УДК 681.3.06

Л.С. Сорока[1], А.А. Кузнецов[2], И.В. Московченко[2], С.А. Исаев[1]

[1] *Харьковский национальный университет им. В.Н. Каразина, Харьков*
[2] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ФОРМИРОВАНИЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН ДЛЯ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Исследуются математические модели и вычислительные методы формирования нелинейных узлов замен симметричных криптографических средств защиты информации. Предлагается вероятностная модель формирования нелинейных узлов замен для блочных симметричных криптоалгоритмов. В основе предлагаемых моделей лежит вероятностный отбор криптографических функций с требуемыми показателями стойкости. Сформированы блоки нелинейной подстановки, которые обладают улучшенными криптографическими свойствами, что позволяет улучшить показатели безопасности современных информационных систем и технологий.

Ключевые слова: *нелинейный узел замен, нелинейность, сбалансированность, автокорреляция, корреляционный иммунитет, критерий распространения.*

Введение

Постановка проблемы в общем виде и анализ литературы. Важное место в обеспечении безопасности информации в современных информационно-телекоммуникационных системах занимают симметричные криптографические средства защиты информации [1 – 5]. Их построение основывается на развитом математическом аппарате теории секретных систем, криптографии и математической теории связи [8 – 11]. В то же время опыт практического использования существующих средств защиты информации показывает, что применяемые на практике системы не обеспечивают современных требований по безопасности информации. Это сопряжено, в первую очередь, с уязвимостью нелинейных узлов замен существующих средств защиты информации к современным методам криптоанализа [6, 7]. Таким образом, актуальной задачей является разработка предложений по совершенствованию симметричных средств защиты информации путем разработки новых подходов и способов построения нелинейных узлов замен с улучшенными свойствами.

Целью данной статьи является разработка вероятностной модели формирования нелинейных узлов замен для симметричных криптографических средств защиты информации.

1. Математическая модель нелинейных узлов замен симметричных средств защиты информации

Математическая модель нелинейных узлов замен блочных симметричных средств защиты информации предложена в [8], в соответствии с которой внутренняя структура и формальное аналитическое описание задается следующими элементами.

1. Множество A входных векторов $a = (a_1, a_2, ..., a_m)$, $a_i \in GF(2)$, $|A| = 2^m$;

2. Множество B выходных векторов $b = (b_1, b_2, ..., b_m)$, $b_i \in GF(2)$, $|B| = |A| = 2^m$;

3. Множество криптографических булевых функций $F = \{f_1, f_2, ..., f_m\}$, представимых в алгебраической нормальной форме:

$$\begin{cases} f_1(x_1,...,x_m) = c_{1,0} \oplus \bigoplus\limits_{i=1}^{m} c_{1,i}x_i \oplus \bigoplus\limits_{1\le i<j\le m} c_{1,ij}x_ix_j \oplus ... \\ ... \oplus c_{1,12...m}x_1x_2...x_m \\ f_2(x_1,...,x_m) = c_{2,0} \oplus \bigoplus\limits_{i=1}^{m} c_{2,i}x_i \oplus \bigoplus\limits_{1\le i<j\le m} c_{2,ij}x_ix_j \oplus ... \\ ... \oplus c_{2,12...m}x_1x_2...x_m \\ ... \\ f_m(x_1,...,x_m) = c_{m,0} \oplus \bigoplus\limits_{i=1}^{m} c_{m,i}x_i \oplus \bigoplus\limits_{1\le i<j\le m} c_{m,ij}x_ix_j \oplus ... \\ ... \oplus c_{m,12...m}x_1x_2...x_m \end{cases} \quad (1)$$

4. Система ограничений:

$$\left\{ Сб_f, N_f \ge N_{тр}, КИ_f(k_1), КР_f(k_2), AC_f \le AC_{тр} \right\}, \quad (2)$$

где $Сб_f$ – требование сбалансированности функции; N_f – значение нелинейности функции; $КИ_f(k_1)$ – степень корреляционного иммунитета функции; $КР_f(k_2)$ – степень критерия распространения функции; AC_f – значение автокорреляция функции; $N_{тр}$ – требуемое значение нелинейности; k_1 – требуемая степень корреляционного иммунитета; k_2 – требуемая степень критерия распространения; $AC_{тр}$ – требуемое значение автокорреляции.

