УДК 681.3.06

А.А. КУЗНЕЦОВ, Ю.А. ИЗБЕНКО, И.В. МОСКОВЧЕНКО

Харьковский университет Воздушных Сил им. И. Кожедуба, Украина

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ МЕТОДОМ ГРАДИЕНТНОГО СПУСКА

Исследуется криптографическая стойкость булевых функций, построенных методом градиентного спуска. Проводится сравнительный анализ с функциями, сформированными с использованием наилучших методов.

булевы функции, криптографические свойства, метод градиентного спуска

Введение

В настоящее время обеспечение безопасности информации в информационно-телекоммуникационных системах является одной из первоочередных задач. Данная задача, в частности, может быть решена за счет использования симметричных схем криптопреобразования, стойкость которых обеспечивается за счет использования нелинейных преобразований. Поэтому разработка нелинейных преобразований, обеспечивающих стойкость к современным методам криптоанализа, является актуальной задачей.

В качестве нелинейных преобразований в симметричных криптосистемах используются нелинейные булевы функции [1 – 9]. Разработка таких функций является областью широких исследований. В [1] представлен метод построения нелинейных булевых функций, основанный на градиентном спуске. В качестве прототипа использовался метод градиентного подъема [2], который является на сегодняшний день одним из наиболее эффективных методов формирования криптографических булевых функций. Оба метода относятся к классу эвристических методов и потенциально позволяют достигать б*о*льших показателей стойкости, нежели другие классы построения функций за счет использования не каких-либо формальных алгебраических конструкций, а интуитивно понятных принципов и ‘ухищрений’. В данной статье исследуются криптографические свойства функций, построенных в соответствии с [1].

Основные результаты исследований

При проведении исследований криптографических свойств нелинейных булевых функций использованы следующие показатели: сбалансированность, нелинейность N_f, алгебраическая степень *deg*, значение функции автокорреляции *ac*, степень корреляционного иммунитета *CI*, степень критерия распространения *PC*. Методика исследования и детальное описание данных показателей представлены [3]. При описании основных показателей использованы следующие типы формализованной записи [4]: (*n, deg,* N_f*, ac*) – если не обсуждаются показатели *CI* и *PC*; (*n, CI/PC, deg,* N_f*, ac*) – если данные показатели обсуждаются (*n* – размерность функции). В качестве дополнительных показателей рассмотрены коэффициент равномерности минимизации корреляции $k_{рм}$ и абсолютное значение корреляции функции C_f [3].

В табл. 1 представлены результаты сравнительной оценки нелинейности функций, полученных при использовании разработанного метода, метода-прототипа и наилучших известных методов.

Приведенные данные свидетельствуют, что среди эвристических методов разработанный метод позволяет достигать наивысшей нелинейности и стремится к верхней границе нелинейности. Высокая нелинейность свидетельствует о высокой степени замешивания данных, что определяет стойкость преобразований. Функции, построенные в соответствии с разработанным методом, по степени нелинейности уступают лишь конструкции Доббертина,

однако, во-первых, данная конструкция не является столь гибкой, как представленный метод, и, во-вторых, данная конструкция не позволяет обсуждать значение функции автокорреляции.

Таблица 1

Сравнительная оценка нелинейности функций

	V_6	V_8	V_{10}	V_{12}
Наивысшая достижимая нелинейность [5]	26	118	494	2014
Наилучший известный рез-т [4]	26	116	492	2010
Конструкция Доббертина [4]	26	116	492	2010
Бент конкатенация [9]	24	112	480	1984
Random [2]	–	112	472	1954
Random + Hill Climbing [2]	–	114	476	1960
Генетический алгоритм [6]	26	116	484	1976
NLT [4]	26	116	486	1992
ACT [4]	26	116	484	1986
Разработанный метод	26	116	488	1998

В табл. 2 приведены сравнительные характеристики основных показателей стойкости функций, полученных с использованием разработанного и наилучших известных эвристических методов. Как видно из таблицы, разработанный метод позволяет строить функции с наилучшими известными на сегодняшний день профилями. Так, на сегодня функции, построенные над V_6, имели наилучший профиль (6,5,26,16), теперь данный профиль имеет вид (6,5,26,8) (значение функции автокорреляции уменьшено в 2 раза); функции, построенные над V_8, имели наилучший профиль (8,7,116,24), теперь – (8,7,116,16) (значение функции автокорреляции уменьшено в 1,5 раза); функции, построенные над V_{10}, имели наилучший профиль (10, 9, 484, 56), теперь – (10, 8, 488, 32) (значение функции автокорреляции уменьшено в 1,75 раза); функции, построенные над V_{12}, имели наилучший профиль (12, 10, 1992, 156), теперь – (12, 11, 1998, 72) (значение функции автокорреляции уменьшено в 2,16 раза).

