УДК 004.056.5

ПРО СЛАБКІСТЬ S ПЕРЕТВОРЕННЯ ШИФРУ СТРУМОК З ЛАНЦЮЖКА КЕРОВАНИХ S-БЛОКІВ

Костянтин Лисицький[1], Катерина Кузнецова[1]

[1] V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
lisickiy@ukr.net, kate.kuznetsova.2000@gmail.com

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
roliynykov@gmail.com

Received on October 2018

Анотація: *Обговорюються особливості побудування S-перетворення шифру Струмок. Зокрема, виконано аналіз пропозиції щодо побудови S-перетворення шифру Струмок з використанням керованих S-блоків. Оцінюються показники його випадковості. Показується, що воно за своєю ефективністю поступається відповідному оригінальному рішенню. З'ясовуються причини таких обставин.*

Ключові слова: *поточний шифр; випадкова підстановка; диференціальна ймовірність; S перетворення; лінійна змішуючи схема.*

1 Вступ

Раніше, в роботі [1], були викладені пропозиції щодо побудови, як попередньо очікувалося, поліпшеної конструкції S перетворення для поточного шифру Струмок. Тоді ми вважали, що застосування для побудови циклової функції ланцюжка з керованих S-блоків має привести до поліпшення динамічних показників приходу багаторазового повторення запропонованої конструкції S перетворення до випадкової підстановці. В даному контексті, під динамічними показниками приходу ітеративного продовження S перетворення до випадкової підстановці, слід розуміти мінімальне число повторень S перетворення в режимі шифрування, вхідного 64-х бітного блоку даних, після якого максимуми диференціальних ймовірностей переходів вхідних різниць у вихідні приходять до асимптотичних значенням, характерних для випадкових підстановок. Відповідні міркування в роботі [1] будувалися на аналізі мінімальної кількості S-блоків, що активізуються на перших циклах шифрування.

У даній роботі ми продовжили дослідження раніше запропонованої конструкції [1] та представляємо додаткові результати експериментів щодо оцінки реального числа S-блоків, які активізуються на кожному циклі при ітеративному продовженні перетворення. В роботі буде показано, що запропонована в [1] конструкція має слабкості, які роблять показники пропонованої конструкції такими, що поступаються оригінальній розробці, в наслідок чого перспективність пропонованої конструкції є явно сумнівною.

2 Альтернативна конструкція S перетворення

Сама конструкція, що була запропонована раніше, в роботі [1], представлена на рис. 1. Дана схема, в своєї основі, повторює конструкцію першого циклу шифру ШУП [2], тільки замість SL перетворень в даному випадку виступають байтові S-блоки (*керовані підстановки*), а замість підсумування за модулем 2 сегментів на вході першого SL перетворення тут використовується інша (*як раніше вважалося, більш ефективна*) схема лінійного змішування, що заснована на багатошаровому підсумуванні за модулем 2 сегментів вхідного блоку даних. Крім того, в даному випадку, підсумування виходу останнього S-блоку виконується тільки з виходом першого S-блоку.

Спочатку здійснюється розбивка вхідного блоку даних з 64 бітів на лівий і правий 32-х бітні підблоки, та формується новий 64-х бітний блок даних, що складається з нового лівого

32-х бітного підблоку, який одержується з допомогою підсумування за модулем 2 лівого і правого 32-х бітних підблоків вихідного блоку даних, і правого підблоку, шо повторює «старий» правий 32-х бітний підблок. Потім здійснюються аналогічні операції з новим лівим напівблоком і далі з новим лівим підблоком чергового напівблоку, де вже він зводиться до байтового розміру.

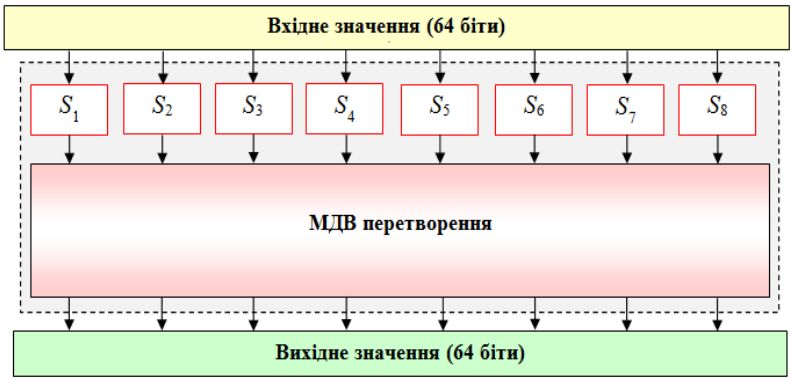

Рис. 1 – S перетворення шифру Струмок

Розміщення рядків з сум байтів після додавання за модулем 2 ілюструється нижче.

