УДК 621.3.06

А.В. КАЗИМИРОВ, Р.В. ОЛЕЙНИКОВ, канд. техн. наук

МЕТОД ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕНЫ НА ОСНОВЕ ГРАДИЕНТНОГО СПУСКА

Введение

Таблицы замены (S-блоки) являются одним из основных компонентов, определяющих уровень стойкости современных симметричных криптографических примитивов. Как правило, они выполняют отображение n-битного входного блока в выходной длиной m бит. Представление подстановок варьируется в зависимости от задачи. В потоковых шифрах узлы нелинейной замены представлены обычно в виде векторных булевых функций [1]. Перестановки являются подклассом S-блоков и широко используются в блочных шифрах в виде таблиц. S-блок может быть достаточно просто преобразован из одной формы в другую.

Для защиты криптографического примитива от различных типов атак подстановки должны соответствовать ряду критериев [2, 3]. Из-за большого количества существующих критериев, их противоречивости или частичной взаимозависимости сложно сформировать подстановку, удовлетворяющую всем известным требованиям. Поэтому на практике используются подстановки, удовлетворяющие основным критериям, существенным для конкретного симметричного алгоритма. Такие S-блоки принято называть оптимальными [4]. Критерии оптимальности могут варьироваться от шифра к шифру. Генерация перестановок с оптимальными критериями довольно трудоемкая задача, особенно для больших значений n и m.

Эта проблема частично решена с помощью классов векторных булевых функций и расширенно аффинных (РА) и Карлет – Шарпин – Зиновьев (КШЗ) эквивалентностей [1, 5].

Однако большинство найденных функций обладают предельными характеристиками δ-равномерности и нелинейности, при этом не обладают другими свойствами (например, высоким показателем алгебраического иммунитета), необходимыми для симметричных криптопримитивов. Поэтому задача генерации оптимальных подстановок является актуальной.

В статье [6] авторами усовершенствован метод генерации стойких булевых функций, основанный на методе градиентного подъема (HillClimbing) [7].

В данной статье предлагается модифицированный вариант метода градиентного спуска для векторного случая, т.е. для функций из $\mathcal{F}_2^n = GF(2^n)$ в $\mathcal{F}_2^m$.

Определения и обозначения

Произвольная подстановка может быть представлена, по крайней мере, в трех различных формах: алгебраической нормальной форме (АНФ), над полем $\mathcal{F}_2$ и в виде таблицы замены. В большинстве блочных алгоритмов S-блоки имеют табличное представление из-за простоты описания и понимания. В то же время произвольная подстановка всегда может быть связана с векторной булевой функцией F принадлежащей $\mathcal{F}_2[x]$. Если подстановка является перестановкой, то функция F определяется однозначно.

Естественный способ представления $F:\mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ в виде алгебраической нормальной формы [1]:

$$\sum_{I\subseteq\{1,\ldots,n\}} a_I\left(\prod_{i\in I} x_i\right), a_I \in \mathcal{F}_2^m, .$$

сумма рассчитывается в $\mathcal{F}_2^m$. Под алгебраической степенью функции F понимается степень её АНФ. F называется аффинной, если она имеет алгебраическую степень не больше 1. При $F(0)=0$ аффинная векторная булева функция является линейной.

Две функции $F,G:\mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ называются расширенно-аффинно (РА) эквивалентными, если существуют такие аффинно-перестановочные функции $A_1(x)=L_1(x)+c_1$, $A_2(x)=L_2(x)+c_2$ и произвольная линейная функция $L_3(x)$, что [1, 5]:

$$F(x)=A_1\circ G\circ A_2(x)+L_3(x).$$

Если L_3 является константой из векторного пространства $\mathcal{F}_2^m$, тогда функции F и G называются аффинно-эквивалентными; а при $L_3=0, c_1=0, c_2=0$ – линейно-эквивалентными. Аффинная эквивалентность использовалась для предотвращения появления фиксированных точек $\left(F(a)=a, \forall a\in\mathcal{F}_2^n\right)$ при генерации подстановки шифра Rijndael [8].