Все функции из множества $F = \{f_1, f_2, ..., f_m\}$ удовлетворяют системе ограничений (2). Узлы замен в соответствии с предложенной моделью зада-

ются значениями функций из множества $F=\{f_1,f_2,...,f_m\}$. Любая функция $\overline{f_\varsigma}(x_1,x_2,...,x_m)$, полученная линейной комбинацией функций из множества $F=\{f_1,f_2,...,f_m\}$:

$$\overline{f}_\varsigma(x_1,x_2,...,x_m)=f_i(x_1,x_2,...,x_m)\oplus$$
$$\oplus f_j(x_1,x_2,...,x_m)\oplus...\oplus f_l(x_1,x_2,...,x_m),$$
$$f_i(x_1,x_2,...,x_m),f_j(x_1,x_2,...,x_m),...$$
$$...,f_l(x_1,x_2,...,x_m)\in F$$

удовлетворяет системе ограничений (2) с возможно другими граничными значениями.

Введем следующие обозначения:

$$\begin{cases}\overline{f}_1(x_1,...,x_m)=f_1(x_1,x_2,...,x_m);\\ \overline{f}_2(x_1,...,x_m)=f_2(x_1,x_2,...,x_m);\\ ...\\ \overline{f}_m(x_1,...,x_m)=f_m(x_1,x_2,...,x_m);\\ \overline{f}_{m+1}(x_1,...,x_m)=f_1(x_1,x_2,...,x_m)\oplus\\ \oplus f_2(x_1,x_2,...,x_m);\\ ...\\ \overline{f}2^m-1(x_1,...,x_m)=f_1(x_1,x_2,...,x_m)\oplus\\ \oplus f_2(x_1,x_2,...,x_m)\oplus...f_m(x_1,x_2,...,x_m).\end{cases}$$

Основные криптографические показатели нелинейных узлов замен (сбалансированность Сб*, нелинейность N*, степень корреляционного иммунитета КИ*, степень критерия распространения КР* и значение автокорреляции АС*) оцениваются по критерию минимального риска:

$$\begin{cases}Сб^*=Сб_{\overline{f}_1}\wedge Сб_{\overline{f}_2}\wedge...\wedge Сб_{\overline{f}_{2^m-1}};\\ N^*=\min\left\{N_{\overline{f}_1},N_{\overline{f}_2},...,N_{\overline{f}_{2^m-1}}\right\};\\ КИ^*(k)=\min\left\{КИ_{\overline{f}_1}(k),КИ_{\overline{f}_2}(k),...,КИ_{\overline{f}_{2^m-1}}(k)\right\};\\ КР^*(k)=\min\left\{КР_{\overline{f}_1}(k),КР_{\overline{f}_2}(k),...,КР_{\overline{f}_{2^m-1}}(k)\right\};\\ AC^*=\max\left\{AC_{\overline{f}_1},AC_{\overline{f}_2},...,AC_{\overline{f}_{2^m-1}}\right\},\end{cases}$$

где $Сб_{\overline{f}_\varsigma}$ – показатель сбалансированности (да/нет); $N_{\overline{f}_\varsigma}$ – показатель нелинейности; $КИ_{\overline{f}_\varsigma}(k)$ – степень корреляционного иммунитета; $КР_{\overline{f}_\varsigma}(k)$ – степень критерия распространения; $AC_{\overline{f}_\varsigma}$ – значение автокорреляции булевой функции $\overline{f_\varsigma}(x_1,x_2,...,x_m)$.

Таким образом, предложенная в [8] математическая модель нелинейных узлов замен блочных симметричных средств защиты информации, на основе аналитического описания основных структурных компонентов накладываемой системы ограничений по нелинейности, сбалансированности, корреляционному иммунитету, критерию распространения и автокорреляции, позволяет в терминах булевой алгебры описывать внутреннюю структуру нелинейных узла замен и оценивать основные показатели их эффективности.