Вхідний рядок байтів: X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8

Після першого шару XOR маємо: $X_1 \oplus X_5$, $X_2 \oplus X_6$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

Після другого шару XOR: $X_1 \oplus X_5 \oplus X_3 \oplus X_7$, $X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

Після третього шару XOR маємо хідні блоки даних: $X_1 \oplus X_5 \oplus X_3 \oplus X_7 \oplus X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

В результаті на вході першого S-блоку маємо $X_1 \oplus X_5 \oplus X_3 \oplus X_7 \oplus X_2 \oplus X_6 \oplus X_4 \oplus X_8$ – суму всіх байтів входу.

Аналіз, якій було наведено в роботі [1], виконаний у припущенні, що при активізації будь-якого S-блоку отримують ненульові різниці входу усі наступні S-блоки та зроблений висновок, що при умові, коли для різниць сегментів пар входів виконується умова: $\Delta X_1 \oplus \Delta X_5 = 0$, $\Delta X_1 = \Delta X_5 \neq 0$, $\Delta X_5 = \Delta X_3 = \Delta X_7 = \Delta X_2 = \Delta X_6 = \Delta X_4 = \Delta X_8 = 0$, в запропонованому рішенні активізується мінімум 4-ри S-блоки першого циклу. – Тобто, в гіршому випадку ланцюжок з S-блокових перетворень запускається з п’ятого S-блоку. Отже, на першому циклі маємо 4-ри активних S-блоки, а на двох перших циклах маємо 12-ть активних S-блоків [1]. На трьох циклах активізується вже мінімум близько 20-ти S-блоків. Але як показали результати наступних експериментів, зроблений в роботі [1] висновок виявився хибним! В даній роботі ми намагаємося розібратися в чому ж тут справа.

3 Результати експериментальних досліджень

Як з’ясувалося, слабкість, про яку йде мова, полягає в тому, що при з'єднанні керованих S-блоків в ланцюжок при однакових байтових різницях на входах сусідніх S-блоків з'являється можливість при проході на S-блоці вхідної різниці в ту ж саму вихідну різницю отримати на вході чергового S-блоку нульову вхідну різницю і розірвати ланцюжок переходів з S-блоків. Такі переходи відповідають діагональним елементам таблиць диференціальних різниць S-блоків, і ймовірність таких переходів виходить досить високою.

Таблиця 1 відображає результати експериментальних досліджень по визначенню реального числа активованих S-блоків для різних варіантів 3-циклового перетворення при активізації входу S-перетворення різними варіантами двобайтових ненульових різниць.

У таблиці 2 наводиться детальне уявлення розподілу S-блоків (практичних значень), що активізуються в межах ланцюжка на кожному циклі, при активації входу "удосконаленого" S-перетворення різними варіантами двобаштових різниць (*де, О – значення, що очікується*).

Якщо для випадку $\Delta X1 = \Delta X2 \neq 0$ на вході першого S-блоку виходить нульова вхідна різниця, то на вході другого S-блоку виявляється ненульова вхідна різниця, яка активізує всі наступні S-блоки (*виходить 7 активізованих S-блоків*), тобто в разі, наприклад, різниць $\Delta X2 = \Delta X3 \neq 0$, як свідчать результати експерименту (див. Табл. 3), замість очікуваних

Таблиця 1 – Кількість активованих S-блоків для різних варіантів 3-циклового перетворення