Произвольная векторная булева функция F является δ-равномерной, если для любого $a\in\mathcal{F}_2^n\setminus\{0\}$ и $b\in\mathcal{F}_2^m$ уравнение $F(x)+F(x+a)=b$ имеет не более δ решений [1]. Векторные булевы функции, используемые как узлы нелинейной замены в блочных симметричных шифрах, должны обладать низким значением δ-равномерности для зашиты от дифференциальных атак [1, 3].

Критерий нелинейность тесно связан с преобразованием Уолша, которое может быть описано функцией

$$\lambda(u,v)=\sum_{x\in\mathcal{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x},$$

где символ «$\cdot$» обозначает скалярное произведение в векторных пространствах $\mathcal{F}_2^n$ и $\mathcal{F}_2^m$. Подстановки с низкими значениями коэффициентов Уолша являются оптимально защищёнными от линейного криптоанализа [1, 3]. S-блоки с предельными значениями $\lambda(u,v)$ существуют лишь для нечётных n.

Эти два критерия являются основными при выборе подстановок для новых шифров. Тем не менее, существует и множество других критериев, таких как: критерий распространения, максимум спектра автокорреляции, корреляционный иммунитет, алгебраический иммунитета, строгий лавинный эффект и т.д. [1, 2, 9]. До сих пор не была доказана необходимость большинства из перечисленных критериев. Например, подстановка используемая в AES не удовлетворяет большинству из них [2].

В данной статье под оптимальной подстановкой понимается перестановка с максимальными показателями алгебраической степени и алгебраического иммунитета с максимальным количеством уравнений; с предельными показателями □-равномерности и нелинейности; отсутствием фиксированных точек (циклов длиной 1).

Например, для n=8 оптимальная подстановка будет иметь алгебраическую степень 7, алгебраический иммунитет 3 с 441 уравнением, иметь δ-равномерность 8 или меньше и нелинейность больше 100; не иметь фиксированных точек.

Генерация подстановок с заданными свойствами

Основная идея метода из [6] состоит в понижении нелинейности заданных бент-последовательностей. Другими словами, в заданной бент-последовательности (таблице истинности) изменяются некоторые биты таким образом, чтобы новая последовательность была сбалансированной, а нелинейность была близкой к нелинейности бент-функции.

В статье предлагается использовать тот же подход, однако с двумя существенными отличиями:

– вместо булевых функций использовать векторные булевы функции;

– вместо бент-функций (последовательностей) использовать векторные булевы функции (подстановки) с максимальными показателями δ-равномерности.

Дополнительно в [6] было показано, что само по себе изменение необходимого количества бит в бент-последовательности не гарантирует достижение нелинейности, близкой к максимальной. Однако для векторного случая в [10] было доказано следующее утверждение.

Утверждение 1. Пусть $F:\mathcal{F}_{2^n} \mapsto \mathcal{F}_{2^n}$. Определим функцию G следующим образом:

$$\begin{cases} G(p_1) = F(p_2), p_1 \neq p_2; \\ G(p_2) = F(p_1); \\ G(x) = F(x), x \neq p_1, p_2. \end{cases}$$

Тогда

$$\delta(F) - 4 \leq \delta(G) \leq \delta(F) + 4,$$
$$Nl(F) - 2 \leq Nl(G) \leq Nl(F) + 2.$$

Функция нелинейности (Nl) произвольной векторной функции F вычисляется следующим образом:

$$Nl(F) = 2^{n-1} - \frac{1}{2}\max_{u \neq 0, v \in \mathcal{F}_{2^n}} |\lambda(u, v)|.$$

Из утверждения 1 видно, что при обмене местами двух значений в некоторой перестановке значения нелинейности и δ-равномерности будут отличаться на фиксированное значение. На основе описанного выше предлагается новый алгоритм генерации подстановок на основе векторных булевых функций.

Алгоритм принимает на вход перестановочную векторную функцию F с минимальным показателем δ-равномерности и количество значений (NP) функции, которые будут изменяться при оптимизации криптографических показателей.

1.Генерация подстановки S на основе выбранной перестановочной (биективной) векторной булевой функции F.

2.Случайный обмен местами NP значений подстановки S и формирование подстановки S_t.

3.Последовательная проверка соответствия критериям в зависимости от их вычислительной сложности. Если подстановка S_t удовлетворяет всем критериям, кроме цикловых свойств, тогда используется РА-эквивалентность для достижения необходимых свойств. При несоответствии хотя бы одному из критериев переход в п. 2.

