УДК 004.056.55

АНАЛИЗ И СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕНЫ СОВРЕМЕННЫХ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

А.А. КУЗНЕЦОВ, И.Н. БЕЛОЗЕРЦЕВ, А.В. АНДРУШКЕВИЧ

Рассматриваются современные блочные симметричные шифры и применяемые в них нелинейные узлы замены (S-блоки). Анализируются показатели и критерии эффективности S-блоков: нелинейность, сбалансированность, корреляционный иммунитет, критерий распространения, автокорреляция и др. Проводятся сравнительные исследования эффективности нелинейных узлов замены современных блочных шифров.

Ключевые слова: блочный симметричный шифр, нелинейный узел замен, криптографическая функция.

ВВЕДЕНИЕ

Интенсивное развитие современных компьютерных систем и технологий, применение облачных вычислений, мобильных устройств удаленного подключения к информационно-коммуникационным сетям приводят к значительному усложнению процедур защиты обрабатываемой и передаваемой информации. Необходимым условием выполнения основных услуг безопасности является применение криптографических средств защиты информации [1].

Блочные симметричные шифры (БСШ) являются одним из наиболее распространенных и эффективных криптографических примитивов [1–5]. Помимо обеспечения услуги конфиденциальности они применяются как основной конструктивный элемент других примитивов (функций хеширования, генераторов псевдослучайных последовательностей и пр.). Важность разработки, исследования и обоснования условий применения современных БСШ подтверждается количеством и масштабностью международных криптографических конкурсов, проведенных в последние годы. Так, например, международные проекты AES, NESSIE, CRYPTREC и пр. были ориентированы на разработку БСШ, удовлетворяющих высоким требованиям криптографической стойкости и эффективности программной и аппаратной реализации. Результатом проведения этих и многих других исследовательских проектов являются принятые в последние годы международные и национальные стандарты криптографического преобразования [2–5].

Разработка, исследование и обоснование условий применения современных БСШ является чрезвычайно сложной и трудоёмкой задачей [1]. Стандартизированный криптоалгоритм должен обеспечивать высокий уровень стойкости, обладать требуемым быстродействием и эффективно функционировать на различных вычислительных платформах [1, 6]. При этом требуемый уровень стойкости БСШ обеспечивается эффективностью составляющих: схемы разворачивания секретного ключа (ключевого расписания), выбранной базовой структуры алгоритма, линейных и нелинейных преобразований, и пр. В данной работе акцентируется внимание на нелинейных узлах замен, критериях и показателях их эффективности. Приводятся результаты сравнительных исследований различных свойств S-блоков современных БСШ, стандартизированных на международном и национальном уровнях [2–5].

1. УЗЛЫ ЗАМЕН СОВРЕМЕННЫХ БСШ

Рассмотрим нелинейные узлы замен современных БСШ, проведем исследования свойств применяемых S-блоков по различным показателям и критериям эффективности [7–12].

БСШ «Калина» – национальный стандарт Украины ДСТУ 7624:2014 [5], разработанный ЧАО «ИИТ». Алгоритм поддерживает размер блока и длину ключа шифрования 128, 256 и 512 бит (длина ключа равна размеру блока или в два раза превышает его), обеспечивая нормальный, высокий и сверхвысокий уровень стойкости. Цикловое преобразование использует таблицы подстановки, приведенные на рис. 1–4 [5].

БСШ «Кузнечик» – алгоритм шифрования, стандартизированный в России как ГОСТ 34.12-2015 [3]. Длина входного блока – 128 бит, длина ключа – 256 бит. Процесс зашифрования основан на последовательном применении нескольких однотипных раундов, каждый из которых содержит сложение с раундовым ключом, нелинейное и линейное преобразование. Нелинейное преобразование использует фиксированный S-блок, представленный на рис. 5.

БСШ «BelT» – государственный стандарт симметричного шифрования и контроля целостности Республики Беларусь. Стандартизирован как СТБ 34.101.31-2011 [4] и введен в действие в 2011 году. Это блочный криптоалгоритм с 256-битным ключом и 8 циклами, оперирующий 128-битными словами. S-блок БСШ «BelT» приведен на рис. 6.