Ненульові байтові різниці	**КІЛЬКІСТЬ АКТИВОВАНИХ S-БЛОКІВ**											
	Варіант зі схемою змішування								**Без схеми змішування**			
	Схема змішування використовується на КОЖНОМУ циклі				Схема змішування використовується ТІЛЬКИ на 1-му циклі				Схема змішування НЕ ВИКОРИСТОВУЄТЬСЯ			
	1-й цикл	2-й цикл	3-й цикл	Σ	1-й цикл	2-й цикл	3-й цикл	Σ	1-й цикл	2-й цикл	3-й цикл	Σ
$\Delta X_1 = \Delta X_2 \neq 0$	7	6	6	19	7	6	6	19	1	6	6	13
$\Delta X_1 = \Delta X_3 \neq 0$	6	6	6	18	6	6	6	18	2	1	6	9
$\Delta X_1 = \Delta X_4 \neq 0$	2	6	6	14	2	6	6	14	3	6	6	15
$\Delta X_1 = \Delta X_5 \neq 0$	4	6	6	16	4	6	6	16	4	6	6	16
$\Delta X_1 = \Delta X_6 \neq 0$	4	4	6	14	4	6	6	16	5	6	6	17
$\Delta X_1 = \Delta X_7 \neq 0$	4	6	6	16	4	6	6	16	6	6	6	18
$\Delta X_1 = \Delta X_8 \neq 0$	3	4	6	13	3	3	6	12	7	6	6	19
$\Delta X_2 = \Delta X_3 \neq 0$	1	6	6	13	1	5	6	12	1	5	6	12
$\Delta X_2 = \Delta X_4 \neq 0$	6	6	6	18	6	6	6	18	2	1	6	9
$\Delta X_2 = \Delta X_5 \neq 0$	3	6	6	15	3	6	6	15	3	6	6	15
$\Delta X_2 = \Delta X_6 \neq 0$	4	5	5	15	4	6	6	16	4	6	6	16
$\Delta X_2 = \Delta X_7 \neq 0$	4	5	6	15	4	3	6	13	5	6	6	17
$\Delta X_2 = \Delta X_8 \neq 0$	4	6	6	16	4	3	6	13	6	6	6	18
$\Delta X_3 = \Delta X_4 \neq 0$	2	5	6	13	2	6	6	14	1	6	6	13
$\Delta X_3 = \Delta X_5 \neq 0$	2	3	6	11	2	6	6	14	2	6	6	14
$\Delta X_3 = \Delta X_6 \neq 0$	4	4	6	14	4	3	6	13	3	2	6	11
$\Delta X_3 = \Delta X_7 \neq 0$	3	4	4	11	3	7	6	16	4	6	6	16
$\Delta X_3 = \Delta X_8 \neq 0$	4	6	6	16	4	5	6	15	5	4	6	15
$\Delta X_4 = \Delta X_5 \neq 0$	3	6	6	15	3	2	6	11	1	6	6	13
$\Delta X_4 = \Delta X_6 \neq 0$	2	6	6	14	2	1	6	9	2	1	6	9
$\Delta X_4 = \Delta X_7 \neq 0$	5	5	6	16	5	4	6	15	3	2	6	11
$\Delta X_4 = \Delta X_8 \neq 0$	2	4	4	10	2	7	7	14	4	3	6	13
$\Delta X_5 = \Delta X_6 \neq 0$	4	6	6	16	4	6	6	16	1	5	6	12
$\Delta X_5 = \Delta X_7 \neq 0$	4	5	6	15	4	6	6	16	2	5	6	13
$\Delta X_5 = \Delta X_8 \neq 0$	5	6	6	17	5	4	6	15	3	4	6	13
$\Delta X_6 = \Delta X_7 \neq 0$	2	4	6	12	2	6	6	14	1	4	6	11
$\Delta X_6 = \Delta X_8 \neq 0$	4	5	5	14	4	5	5	14	2	1	6	9
$\Delta X_7 = \Delta X_8 \neq 0$	5	6	6	17	5	5	6	16	1	3	6	10
Мін кількість	*1*	*3*	*4*	*10*	*1*	*1*	*5*	*9*	*1*	*1*	*6*	*9*
Середнє число	*3,68*	*5,25*	*5,82*	*14,8*	*3,68*	*5,04*	*5,93*	*14,7*	*3*	*4,46*	*6*	*13,5*

Таблиця 2 - Значення, що не відповідають очікуваним результатам активізації S-блоків

Ненульові байтові різниці	**ПОЗИЦІЇ АКТИВОВАНИХ S-БЛОКІВ**					
	Схема змішування використовується на кожному циклі			Схема змішування використовується на кожному циклі		
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
$\Delta X_1 = \Delta X_4 \neq 0$ O = 7	2	2	5	2	5	6
	0110 0000	1100 0000	0111 1011	0110 0000	0111 0110	1101 1110
$\Delta X_1 = \Delta X_8 \neq 0$ O = 7	3	4	6	3	2	6
	0110 0001	1110 0001	1011 1101	0110 0001	0100 0001	1011 0111

