейности, позволяют обсуждать степень критерия распространения и алгебраическую степень функций. Таким образом, является целесообразной разработка комбинированного метода построе-

ния высоко нелинейных булевых функций, основанного на концепции критерия распространения, который, в отличие от известных, объединил бы в себе принципы эвристических и систематических методов и позволил строить высоко нелинейные булевы функции с высокой алгебраической степенью и удовлетворяющие строгому лавинному критерию.

Список литературы: 1.B.Schneier. Applied Cryptography. 2nd edition, John Wiley & Sons, New York,1996. 2.W.Maier, O.Staffelbach. Nonlinearity criteria for cryptographic functions // In Advances in Cryptology – EUROCRYPT’89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562,1990. 3.J. Seberry, X.-M. Zhang and Y.Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // In Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995. 4.T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory, vol. IT-30, pp. 776-780, Oct. 1984. 5.P.Camion, C.Carlet, P.Charpin, N.Sendrier. On Correlation-immune functions // In Advances in Cryptology – Crypto’91, vol.576, Lecture Notes in Computer Science, Springer-Verlag. - P.87-100. 6.J.Seberry, X.M.Zhang, Y.Zheng. On Contractions and Nonlinearity of Correlation Immune Functions // In Advances in Cryptology – EUROCRYPT’93, vol.765, Lecture Notes in Computer Science, Springer-Verlag, pp.181-199,1994. 7.X.-M. Zhang and Y.Zheng. Cryptographically resilient functions // IEEE Transactions on Information Theory, September 1997, pp.457- 478. 8.Y.Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity. – Moscow State University. – 2000. – <http://www.mech.math.msu.ru>. 9.B.Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria // In Lecture Notes in Computer Science 547; Advances in Cryptology: Proc. Eurocrypt’91, 1991, pp. 141-152. Berlin: Springer-Verlag. 10.S.Maitra, E.Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA, May, 2001, Norway. 11.E.Pasalic, T.Johansson, S.Maitra, P.Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity. In Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001. 12.T.Honda, T.Satoh, T.Iwata, K.Kurosawa. Balanced Boolean functions satisfying PC(2) and very large degree. <http://www.ss.titech.ac.jp>. 13.K.Kurosawa, T.Satoh. Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria. In Advances in Cryptology EUROCRYPT’97 Proceedings, Lecture notes in Computer Science 1233, p.434-449. Springer-Verlag, 1997. 14.Потуй А.В, Избенко Ю.А. Обоснование выбора метода построения криптографически стойких булевых функций // Радиотехника. Всеукраинский межведомственный научно-технический сборник. - 2002. - № 126. - С. 132 - 138.