2. Разработка вероятностной модели формирования нелинейных узлов замен для симметричных криптографических средств защиты информации

В соответствии с формальным аналитическим описанием нелинейных узлов замен для симметричных криптографических средств защиты информации задача синтеза нелинейных блоков подстановок с улучшенными свойствами состоит в поиске совокупности (множества) компонентных криптографических булевых функций $F=\{f_1,f_2,...,f_m\}$, задающих функциональное соответствие множеств входных векторов и выходных векторов, т.е. определяющих отображение $\varphi: A\to B$, и удовлетворяющих системе ограничений (2) на криптографические показатели. Кроме того, в соответствии с математической моделью, соответствующей системе ограничений должны так же удовлетворять и компонентные булевы функции $\overline{f}_i(x_1,...,x_m)$, полученные посредством линейной комбинацией булевых функций $f_i(x_1,...,x_m)$ из множества F.

Таким образом, синтез нелинейного узла замен можно реализовать итеративной процедурой поэлементного вероятностного формирования множества F с последовательной проверкой криптографических свойств функций на соответствие установленной системе ограничений. Следовательно, вероятностная модель формирования нелинейного узла замен описывается следующими структурными элементами (см. рис. 1):

1. *Система ограничений по нелинейности и автокорреляции криптографических булевых функций*. Используется как исходная информация, задающая основные параметры вычислительного метода формирования криптографических булевых функций посредством градиентного поиска.

2. *Процедуры вычислительного поиска криптографической булевой функции методом градиентного спуска*. По введенным ограничениям с использованием метода градиентного спуска осуществляется вероятностный поиск булевой функции. Результатом является случайно сформированная булева функция, удовлетворяющая требуемым значениям нелинейности и автокорреляции.

3. *Система ограничений на компонентные криптографические булевы функции и их линейные комбинации*. Используется как исходная информация, задающая основные параметры отбора случайно формируемых булевых функций, удовлетворяю-

щих требуемым значениям нелинейности и автокорреляции.

4. *Процедуры проверки выполнения системы ограничений на компонентные функции и их линейные комбинации*. Формируемые булевы функции с требуемыми значениями нелинейности и автокорреляции подвергаются проверке на соответствие системным требованиям, т.е. на пригодность использования в совокупности с другими булевыми функциями.

5. *Процедуры отбора функций, удовлетворяющих заданным требованиям*. Функции, прошедшие проверку на соответствие системным требованиям, отбираются для дальнейшего использования в нелинейном узле замен.

6. *Процедуры отбраковки функций, не удовлетворяющих заданным требованиям и формирование запроса на следующую функцию*. Функции, не прошедшие проверку на соответствие системным требованиям отбраковываются (не используются). Формируется запрос на вероятностный поиск следующей булевой функции с помощью метода градиентного спуска.

7. *Формирование множества компонентных криптографических булевых функций и соответствующей таблицы замен*. Из отобранных по критерию соответствия системным требованиям булевых функций формируется множество F, соответствующая таблица замен и синтезируется устройство, реализующее заложенную в него логику преобразований.

В ходе проведенных исследований с использованием разработанного пакета программ сформированы 4 нелинейные булевы функции над V_8, удовлетворяющие системе ограничений:

$$\{Сб_f,\ N_f \ge 112,\ КИ_f(0),\ КР_f(1),\ AC_f \le 24\}.$$

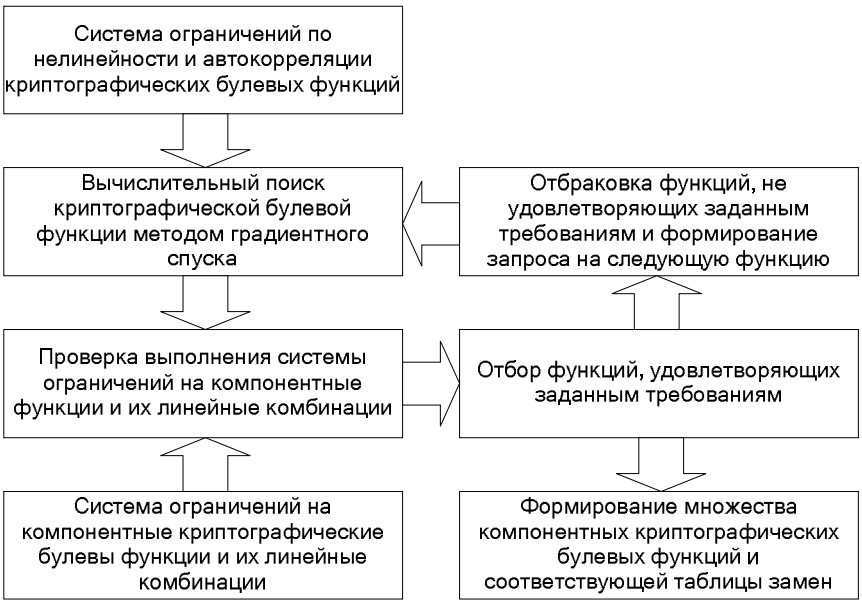

Рис. 1. Основные элементы предлагаемой вероятностной модели формирования нелинейных узлов замен