Таблица 2

Наилучшие известные профили (n, $deg(f)$, N_f, AC)

NLT [4]	(5,3,12,8); (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24); (8,5,112,16)
	(9,8,238,40)	(10,9,486,72) (10,9,484,64)	(11,9,984,96) (11,10,982,96)	(12,10,1992,156) (12,10,1990,144)
ACT [4]	(5,3,12,8); (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24); (8,5,112,16)
	(9,8,238,40)	(10,9,484,56)	(11,10,982,88)	(12,11,1986,128)
Разработанный метод	-	(6,5,26,8)	-	(8,7,116,16)
	-	(10,8,488,32)	-	(12,11,1998,72)

В табл. 3 приведены сравнительные характеристики наилучших известных методов, позволяющих строить функции с низкими значениями автокорреляции. Как видно, разработанный метод позволяет строить функции с наинизшими известными на сегодняшний день значениями автокорреляции. Можно отметить, что только над V_8 *NLT* и *ACT* методы позволяют строить функции с AC=16, как и предложенный метод, однако при этом функции, полученные использованием *NLT* и/или *ACT* методов, имеют нелинейность 112. Разработанный же метод при том же самом значении автокорреляции позволяет строить функции с нелинейностью 116. Над всеми же остальными векторными пространствами предложенная автокорреляция является недостижимой для других методов.

Таблица 3

Наилучшие известные значения автокорреляции

	V_5	V_6	V_7	V_8	V_9	V_{10}	V_{11}	V_{12}
Zhang Zheng [9]	8	16	16	24	32	48	64	96
Maitra [8]	8	16	16	24	32	40	64	80
NLT [4]	8	16	16	16	40	64	96	144
ACT [4]	8	16	16	16	40	56	88	128
Разработанный метод		8	–	16	–	32	–	72

Рассмотрим также дополнительные показатели стойкости. Коэффициент равномерной минимизации корреляции и абсолютное значение корреляции определяют спектральные свойства функций и отражают их корреляционные свойства. Коэффициент равномерной минимизации корреляции определяет,

во сколько раз, по сравнению с бент-функцией, ухудшилась равномерность спектра функции. Абсолютное значение корреляции функции, как следует из названия, определяет значение максимальной корреляции функции с некоторой аффинной функцией. В табл. 4 представлены дополнительные показатели стойкости, характеризующие спектральные свойства бент-функций, функций, построенных в соответствии с предлагаемым и известными алгебраическими и эвристическими методами построения высоконелинейных нелинейных булевых функций.

Приведенные данные показывают, что булевы функции, построенные в соответствии с разработанным методом, при равных наивысших показателях нелинейности с другими функциями имеют максимально достижимую алгебраическую степень, при этом все остальные известные методы уступают по своим спектральным характеристикам.

Таблица 4

Дополнительные показатели стойкости нелинейных булевых функций

	N_f	$deg(f)$	k_{pm}	C_f
Бент-функция [4]	120	4	1	0,06250
Разработанный метод	116	7	1,058333	0,09375
Метод Кларка [4]	116	6	1,099567	0,09375
Метод Маитры-Пасалика[7]	116	6	1,154545	0,09375
Метод Себерри-Чжаня (*КИ*)[9]	112	4	1,322917	0,12500

Обсуждая дополнительные показатели стойкости, можно отметить, что функции, полученные в соответствии с разработанным методом, имеют наилучшие спектральные характеристики: их коэффициенты корреляции наиболее равномерно минимизированы, абсолютные значения корреляции имеют наинизшие значения по сравнению с функциями, построенными согласно известных методов.

Выводы

На основе проведенных исследований можно сделать вывод о том, что функции, сформированные в соответствии с разработанным методом построения, имеют высокие показатели стойкости и превосходят по данным показателям известные функции.

Литература

1. Кузнецов А.А, Избенко Ю.А., Московченко И.В. Метод построения криптографически стойких булевых функций на основе градиентного спуска // Збірник наукових праць ХУ ПС. – Х.: ХУПС, 2007. – Вип. 1 (13). – С. 63-66.

2. Millan W., Clark A., Dawson E. Smart Hill Climbing Finds Better Boolean Functions // Workshop on Selected Areas in Cryptography 1997 (SAC'97) : Workshop Record, 1997 – P. 50.

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

4. Evolving of Boolean functions satisfying multiple criteria / J. Clark and s.o. // Proc. of INDOCRYPT'02, LNCS. – Springer, 2002. – Vol. 2551. – P. 246-259.

5. Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // EUROCRYPT'89 (Comp. Science). – Springer-Verlag, 1990. – Vol. 434. – P. 549-562.

6. Millan W., Clark A., Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean functions // 1st Int. Conf. on Inf. and Commun. Security. – Springer Verlag, 1997. – N. 1334. – P. 149-158.

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

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

9. Seberry J, Zhang X.-M., Zheng Y. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // In Information and Computation. – 1995. – Vol. 119, No 1. – P. 1-13.

Поступила в редакцию 6.06.2007

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.