4.Выход из алгоритма. Необходимая подстановка будет храниться в S_t.

Практические результаты

Перед разработкой предложенного алгоритма была проверена практическая возможность нахождения подстановок с оптимальными показателями для n=8. Задача заключалась в нахождении четырех КШЗ-неэквивалентных подстановок с нелинейностью больше или равной 100. Для реализации данной практической задачи использовался кластер с 4096 процессорами.

Программа генерировала случайную перестановку и проверяла её на оптимальность. После 12 часов работы кластера было найдено 27 оптимальных подстановок, 4 из которых оказались КШЗ-неэквивалентными. Пример одной из подстановок в шестнадцатеричном представлении приведен в табл. 1.

Таблица 1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	14	9D	B9	E7	67	4C	50	82	CA	E5	1D	31	0A	C6	B2	51
1	A2	D8	54	90	D0	CE	2D	7D	C7	7E	D7	94	DF	83	8E	6C
2	66	D2	6F	16	1E	76	FE	CC	AA	5A	8F	17	BD	2C	AC	EA
3	7B	65	A9	10	C0	92	EE	BE	6A	6E	48	96	95	E9	32	BC
4	A1	42	D5	A7	81	B4	5F	E6	C2	5D	AD	3A	B7	0C	8D	01
5	98	FD	12	02	75	13	0F	6B	22	E2	AB	F7	7F	BA	97	D1
6	64	D9	C4	59	AF	23	33	37	DE	AE	60	05	63	A8	52	A5
7	4E	E0	DD	71	F2	24	34	57	47	A4	B3	9E	2F	C1	B8	CB
8	2B	D4	0D	36	91	8B	9C	26	25	61	A3	D6	EB	35	53	F4
9	2E	88	80	E4	30	DB	FC	0E	77	8C	93	A6	78	06	E1	EC
A	F9	03	A0	27	DA	EF	5C	00	7A	45	E8	40	1A	4B	5E	73
B	C3	FF	F5	F3	B0	C5	49	21	FA	11	39	84	43	38	85	07
C	F0	79	46	F8	E3	1F	09	B6	CD	55	1C	1B	FB	7C	ED	6D
D	15	56	86	20	68	4A	41	4F	D3	99	08	F6	3F	89	62	04
E	CF	C8	69	9F	19	5B	44	9B	87	B1	3D	BB	DC	2A	BF	58
F	3C	8A	18	3E	72	0B	28	4D	B5	9A	C9	74	29	F1	3B	70

Данная подстановка обладает следующими характеристиками:

– нелинейность 100;

– абсолютное значение автокорреляции 96;

– минимальная алгебраическая степень 7;

– 8-равномерная;

– алгебраический иммунитет: система из 441 уравнений 3-й степени.

Далее был проведен поиск подстановки с нелинейностью 102. Однако после 48 часов работы кластера, что эквивалентно около 22 лет работы одного однопроцессорного компьютера, ни одной подстановки найдено не было. Таким образом, можно заключить, что с практической точки зрения генерация таких подстановок является вычислительно крайне сложной задачей.

Однако алгоритм, описанный выше, позволяет найти такие подстановки. В качестве примера возьмём функцию $F(x) = x^{-1}$. Увеличивая значения *NP* (начиная с 1) экспериментальным путем найдено значение *NP=21*, при котором достигаются все необходимые свойства подстановки. Пример такой перестановки представлен в табл. 2.

Данная подстановка обладает следующими характеристиками:

– нелинейность 102;

– абсолютное значение автокорреляции 88;

– минимальная алгебраическая степень 7;

– 8-равномерная;

– алгебраический иммунитет: система из 441 уравнений 3-й степени.

За 12 часов на 8-ядерном компьютере сгенерировалось достаточно подстановок для того, чтобы найти 4 КШЗ-неэквивалентных перестановки, что говорит об эффективности предложенного метода.

Дополнительные тесты показали, что для нелинейности больше 102, подстановки не являются оптимальными по показателю алгебраического иммунитета. Однако существуют перестановки с нелинейностью 104 (106) и алгебраическим иммунитетом 2, в которых количество уравнений системы незначительное (начиная от двух).