БСШ «AES» – криптоалгоритм, стандартизированный в США как FIPS-197. На международном уровне стандартизирован в ISO/IEC 18033-3 [2]. Обрабатывает 128-битные блоки данных, используя ключи шифрования длиной 128, 192 и 256 бит. В зависимости от длины ключа

выполняется 10, 12 или 14 раундов шифрования. Таблица подстановок БСШ «AES» приведена на рис. 7.

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

Рис. 1

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

Рис. 2

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

Рис. 3

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

Рис. 4

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

Рис. 5

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

Рис. 6

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

Рис. 7

БСШ «Camellia» – алгоритм шифрования с размером блока 128 бит и ключа 128, 192, 256 бит. Один из финалистов европейского конкурса NESSIE (наряду с AES и Shacal-2), разработка японских компаний Nippon Telegraph and Telephone Corporation и Mitsubishi Electric Corporation. Рекомендован CRYPTREC для промышленного и государственного использования. Стандартизирован на международном уровне в ISO/IEC 18033-3 [2]. Цикловая функция использует нелинейное преобразование, блок линейного рассеивания и байтовую перестановку. Четыре S-блока этого шифра приведены на рис. 8–11.

БСШ «CAST» – канадский криптоалгоритм, разработанный Карлайслом Адамсом (Carlisle Adams) и Стаффордом Таваресом (Stafford Tavares). Использует 64-битовый блок и 128-битовый ключ, 16 раундов преобразования. В ISO/IEC 18033-3 [2] стандартизирован алгоритм CAST-128, который использует восемь S-блоков, реализующих отображение 8-ми битных входных векторов в 32-х битные выходные. Четыре S-блока используются в раундовой функции

алгоритма, оставшиеся четыре используются в схеме разворачивания ключа. В данной работе исследованы все восемь таблиц подстановок. Их описание приведено в [2].

БСШ «SEED» – симметричный криптоалгоритм, разработанный корейским агентством информационной безопасности (Korean Information Security Agency, KISA) в 1998 году. Также стандартизирован на международном уровне в ISO/IEC 18033-3 [2]. Алгоритм широко используется финансовыми и банковскими структурами, производственными предприятиями и бюджетными учреждениями Южной Кореи, а также в протоколах TLS и S/MIME. Алгоритм представляет собой сеть Фейстеля с 16 раундами, 128-битовыми блоками и 128-битовым ключом. Использует две таблицы подстановки, полученные на основе дискретного возведения в степень (см. рис. 12, 13).

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

Рис. 8

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

Рис. 9

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

Рис. 10

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

Рис. 11

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

Рис. 12

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

Рис. 13

2. КРИТЕРИИ И ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН

Рассмотрим критерии и показатели эффективности нелинейных узлов замен, непосредственно влияющие на уровень стойкости современных БСШ к различным криптоаналитическим атакам.

Под эффективностью функционирования любой технической системы понимают соответствие полученных результатов функционирования требуемому. Очевидно, что основным требованием к нелинейным узлам является обеспечение стойкости к известным методам криптографического анализа. Другими словами, нелинейный узел будем считать эффективным, если он обеспечивает стойкость к известным на сегодняшний день методам криптографического анализа.

В большинстве известных работ в области анализа и синтеза нелинейных узлов замен современных БСШ используется математический аппарат криптографических булевых функций [7–12]. При этом каждый S-блок представляется совокупностью компонентных булевых функций, свойства которых характеризуют эффективность нелинейного узла замен. В качестве основных критериев и показателей эффективности используют [7–12]: сбалансированность и нелинейность компонентных булевых функций; корреляционный иммунитет; критерий распространения; алгебраическая степень; значение функции автокорреляции.

Введем основные понятия и определения, используемые в дальнейшем при оценке эффективности нелинейных узлов замен [7–12].

Булевой функцией f от n переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, ..., x_n)$ длины n в поле $GF(2)$. Обычно булевы функции представляются в алгебраической нормальной форме. *Поле* $GF(2^n)$ состоит из 2^n векторов α_i: $\alpha_0 = (0,...,0,0)$, $\alpha_1 = (0,...,0,1)$,..., $\alpha_{2^n-1} = (1,...,1,1)$, $\alpha_i \in V_n$, где V_n – векторное пространство в $GF(2^n)$.

