УДК 681.3.06

А.А. Кузнецов, Ю.А. Избенко, И.В. Московченко

Харьковский университет Воздушных Сил им. И. Кожедуба

МЕТОД ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ БУЛЕВЫХ ФУНКЦИЙ НА ОСНОВЕ ГРАДИЕНТНОГО СПУСКА

Рассматриваются криптографические булевы функции, исследуются методы их построения. Предлагается метод построения криптографически стойких булевых функций на основе градиентного спуска.

криптографические булевы функции, градиентный спуск

Введение

Постановка проблемы в общем виде и анализ литературы. Актуальным направлением развития криптографии является разработка и исследование криптографических булевых функций [1 – 4]. Так, например, блоки нелинейной подстановки симметричных шифров эффективно описываются в терминах булевой алгебры и дают мощный механизм их конструирования. В работе [5] теоретически доказано, что применение итеративных процедур градиентного поиска позволит формировать булевы функции с высокими показателями нелинейности и алгебраической степени, удовлетворяющих строгому лавинному критерию. Следовательно, разработка эффективных методов построения криптографически стойких булевых функций на основе градиентного поиска является актуальной научно-технической задачей.

Основной материал

Предлагаемый метод построения криптографических булевых функций является дальнейшим развитием эвристического метода градиентного подъема. Данный метод основан на использовании свойств нелинейных последовательностей, отличается от известных введением дополнительных процедур восстановления и модификации алгебраически нормальных форм булевых функций, и позволяет строить нелинейные булевы функции с высокими показателями стойкости.

В работе [6] показано, что для бент-функций справедливо выражение

$$N_{бент} = 2^{n-1} - 2^{n/2-1}, \quad (1)$$

при этом значения преобразования Уолша являются равномерно распределенными

$$| F(w) | = 2^{n/2} \quad (2)$$

для всех значений w, w = 1,…, 2^n.

Для сбалансированных функций справедливо выражение [6]

$$N_f \le 2^{n-1} - 2^{n/2-1} - 2. \quad (3)$$

Отметим, что нелинейность напрямую связана со значениями преобразования Уолша [6]:

$$F(w) = 2^n - 2\,N_f. \quad (4)$$

Как видно из приведенных данных, чем выше значение нелинейности функции, тем меньше ее значения преобразования Уолша, и наоборот, чем выше значения преобразования Уолша функции, тем ниже ее нелинейность.

Основной идеей предлагаемого метода является эффективное понижение нелинейности заданных бент-последовательностей при каждой из $2^{n/2-1}$ обязательных комплементаций. Для наглядной иллюстрации принципа работы предложенного метода в табл. 1 представлены расчетные данные для четных векторных пространств V_4 – V_{12}, принимаемые к рассмотрению при дальнейших расчетах. Так, в столбце 2 на основании (1) и (2) указана нелинейность (значение преобразования Уолша) бент-последовательностей, рассматриваемых как входные данные, в столбце 3 на основании (3) и (4) указана максимально достижимая нелинейность (макс. значение преобразования Уолша) функций, которые мы хотели бы получить в качестве выходных данных, и в столбце 4 указано количество бит, которое необходимо изменить в бент-последовательностях для получения желаемого результата.

Отметим, что само по себе изменение необходимого количества бит в бент-последовательности не гарантирует достижение нелинейности, близкой к максимальной. Так, например, если мы хотим модифицировать бент-последовательность над V_8 (V_{10}) и выполним необходимые 8 (16) комплементаций таблицы истинности, то может оказаться, что вместо желаемой сбалансированной высоконелинейной последовательности с нелинейностью 116 (492) мы получим последовательности с нелинейностью 112 (476). И чем больший размер векторного пространства мы используем, тем существенней будет разница между полученным и ожидаемым результатами. На рис.1 представлены возможные потери нелинейности при непосредственной комплементации необходимого числа позиций бент-последовательности.

Таблица 1

Расчетные значения некоторых показателей булевых функций, полученных в соответствии с методом градиентного спуска

	Максимально достижимые показатели для бент-функций		Максимально достижимые показатели для сбалансированных функций / Наилучший известный результат		Необходимо изменить __ позиций в бент-последовательности
	N_f	F(w)	N_f	F(w)	
V_4	6	4	4/4	8/8	2 позиции
V_6	28	8	26/26	12/12	4 позиции
V_8	120	16	118/126	20/24	8 позиции
V_{10}	496	32	494/492	36/40	16 позиции
V_{12}	2016	64	2014/2010	68/76	32 позиции