Продовження таблиці 2

$\Delta X2 = \Delta X3 \neq 0$ O = 7	1	1	6	1	5	6
	0100 0000	1000 0000	1011 1101	0100 0000	0110 1110	1111 0011
$\Delta X_2 = \Delta X_5 \neq 0$ O = 7	3	6	6	3	2	6
	0111 0000	0110 1111	1111 1010	0111 0000	0111 1101	1111 0110
$\Delta X_2 = \Delta X_7 \neq 0$ O = 7	3	5	6	3	4	5
	0100 0011	1111 1000	1111 1100	0100 0011	0111 1000	1111 1000
$\Delta X_3 = \Delta X_4 \neq 0$ O = 7	2	2	6	2	5	6
	0110 0000	1100 0000	1101 1101	0110 0000	0110 1011	1111 0110
$\Delta X_3 = \Delta X_5 \neq 0$ O = 6	2	3	6	2	4	6
	0011 0000	1110 0000	1010 1111	0011 0000	0010 1011	0110 1111
$\Delta X_3 = \Delta X_6 \neq 0$ O = 6	4	6	6	4	3	6
	0111 1000	1100 1111	0111 1110	0111 1000	0111 0000	0111 1011
$\Delta X_3 = \Delta X_8 \neq 0$ O = 6	3	6	6	3	5	6
	0110 0001	0011 1111	1111 1001	0110 0001	0111 0110	1101 1101
$\Delta X_4 = \Delta X_5 \neq 0$ O = 7	3	6	6	3	5	5
	0111 0000	0011 1111	1101 0111	01110000	01101011	11101001
$\Delta X_4 = \Delta X_6 \neq 0$ O = 6	2	6	6	2	1	5
	00011000	11010111	01101111	00011000	00010000	01101111
$\Delta X_4 = \Delta X_7 \neq 0$ O = 7	4	6	6	4	4	6
	0110 0011	1110 1110	0111 1101	0110 0011	0111 1000	0011 1111
$\Delta X_5 = \Delta X_6 \neq 0$ O = 5	4	6	6	4	3	6
	0111 1000	0011 1111	1111 0101	0111 1000	0111 0000	0011 1111
$\Delta X_5 = \Delta X_7 \neq 0$ O = 6	4	5	6	4	3	6
	0011 1100	1111 1000	0011 1111	0011 1100	0011 1000	1010 1111
$\Delta X_6 = \Delta X_7 \neq 0$ O = 7	2	3	6	2	5	6
	0100 0100	0000 0111	1011 1101	0100 0100	0110 1101	1110 1101
$\Delta X_6 = \Delta X_8 \neq 0$ O = 5	3	6	6	3	3	6
	00011001	11101011	10110111	00011001	00010110	11101011
$\Delta X_7 = \Delta X_8 \neq 0$ O = 7	4	5	6	3	5	6
	0110 0011	1110 0011	1010 1111	0110 0010	0101 1101	0111 1110

шести активованих S-блоків виходить лише один активний S-блок. Це робиться за рахунок того, що при проході другого S-блоку при S(X2) = X2 на вході третього S-блоку виходить нульова вхідна різниця X2 = ΔX3 ≠ 0, яка розриває ланцюжок ненульових переходів різниць для наступних S-блоків.

Отже, отримані результати свідчать, про те що "удосконалені" схеми з додатним змішуванням сегментів на вході першого циклу мають показники не кращі ніж схема без змішуючого перетворення. Загальний висновок тут міститься в тому, що додатне лінійне перетворення практично не покращує показників випадковості схеми з ланцюжка керованих підстановок. Результати виявляються близькими (не краще ніж) до схеми S перетворення з множенням на МДВ матрицю, тобто з випадком, коли на першому циклі активізується лише один S-блок. Тобто активізація S-блоків першого циклу виявляється фіктивною (*не ефективною*). Таким чином, це значить, що лінійні перетворення на вході першого циклу не можуть покращити показників випадковості схеми.

Причиною цього виявляється те, що лінійні перетворення на вході першого циклу не забезпечують випадкового зв'язку між байтами на входах S-блоків і тому для цих S-блоків не виконується умова, що ймовірності переходів S-блоків не перемножуються, а скоріше підсумовуються.