Последовательностью функции f называется (1,-1)-последовательность, определенная как $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, ..., (-1)^{f(\alpha_{2^n-1})})$. *Таблицей истинности функции f* называется (0,1)-последовательность, определенная как $(f(\alpha_0), f(\alpha_1), ..., f(\alpha_{2^n-1}))$.

Последовательность функции f является *сбалансированной*, если ее (0,1)-последовательность ((1,-1)-последовательность) содержит одинаковое количество нулей и единиц (единиц и минус единиц). Функция f является сбалансированной, если сбалансирована ее последовательность.

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

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

Аффинной функцией f называется функция вида $f = a_1x_1 \oplus ... \oplus a_nx_n \oplus c$, где a_j, $c \in GF(2)$, $j = 1, 2,..., n$. Функция f называется линейной, если $c = 0$.

Весом Хэмминга вектора α, обозначаемым как $W(\alpha)$, является количество единиц в векторе (последовательности). *Расстоянием Хэмминга d(f,g)* между последовательностями двух функций f и g является количество позиций, в которых различны последовательности этих функций.

Нелинейность N_S преобразования – минимальное расстояние Хэмминга между выходной последовательностью S и всеми выходными последовательностями аффинных функций над некоторым полем:

$$N_s = \min\{d(S,\varphi)\},$$

где φ – множество аффинных функций.

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

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

где φ – множество аффинных функций.

Для произвольной функции f нелинейность N_f над $GF(2^n)$ может достигать $N_f \le 2^{n-1} - 2^{n/2-1}$. Для сбалансированной функции f над $GF(2^n)$ ($n \ge 3$) нелинейность N_f может достигать:

$$N_f \le \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2, n = 2k \\ \left\lfloor\left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor\right\rfloor, n = 2k = 1, \end{cases}$$

где $\lfloor\lfloor x \rfloor\rfloor$ – максимальное четное целое, меньшее либо равное 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:

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

Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша: функция f над полем $GF(2^n)$ имеет корреляционный иммунитет порядка k, $КИ(k)$, если ее преобразование Уолша удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$:

$$\forall\omega\in V_n\ F(\varpi) = 0 \qquad (f) = k\ .$$

Преобразование Уолша $F(\omega)$ функции f над полем $GF(2^n)$ определяется как принимающая действительные значения функция

$$F(\omega) = 2^{-n}\sum\nolimits_x (-1)^{f(x)\oplus\langle\varpi,x\rangle},$$

где $\omega \in V_n$, $f(x)$, $\langle\omega,x\rangle \in N$ ($\langle\omega, x\rangle$ – скалярное произведение $w_1x_1 \oplus ... \oplus w_nx_n$).

Корреляционно-иммунная функция k-го порядка – функция, обладающая корреляционным иммунитетом порядка k. Сбалансированные корреляционно-иммунные функции называются *эластичными функциями*.

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

– *критерию распространения* относительно вектора a, КР(a), если функция $f(x) \oplus f(x \oplus a)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, ..., x_n)$

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

– *критерию распространения степени* k, КР(k), если удовлетворяется критерий распространения относительно всех векторов $a \in V_n$ при $1 \le W(a) \le k$:

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

– *строгому лавинному критерию* (СЛК), если f удовлетворяет критерию распространения степени 1:

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

Алгебраическая степень deg(f) является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме.

Автокорреляционная функция $\hat{r}(s)$ для $s\in 0...2^n-1$ определена как

$$\hat{r}(s) = \sum_{x=0}^{2^n-1}\hat{f}(x)\hat{f}(x\oplus s).$$

Говорят, что функция f удовлетворяет *характеристике распространения* m, если

$$(1\le|s|\le m)\Rightarrow\left|\hat{r}(s)\right| = 0.$$

Аналогично, автокорреляция $AC(f)$ функции f определяется как модуль наибольшего значения $\hat{r}(s)$:

$$AC(f) = \max_{s\ne 0}\left|\sum_x \hat{f}(x)\hat{f}(x\oplus s)\right| = \max_{s\ne 0}\left|\hat{r}(s)\right|.$$

Автокорреляция обеспечивает утечку информационного потока со входа на выход функции. В некоторых случаях очень сильная взаимосвязь может быть представлена как линейная структура (для которых справедливы равенства $f(x) \oplus f(x\oplus s) = 1$ или $f(x) \oplus f(x\oplus s) = 0$). Они, как правило, избегаемы.