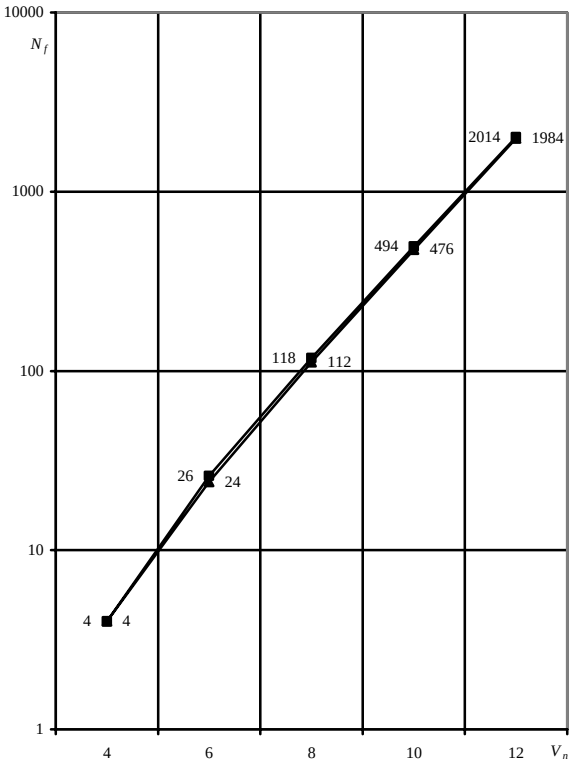

Рис. 1. Возможные потери нелинейности при комплементации

Как показывает практика, такое различие между полученными и ожидаемыми значениях обусловлено тем, что каждый раз могут комплементироваться позиции, изменение которых влечет за собой только увеличение максимального значения преобразования Уолша (уменьшение нелинейности), т.е. все значения WH изменятся на +2. Следовательно, для достижения заданной верхней границы нелинейности необходимо из общего числа позиций x таблицы истинности, подлежащих комплементации, определить то число позиций y, изменение которых повлечет изменение WH на +2, и то число позиций z, изменение которых повлечет изменение WH на –2, $x = y + z$.

Расчетное соотношение для вычисления количества позиций в таблице истинности функции, которые необходимо инвертировать с целью получения максимально-достижимой нелинейности, представлено в Утверждении 1.

Утверждение 1. Для того, чтобы модифицировать бент-последовательность и получить сбалансированную последовательность, обладающую максимально достижимой для сбалансированной функции нелинейностью, необходимо инвертировать n^- позиций таблицы истинности таким образом, чтобы все значения WH изменились на +2, и n^+ позиций таблицы истинности таким образом, чтобы все значения WH изменились на –2, причем

$$n^- = \mathrm{Razn} + \left(\mathrm{NeedSteps} - \mathrm{Razn}\right)/2\,; \qquad (5)$$

$$n^+ = \left(\mathrm{NeedSteps} - \mathrm{Razn}\right)/2 = \mathrm{NeedSteps} - n^-\,, \qquad (6)$$

где NeedSteps – количество позиций в бент-последовательности, которые необходимо инвертировать; Razn – количество позиций в бент-последовательности, которые необходимо инвертировать для именения нелинейности с $N_{бент}$ на $N_{сбаланс}$.

Доказательство. Согласно (1), (3), разница между $N_{бент}$ и $N_{сбаланс}$ равна 2. Такой разницы в нелинейности можно достичь, если произвести две комплементации таблицы истинности таким образом, чтобы все значения WH изменились на +2. Таким образом, из общего числа $2^{n/2-1}$ обязательных комплементаций NeedSteps, Razn комплеметаций должно быть направлено на понижение нелинейности с $N_{бент}$ на $N_{сбаланс}$. Оставшиеся NeedSteps – Razn комплеметаций должны быть произведены таким образом, чтобы их суммарные данные были равны 0, т.е. они должны компесировать друг друга. Следовательно, должно быть произведено

$$\left(\mathrm{NeedSteps} - \mathrm{Razn}\right)/2$$

комплементаций, при которых все значения WH изменились бы на +2 и

$$\left(\mathrm{NeedSteps} - \mathrm{Razn}\right)/2$$

комплементаций, при которых все значения WH изменились бы на –2. Таким образом, общее число комплементаций n^-, при которых нелинейность должна уменьшиться, будет определяться выражением (5). Общее число комплементаций n^+, при которых нелинейность должна увеличиться, будет определяться выражением (6), что и завершает доказательство. Альтернативное доказательство утверждения 1 можно получить, проводя аналогичные рассуждения в терминах преобразования Уолша, опираясь на $F_{бент}$ (w) и $F_{сбаланс}$.(w).

В табл. 2 представлены расчетные данные, отображающие необходимое число требуемых комплементаций бент-последовательности для заданного векторного пространства.

Поскольку в практических приложениях может возникнуть задача построения функций с заданной нелинейностью, представляется целесообразным дать обобщающую формулировку утверждения 1 в контексте получения булевых функций с заданной нелинейностью, полученных путем комплементации позиций таблицы истинности бент-последовательности.