Таблиця 3 – Статистичні дані ймовірності активізації 1-8-ми S-блоків для різних варіантів схеми

	Очікувана кількість активованих S-блоків	ВАРІАНТ ЗІ СХЕМОЮ ЗМІШУВАННЯ						БЕЗ СХЕМИ ЗМІШУВАННЯ		
		Схема змішування використовується на кожному циклі			Схема змішування використовується на 1-му циклі			Схема змішування не використовується		
		1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
$\Delta X_1 = \Delta X_2 \neq 0$	7	7 - 255 - 99.6%	6 - 28 - 10.98% 7 - 227 - 88.67%	6 - 19 - 7.42 % 7 - 236 - 92.18%	7 - 255 - 99.61%	5 - 14 - 5.47% 6 - 241 - 94.14%	6 - 25 - 9.76% 7 - 230 - 89.84%	1 - 112 - 43.75% 8 - 143 - 55.86%	6 - 22 - 8.59% 7 - 233 - 91.02%	6 - 23 - 8.98% 7 - 232 - 90.62%
$\Delta X_1 = \Delta X_3 \neq 0$	6	6 - 255 - 99.61%	6 - 27 - 10.55% 7 - 227 - 88.67% 8 - 1 - 0.39 %	6 - 31 - 12.11% 7 - 223 - 87.11% 8 - 1 - 0.39%	6 - 255 - 99.6%	4 - 2 - 0.78% 5 - 252 - 98.44% 6 - 1 - 0.39%	5 - 1 - 0.39% 6 - 23 - 8.98% 7 - 231 - 90.23%	2 - 152 - 59.37% 8 - 103 - 40.23%	6 - 13 - 5.08% 7 - 242 - 94.53%	6 - 20 - 7.81% 7 - 235 - 91.8%
$\Delta X_1 = \Delta X_4 \neq 0$	7	2 - 144 - 56.25% 7 - 111 - 43.36%	2 - 1 - 0.39% 6 - 18 - 7.03% 7 - 236 - 92.19%	5 - 1 - 0.39% 6 - 32 - 12.5 % 7 - 222 - 86.72%	2 - 168 - 65.62% 7 - 87 - 33.98%	5 - 14 - 5.47% 6 - 238 - 92.97% 7 - 3 - 1.17%	6 - 29 - 11.33% 7 - 226 - 88.28%	3 - 157 - 61.33% 8 - 98 - 38.28%	6 - 12 - 4.69% 7 - 243 - 94.92%	6 - 21 - 8.20% 7 - 234 - 91.40%
$\Delta X_1 = \Delta X_5 \neq 0$	4	4 - 255 - 99.60%	6 - 23 - 8.98 % 7 - 232 - 90.63%	6 - 27 - 10.55% 7 - 228 - 89.06%	4 - 255 - 99.61%	3 - 240 - 93.75% 4 - 15 - 5.86%	6 - 26 - 10.15% 7 - 229 - 89.45%	4 - 162 - 63.28% 8 - 93 - 36.33%	3 - 1 - 0.39% 6 - 15 - 5.86% 7 - 239 - 93.36%	6 - 21 - 8.20% 7 - 234 - 91.40%
$\Delta X_1 = \Delta X_6 \neq 0$	7	4 - 169 - 66.02% 7 - 86 - 33.59%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	6 - 33 - 12.89 % 7 - 222 - 86.72%	4 - 150 - 58.59% 7 - 105 - 41.02%	3 - 1 - 0.39% 5 - 4 - 1.56% 6 - 250 - 97.66%	5 - 1 - 0.39% 6 - 25 - 9.77% 7 - 228 - 89.06% 8 - 1 - 0.39%	5 - 167 - 65.23% 8 - 88 - 34.38%	4 - 1 - 0.39% 6 - 13 - 5.078% 7 - 241 - 94.14%	6 - 15 - 5.86% 7 - 240 - 93.75%
$\Delta X_1 = \Delta X_7 \neq 0$	6	4 - 155 - 60.54% 6 - 100 - 39.06%	5 - 1 - 0.39 % 6 - 24 - 9.37 % 7 - 230 - 89.84%	5 - 1 - 0.39 % 6 - 15 - 5.86 % 7 - 239 - 93.36%	4 - 163 - 63.67% 5 - 0 - 0% 6 - 92 - 35.94%	4 - 8 - 3.12% 5 - 245 - 95.70% 6 - 2 - 0.78%	6 - 23 - 8.98% 7 - 232 - 90.62%	6 - 167 - 65.23% 8 - 88 - 34.37%	6 - 16 - 6.25% 7 - 239 - 93.36%	6 - 24 - 9.37% 7 - 231 - 90.23%