Рассмотренные критерии и показатели эффективности S-блоков отражают способность нелинейного узла противостоять атакам определенного типа. Нелинейность, критерий распространения и корреляционная иммунность характеризуют способность противостоять корреляционным атакам, алгебраическая степень и автокорреляция – аналитическим атакам, сбалансированность – статистическим.

Проведем исследования эффективности нелинейных узлов замен современных БСШ «Калина», «Кузнечик», «BelT», «AES», «SEED», «Camellia», «CAST».

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

Для проведения экспериментальных исследований эффективности различных S-блоков в среде IntelliJ IDEA 15 Community edition на языке Java был разработан программный вычислительный комплекс. Он позволяет рассчитать основные показатели эффективности нелинейных узлов замены: сбалансированность, нелинейность, автокорреляцию, алгебраическую степень, степень критерия распространения и корреляционного иммунитета криптографических булевых функций. Показатели эффективности S-блока оцениваются по критерию минимального риска (худший случай) по всем компонентным булевым функциям и их линейным комбинациям. Результаты экспериментальных исследований сведены в табл. 1–5. Использованы следующие обозначения: B – сбалансированность; N – нелинейность; A – автокорреляция; AD – алгебраическая степень; PC – критерий распространения; CI – корреляционная иммунность; f_n – функция, соответствующая n-му выходу S-блока; S-box – показатели эффективности S-блока по критерию минимального риска (худший случай среди всех компонентных булевых функций); Linear combinations (LC) – показатели эффективности S-блока по критерию минимального риска (худший случай среди всех линейных комбинаций булевых функций).

Полученные результаты показали разнообразие мнений разработчиков исследуемых шифров относительно концепций формирования S-блоков. Так, например, БСШ «CAST-128» имеет превосходные результаты по показателям нелинейности, автокорреляции и критерию распространения, однако имеет низкую алгебраическую степень, а также низкие показатели стойкости для линейных комбинаций булевых функций S-блока. Разработчики БСШ «SEED» также сделали упор на увеличение эффективности таблицы подстановки за счет снижения автокорреляции. Однако их S-блок имеет меньшее значение нелинейности, а также является несбалансированным.

Таблица 1

Показатели эффективности подстановок шифра «Калина»

	S_1-блок						S_2-блок						S_3-блок						S_4-блок					
	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI
f_1	+	106	48	7	0	0	+	106	48	7	0	0	+	106	56	7	0	0	+	108	56	7	0	0
f_2	+	106	64	7	0	0	+	106	64	7	0	0	+	104	64	7	0	0	+	104	56	7	0	0
f_3	+	106	56	7	0	0	+	106	56	7	0	0	+	106	56	7	0	0	+	108	64	7	0	0
f_4	+	104	72	7	0	0	+	104	72	7	0	0	+	106	56	7	0	0	+	108	48	7	0	0
f_5	+	104	56	7	0	0	+	104	56	7	0	0	+	108	48	7	0	0	+	104	64	7	0	0
f_6	+	106	56	7	0	0	+	106	56	7	0	0	+	104	56	7	0	0	+	108	56	7	0	0
f_7	+	106	64	7	0	0	+	106	64	7	0	0	+	106	56	7	0	0	+	104	64	7	0	0
f_8	+	106	64	7	0	0	+	106	64	7	0	0	+	104	56	7	0	0	+	108	48	7	0	0
S-box	+	104	72	7	0	0	+	104	72	7	0	0	+	104	64	7	0	0	+	104	64	7	0	0
LC	+	104	72	7	0	0	+	104	72	7	0	0	+	104	72	7	0	0	+	104	72	7	0	0

Таблица 2

Показатели эффективности подстановок шифров «Кузнечик», «BelT», «AES», «Camellia»