Таблица 2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C4	CA	FF	B1	BE	2C	6F	C2	AA	62	3F	84	2B	F0	5C	30
1	86	A5	6B	DA	BF	31	4B	40	52	3B	02	79	27	EA	BA	61
2	BD	69	44	63	0C	72	B0	1A	3C	70	76	E7	CB	19	14	C8
3	7B	22	11	8B	99	9B	B9	20	92	FC	7A	6A	DD	D0	4C	EB
4	74	C1	53	D5	AE	AB	09	34	C0	F1	59	B8	57	F5	D4	DB
5	95	1D	15	A3	E8	A1	D9	C5	88	67	39	A2	E1	96	F2	37
6	A0	41	FB	47	CC	46	4D	56	8D	3A	A6	FE	4A	BB	04	B4
7	D8	94	AD	87	75	33	83	DE	68	06	51	18	0E	BC	A4	E4
8	F9	64	E3	85	8E	66	F7	D3	B5	CF	32	F8	60	CE	17	ED
9	7F	49	8F	4E	5F	E5	E9	1E	B7	0A	7C	4F	A9	0D	C7	0F
A	B6	77	01	5E	13	D1	AF	91	9D	36	2A	48	58	A7	5B	FD
B	D7	D6	16	5D	93	1B	98	80	DC	C3	7E	CD	2F	3E	03	F3
C	54	6C	0B	B3	35	E0	38	E6	C9	EC	5A	7D	73	21	9A	25
D	F6	C6	42	90	6E	12	07	8A	8C	DF	9F	82	29	81	89	EE
E	1C	00	28	05	2E	10	26	43	08	65	9C	9E	78	FA	3D	45
F	EF	AC	A8	71	50	1F	97	2D	24	6D	B2	55	E2	23	D2	F4

Выводы

Предложен метод, позволяющий генерировать подстановки для применения в современных блочных симметричных шифрах с высокими требованиями стойкости к различным типам атак. Новый метод основан на уже известном методе градиентного спуска. Предложенный алгоритм ориентирован на векторный случай. Он позволяет находить подстановки с заданными свойствами, в отличие от предыдущего, где находились лишь отдельные булевы функции.

Список литературы: 1. *Y. Crama and P.L. Hammer.* Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications v. 2. Cambridge University Press, 2010. isbn: 9780521847520. 2. *Oliynykov R.* An Impact Of S-Box Boolean Function Properties To Strength Of Modern Symmetric Block Ciphers / R. Oliynykov, O. Kazymyrov // Радиотехника. – 2011. – Вип. 166. – С. 11-17. 3. *Vincent Rijmen.* "Cryptanalysis and design of iterated block ciphers". Doctoral thesis. K.U.Leuven, 1997. 4. *Казимиров А.В.* Использование векторных функций при генерации подстановок для симметричных криптографических преобразований / А.В. Казимиров, Р.В. Олейников // Прикладная радиоэлектроника. – 2012. 5. *Budaghyan L.* Verification of Restricted EA-Equivalence for Vectorial Boolean Functions / L. Budaghyan, O. Kazymyrov // Arithmetic of finite Fields. 4th International Workshop, WAIFI 2012. 6. *Кузнецов А.А.* Построение криптографических функций с использованием метода градиентного спуска / А.А. Кузнецов, Ю.А. Избенко, И.В. Московченко // Системи озброєння і військова техніка. – Х. : ХУПС, 2006. – Вип. 4 (8). – С. 70-74. 7. *W. Millan, A. Clark, E. Dawson.* Smart Hill Climbing Finds Better Boolean Functions, In Proceedings of the Workshop on Selected Areas on Cryptography, SAC'97. Springer-Verlag (1997), 50-63. 8. *J. Daemen and V. Rijmen.* "AES proposal: Rijndael". In: First Advanced Encryption Standard (AES) Conference. 1998. 9. *О. А. Логачев,* А. А. Сальников, В. В. Ященко. Булевы функции в теории кодирования и криптологии. – М. : МЦНМО, 2004. – 470 с. 10. *Yuyin Yu* Constructing differential 4-uniform permutations from know ones / Yuyin Yu, Mingsheng Wang, Yongqiang Li. Electronic form: http://eprint.iacr.org/2011/047.pdf

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 10.11.2013