Таблица 2

Расчетные данные необходимого числа требуемых комплементаций бент-последовательности в соответствии с методом градиентного спуска

	Необходимо изменить позиций в бент-последовательности, NeedSteps	Необходимо изменить значение нелинейности		Требуется для этого измений, n^- и n^+
		N_f, с _ на _	F(w), с _ на _	
V_4	2	$6 \to 4$	$4 \to 8$	$n^- = 2$ (изм-я с F(w) = +2)
V_6	4	$28 \to 26$	$8 \to 12$	$n^- = 3$ (изм-я с F(w) = +2) $n^+ = 1$ (изм-я с F(w) = –2)
V_8	8	$120 \to 116$	$16 \to 24$	$n^- = 6$ (изм-я с F(w) = +2) $n^+ = 2$ (изм-я с F(w) = –2)
V_{10}	16	$496 \to 492$	$32 \to 40$	$n^- = 10$ (изм-я с F(w) = +2) $n^+ = 6$ (изм-я с F(w) = –2)
V_{12}	32	$2016 \to 2010$	$64 \to 76$	$n^- = 19$ (изм-я с F(w) = +2) $n^+ = 13$ (изм-я с F(w) = –2)

Утверждение 2. Для того, чтобы модифицировать бент-последовательность, обладающую нелинейностью $N_{бент}$ и получить сбалансированную последовательность, обладающую требуемой нелинейностью $N_{треб}$, необходимо инвертировать n^- позиций таблицы истинности таким образом, чтобы все значения WH изменились на +2, и n^+ позиций таблицы истинности таким образом, чтобы все значения WH изменились на –2, причем

$$n^- = Razn + (NeedSteps - Razn)/2;$$

$$n^+ = (NeedSteps - Razn)/2 = NeedSteps - n^-,$$

где переменная Razn, определенная в терминах нелинейности, имеет вид

$$Razn = N_{бент} - N_{треб}, \qquad (7)$$

переменная Razn, определенная в терминах преобразования Уолша, имеет вид

$$Razn = (F_{треб}(w) - F_{бент}(w))/2. \qquad (8)$$

Доказательство утверждения аналогично доказательству Утверждения 1.

Результат последнего утверждения позволяет применить конструктивный подход к формированию сбалансированных высоко нелинейных булевых функций путем модификации бент-последовательности. Основным достоинством такого подхода являются высокие значения обеспечиваемой нелинейности, которые лежат в теоретическом пределе (рис. 1). В целом предлагаемый метод структурно состоит из трех основных этапов.

На первом этапе используется метод градиентного спуска, позволяющий получить высоко нелинейную последовательность $\xi = \varepsilon_0 \varepsilon_1 \cdots \varepsilon_{2^n-1}$, где n – размерность векторного пространства.

На втором этапе используется процедура восстановления алгебраической нормальной формы функции по выходной последовательности ξ. Использование данной процедуры позволяет по известной последовательности $\xi = \varepsilon_0 \varepsilon_1 \cdots \varepsilon_{2^n-1}$ восстановить исходную алгебраическую нормальную форму булевой функции.

На третьем этапе, в зависимости от среды практического приложения, используется процедура модификации алгебраической нормальной формы функции f(x), позволяющая при сохранении основных показателей стойкости нелинейного преобразования (сбалансированности и нелинейности) путем применения аффинных преобразований f(xA)\ f(C_f x) изменить вид что позволит улучшить либо динамические свойства нелинейного преобразования (матрица A), либо корреляционные свойства (матрица C_f).

Выводы

В результате проведенных исследований разработан метод построения криптографически стойких булевых функций на основе градиентного спуска. Показано, что практическое использование разработанного метода позволяет формировать криптографические булевы функции с высокими показателями стойкости.

Список литературы

1. Горбенко И.Д., Потий А.В., Избенко Ю.А. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197) // Радиотехника. – Х.: ХНУРЭ, 2004. – № 126. – С. 132-138.

2. Maitra S., Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA, May, 2001, Norway.

3. Pasalic E., Johansson T. Further Results on the Relation Between Nonlinearity and Resiliency for BF // IEEE Trans. on Information Theory. – July 2002. – Vol 48, No. 7. – P. 1825-1834.

4. Pasalic E., Johansson T., Maitra S., Sarkar P New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier. – January 2001.

5. Millan W., Clark A. and Dawson E. Heuristic Design of Cryptographically Strong Balanced Boolean Functions // Cryptology EUROCRYPT'98. – Springer Verlag LNCS 1403. – 1998.– P. 489–499.

6. Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Cryptology – EUROCRYPT'89, Lecture Notes in Computer Science: Springer-Verlag, 1990. – Vol.434. – P. 549-562,

Поступила в редколлегию 18.12.2006

Рецензент: д-р техн. наук проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.