	S-блок «Кузнечик»						S-блок «BelT»						S-блок «AES»						S-блок «Camellia»					
	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI
f1	+	104	64	7	0	0	+	106	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f2	+	106	56	7	0	0	+	106	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f3	+	116	24	7	0	0	+	106	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f4	+	104	64	7	0	0	+	104	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f5	+	110	48	7	0	0	+	108	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f6	+	106	64	7	0	0	+	106	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f7	+	102	72	7	0	0	+	108	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f8	+	104	64	7	0	0	+	108	64	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
S-box	+	102	72	7	0	0	+	104	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
LC	+	102	80	7	0	0	+	102	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0

Таблица 3

Показатели эффективности подстановок шифра «SEED»

S_1-блок	B	N	A	AD	PC	CI	S_2-блок	B	N	A	AD	PC	CI
f_1	+	110	40	7	0	0	f_1	+	112	32	7	0	0
f_2	-	111	36	8	0	0	f_2	+	112	32	7	0	0
f_3	+	112	32	7	0	0	f_3	+	112	32	7	0	0
f_4	+	112	40	7	0	0	f_4	+	112	32	7	0	0
f_5	+	110	40	7	0	0	f_5	+	111	36	8	0	0
f_6	-	111	36	8	0	0	f_6	-	113	36	8	0	0
f_7	-	111	36	8	0	0	f_7	+	112	32	7	0	0
f_8	+	111	36	8	0	0	f_8	+	111	36	8	0	0
S-box	-	110	40	7	0	0	S-box	-	111	36	7	0	0
LC	-	109	44	7	0	0	LC	+	111	36	7	0	0

Таблица 4

Показатели эффективности подстановок шифра «CAST-128»

	S_1-блок						S_2-блок						S_3-блок						S_4-блок					
	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI
f1	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f2	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f3	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f4	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f5	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f6	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f7	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f8	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f9	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f10	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f11	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f12	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f13	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f14	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f15	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f16	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f17	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f18	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f19	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f20	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0

f21	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f22	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f23	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f24	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f25	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f26	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f27	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f28	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f29	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f30	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f31	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f32	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
S-box	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
LC	-	88	112	4	0	0	+	92	96	4	0	0	-	92	96	4	0	0	+	92	112	4	0	0

Таблица 5

Показатели эффективности подстановок шифра «CAST-128»

	S_5-блок						S_6-блок						S_7-блок						S_8-блок					
	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI	B	N	A	AD	PC	CI
f1	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f2	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f3	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f4	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f5	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f6	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f7	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f8	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f9	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f10	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f11	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f12	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f13	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f14	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f15	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f16	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0
f17	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f18	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f19	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f20	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f21	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f22	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f23	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f24	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f25	-	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f26	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f27	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f28	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
f29	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f30	+	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
f31	-	120	0	4	8	0	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0
f32	+	120	0	4	8	0	-	120	0	4	8	0	+	120	0	4	8	0	+	120	0	4	8	0
S-box	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0	-	120	0	4	8	0
LC	+	92	144	4	0	0	+	80	112	4	0	0	+	92	96	4	0	0	+	92	128	4	0	0

Таблица подстановки БСШ «AES» имеет высокую алгебраическую степень, хорошие показатели по нелинейности и автокорреляции, однако имеет нулевой критерий распространения. Кроме того, S-блок БСШ «AES» сформирован на основе алгебраической конструкции Нибер-Динга, что создает предпосылки для возможной реализации алгебраического криптоанализа. БСШ «Camellia» показал одинаковые с «AES» результаты. Остальные проанализированные S-блоки не являются алгебраическими, но при этом теряют в нелинейности и автокорреляции.

Таблицы подстановки шифров, утвержденных в качестве государственных стандартов Украины, Российской Федерации и Белоруссии представляют собой наиболее сбалансированное, компромиссное решение. Среди них лучшими показателями обладает S-блок украинского шифра «Калина», вслед за ним идет белорусский «BelT» и российский «Кузнечик».

ВЫВОДЫ

Полученные результаты позволяют судить об основных концепциях формирования нелинейных узлов замен современных БСШ. Как правило, нелинейные узлы разрабатываются с учетом наиболее вероятных угроз и особое внимание уделяется специфическим показателям эффективности. Перспективные шифры должны противостоять всем наиболее распространенным существующим атакам.