Любая функция $\overline{f_\varsigma}(x_1, x_2, ..., x_m)$, полученная линейной комбинацией функций $\{f_1, f_2, f_3, f_4\}$, также является сбалансированной и удовлетворяет системе ограничений:

$$\{Сб_f,\ N_f \ge 110,\ КИ_f(0),\ КР_f(1),\ AC_f \le 56\}.$$

Для построения блока нелинейных замен, реализующего отображение элементов из $GF(2^8)$, дополнительно сформированы четыре булевы функции $\{f_5, f_6, f_7, f_8\}$ методом случайной генерации. Нелинейные булевы функции $\{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ аналитически задают узел замен, формализовано описывают его внутреннюю структуру и определяют основные показатели эффективности (4).

Представим входной вектор $a = (a_1, a_2, ..., a_8)$ в виде $a = (x, y)$, где $x = (a_1, a_2, a_3, a_4)$, $y = (a_5, a_6, a_7, a_8)$. Выходной вектор $b = (b_1, b_2, ..., b_8)$ представим в виде $b = (z, u)$, где $z = (b_1, b_2, b_3, b_4)$, $u = (b_5, b_6, b_7, b_8)$.

Таблица замен сформированного нелинейного узла замен представлена в табл. 1, где каждая строка соответствует конкретному значению x, каждый столбец соответствует конкретному значению y, в ячейках таблицы указаны соответствующие значения z и u, а собственные значения x, y, z и u представлены в шестнадцатеричном формате.

Как следует из данных, приведенных в табл. 1, сформированный нелинейный узел замен реализует биективное отображение и может быть использован при построении криптографических средств защиты информации.

Таблица замен и соответствующий нелинейный узел сформированы с использованием разработанного метода формирования криптографических булевых функций, его основные криптографические свойства соответствуют приведенной системе ограничений.

Таблица 1

Таблица замен
сформированного нелинейного узла

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	f0	4a	ed	f4	d1	db	bc	67	7d	f7	a0	fb	6c	d6	51	ba
	1	eb	7f	46	c3	aa	ef	e7	02	f6	72	ab	3e	37	52	3b	4e
	2	3f	15	ec	85	5a	a4	4d	66	03	39	30	b9	ca	78	91	0a
	3	54	11	e3	82	fd	f1	b6	13	48	2c	2b	6e	f9	ac	7b	2e
	4	5f	b5	f2	69	71	cb	4c	97	92	e8	ff	25	dc	96	79	ea
	5	14	60	99	0c	6a	be	d7	c2	89	6d	40	c1	bf	12	7a	ae
	6	70	c8	93	d8	ee	94	2d	a6	cc	76	6f	b4	e2	a8	81	3a
	7	6b	9f	58	3d	65	01	16	63	a7	53	64	41	09	1c	8a	ce
	8	a1	bb	cd	b3	08	da	ad	36	d2	88	9d	24	33	e9	1f	f5
	9	4b	af	e6	d3	2a	0e	b7	32	28	8c	95	c0	c9	5c	84	b0
	A	7e	d4	8d	26	2f	05	7c	07	3c	56	8f	d0	1d	df	8e	c5
	B	04	90	55	b2	45	31	86	5b	06	62	d5	10	27	a2	c4	50
	C	9e	74	43	68	b1	1a	dd	fe	bd	87	00	9b	f3	29	1e	75
	D	34	20	a9	18	9a	de	77	22	c7	73	38	cf	d9	fc	44	e0
	E	e1	1b	42	49	4f	a5	9c	47	23	19	80	0b	0d	57	5e	e5
	F	35	21	c6	a3	8b	0f	98	5d	17	83	e4	61	59	b8	fa	f8

Выводы

Использование предложенной вероятностной модели формирования нелинейных узлов замен позволяет формировать блоки нелинейной подстановки для симметричных криптографических средств защиты информации. Установлено, что формируемые таким образом нелинейные узлы замен обладают улучшенными свойствами, такими как нелинейность, автокорреляция, корреляционный иммунитет и критерий распространения, их применение в симметричных криптографических средствах защиты информации позволяет улучшить показатели безопасности информационных систем и технологий.