Выбранные показатели эффективности нелинейных узлов замен характеризуют первоочередные требования к обеспечению их стойкости. Полученные результаты не позволяют однозначно определить лучший S-бокс, из-за различных концептуальных особенностей в проектировании каждого из них. Однако среди шифров, которые стандартизированы в постсоветских странах, лучшим по показателям эффективности нелинейных узлов замен следует отметить S-блок шифра «Калина». Также стоит обратить внимание на канадский шифр CAST-128, булевы функции в S-блоке которого удовлетворяют критерию распространения степени 8 и обладают нулевой автокорреляцией.

Перспективным направлением дальнейших исследований является анализ свойств нелинейных узлов усложнения поточных криптоалгоритмов, обоснование рекомендаций и предложений по разработке национального стандарта поточного шифрования Украины.

Литература

[1] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навч. закладів. – Харків: Вид-во «Форт», 2013. – 880 с.

[2] Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers (ISO/IEC 18033-3), 80 с.

[3] ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015г. – 25 с.

[4] СТБ 34.101.31-2011 Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. – Минск: Госстандарт, 2011г. – 35 с.

[5] Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Мінекономрозвитку України, 2015. – 238 с.

[6] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІІТ»; кер. І.Д. Горбенко – Харків, 2014, Том 4. – 304 с.

[7] *Bart Preneel.* Analysis and Design of Cryptographic Hash Functions. [Электронный ресурс] – Режим доступа: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

[8] *Carlet C.* Vectorial Boolean functions for // Cambridge Univ. Press, Cambridge. – 95 p. [Электронный ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf

[9] *Carlet C.* Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Электронный ресурс] – Режим доступа: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf

[10] Zhuo Zepeng, Zhang Weiguo On correlation properties of Boolean functions // Chinese Journal of Electronics. Jan, Vol.20, 2011, №1, 143-146 pp.

[11] O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology. -1994. – p. 133-151.

[12] Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – p.219–231.

Поступила в редколлегию 13.11.2015

Кузнецов Александр Александрович, фото и сведения об авторе см. на с. 334.

Белозерцев Иван Никитович, студент факультета компьютерных наук ХНУ им. В.Н.Каразина. Научные интересы: криптография, блочные симметричные шифры, теория обработки и передачи данных.

Андрушкевич Алина Вадимовна, аспирантка ХНУРЭ, инженер 1 кат. кафедры БИТ ХНУРЭ. Научные интересы: анализ стойкости симметричных шифров, криптография и аутентификация.

УДК 004.056.55

Аналіз та порівняльні дослідження нелінійних вузлів замін сучасних блокових симетричних шифрів / О.О. Кузнецов, І.М. Білозерцев, А.В. Андрушкевич // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – № 4. – С. 343–350.

Розглядаються сучасні блокові симетричні шифри і застосовані в них нелінійні вузли заміни (S-блоки). Аналізуються показники та критерії ефективності S-блоків: нелінійність, збалансованість, кореляційний імунітет, критерій розповсюдження, автокореляція та ін. Проводяться порівняльні дослідження ефективності нелінійних вузлів заміни сучасних блокових шифрів.

Ключові слова: блоковий симетричний шифр, нелінійний вузол замін, криптографічна функція.

Табл.: 5. Іл.: 14. Бібліогр.: 12 найм.

UDC 004.056.55

Analysis and comparative research of nonlinear substitution components of the state-of-the-art block ciphers/ A.A. Kuznetsov, I.M. Bilozertsev, A.V. Andrushkevych // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 343–350.

The paper examines state-of-the-art block ciphers and nonlinear substitution components (S-blocks) which are used in them. Properties and criteria of S-block effectiveness such as nonlinearity, balance, correlation immunity, propagation criteria, autocorrelation etc. are analyzed. A comparative research of the effectiveness of nonlinear substitution components of state-of-the-art block ciphers is conducted.

Keywords: symmetric block cipher, nonlinear substitution component, cryptographic function.

Tab.: 5. Fig.: 14. Ref.: 12 items.