Список литературы

1. Барсуков В.С. Технологии электронных коммуникаций: В 20 т. Т.20: Безопасность связи в каналах телекоммуникаций / В.С. Барсуков, С.В. Дворянкин, И.И. Шеремет. – М.: Электронные знания, 1992. – 122 с.

2. Береза А.С. Основы построения АСУ. Основы структурного анализа и синтеза АСУ / А.С. Береза. – Х.: ХВУ, 1997. – 210 с.

3. Береза А.С. Основы построения АСУ. Системотехнические основы построения АСУ / А.С. Береза. – Х.: ХВУ, 1996. – 355 с.

4. Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.

5. Мамаев Е. Технологии защиты информации в Интернете / Е. Мамаев. – СПб.: ИД Питер, 2001. – 848 с.

6. Потий А.В. Исследование методов криптоанализа поточных шифров. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. / А.В. Потий, Ю.А. Избенко // ДСТСЗІ СБУ, НТУ "КПІ". – 2003. – № 6. – С. 34-49.

7. Потий А.В. Система показателей оценки эффективности функционирования схем поточного шифрования // Радиотехника: Всеукраинский межведомственный научно-технический сборник / А.В. Потий, Ю.А. Избенко. – 2003. – № 123. – С. 146-158.

8. Столлингс В. Компьютерные системы передачи данных / В. Столлингс. – М.: Вильямс, 2002. – 928 с.

9. Шеннон К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике. – М.: Инлит. – 1963. – С. 333-402.

10. Rueppel R.A. Analysis and Design of Stream Ciphers / R.A. Rueppel. – Berlin, Springer-Verlag, 1986.

11. B.Schneier. Applied Cryptography. 2nd edition. / B.Schneier. John Wiley & Sons, New York,1996.

12. Кузнецов А.А. Разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения / А.А. Кузнецов, И.В. Московченко // Радіоелектронні і комп'ютерні системи. – 2008. – №2 (29). – С. 94-100.

Поступила в редколлегию 12.05.2009

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный университет сельского хозяйства им. П. Василенко, Харьков.

ІМОВІРНА МОДЕЛЬ ФОРМУВАННЯ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІН ДЛЯ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Л.С. Сорока, О.О. Кузнецов, І.В. Московченко, С.О. Ісаєв

Досліджуються математичні моделі та обчислювальні методи формування нелінійних вузлів замін симетричних криптографічних засобів захисту інформації. Запропонована імовірна модель формування нелінійних вузлів замін для блокових симетричних криптоалгоритмів. В основі моделей, що запропоновані, лежить імовірнісний відбір криптографічних функцій з потрібними показниками стійкості. Сформовані блоки нелінійної підстановки, які володіють поліпшеними криптографічними властивостями, що дозволяє покращити показники безпеки сучасних інформаційних систем і технологій.

Ключові слова: *нелінійних вузол замін, нелінійність, збалансованість, автокореляція, кореляційний імунітет, критерій розповсюдження.*

PROBABILISTIC MODEL OF SUBSTITUTION BOX GENERATION FOR SYMMETRIC CRYPTOGRAPHIC METHODS OF INFORMATION SECURITY

L.S. Soroka, A.A. Kuznetsov, I.V. Moskovchenko, S.A. Isaev

The probabilistic model of forming of nonlinear knots of replacements is offered for sectional symmetric cryptoalgorithms. Offered models the probabilistic selection of cryptographic functions is underlaid with the required indexes of firmness. The blocks of nonlinear substitution, which possess the improved cryptographic properties, are formed, that allows to improve the indexes of safety of the modern informative systems and technologies.

Keywords: *nonlinear node of the change, nonlinear, balanced, autocorrelation, correlation immunity, criterion of the spreading.*