$\Delta X_1 = \Delta X_8 \neq 0$	7	3 - 147 - 57.42% 6 - 66 - 25.78% 7 - 42 - 16.40%	4 - 1 - 0.39% 6 - 22 - 8.59% 7 - 232 - 90.62%	6 - 29 - 11.32% 7 - 226 - 88.28%	3 - 154 - 60.16% 6 - 62 - 24.22% 7 - 39 - 15.23%	2 - 1 - 0.39% 5 - 6 - 2.34% 6 - 248 - 96.88%	6 - 18 - 7.03% 7 - 237 - 92.58%	7 - 166 - 64.84% 8 - 89 - 34.77%	6 - 21 - 8.20% 7 - 233 - 91.02% 8 - 1 - 0.39%	5 - 1 - 0.39% 6 - 21 - 8.20% 7 - 233 - 91.02%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_2 = \Delta X_3 \neq 0$	7	1 - 102 - 39.84% 7 - 153 - 59.77%	1 - 1 - 0.39% 6 - 30 - 11.72% 7 - 224 - 87.5%	6 - 20 - 7.81% 7 - 234 - 91.4% 8 - 1 - 0.39%	1 - 97 - 37.89% 7 - 158 - 61.72%	5 - 10 - 3.90% 6 - 245 - 95.70%	6 - 27 - 10.55% 7 - 228 - 89.06%	7 - 149 - 58.20%	5 - 15 - 5.86% 6 - 237 - 92.58% 7 - 3 - 1.172%	5 - 12 - 4.69% 6 - 243 - 94.92%
$\Delta X_2 = \Delta X_4 \neq 0$	5	5 - 255 - 99.60%	6 - 20 - 7.81% 7 - 235 - 91.8%	6 - 17 - 6.64% 7 - 238 - 92.97%	5 - 255 - 99.60%	3 - 4 - 1.56% 4 - 248 - 96.88% 5 - 3 - 1.17%	6 - 30 - 11.72% 7 - 225 - 87.89%	2 - 159 - 62.12% 7 - 96 - 37.5%	1 - 1 - 0.39% 5 - 12 - 4.69% 6 - 242 - 94.53%	5 - 13 - 5.07% 6 - 242 - 94.53%
$\Delta X_2 = \Delta X_5 \neq 0$	7	3 - 147 - 57.42% 7 - 108 - 42.19%	6 - 18 - 7.03% 7 - 237 - 92.58%	6 - 29 - 11.32% 7 - 226 - 88.28%	3 - 161 - 62.89% 7 - 94 - 36.72%	2 - 2 - 0.78% 5 - 13 - 5.08% 6 - 238 - 92.97% 7 - 2 - 0.78%	6 - 26 - 10.16% 7 - 229 - 89.45%	3 - 163 - 63.67% 7 - 92 - 35.93%	2 - 2 - 0.78% 5 - 10 - 3.90% 6 - 243 - 94.92%	5 - 13 - 5.08% 6 - 241 - 94.14% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_6 \neq 0$	3	3 - 255 - 99.61%	5 - 4 - 1.56% 6 - 164 - 64.06% 7 - 87 - 33.98%	5 - 1 - 0.39% 6 - 26 - 10.16% 7 - 228 - 89.06%	3 - 255 - 99.61%	2 - 220 - 85.94% 3 - 35 - 13.67%	5 - 3 - 1.17188% 6 - 172 - 67.1875% 7 - 80 - 31.25%	4 - 157 - 61.33% 7 - 98 - 38.28%	3 - 2 - 0.78% 5 - 11 - 4.3% 6 - 242 - 94.53%	5 - 20 - 7.81% 6 - 234 - 91.40% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_7 \neq 0$	7	3 - 100 - 39.06% 5 - 88 - 34.37% 7 - 67 - 26.17%	5 - 3 - 1.17% 6 - 26 - 10.15% 7 - 225 - 87.89% 8 - 1 - 0.39%	6 - 20 - 7.81% 7 - 235 - 91.8%	3 - 98 - 38.28% 5 - 101 - 39.45% 7 - 56 - 21.86%	4 - 1 - 0.39% 5 - 5 - 1.95% 6 - 249 - 97.27%	5 - 1 - 0.39% 6 - 25 - 9.77% 7 - 228 - 89.06% 8 - 1 - 0.39%	5 - 165 - 64.45% 7 - 90 - 35.16%	4 - 1 - 0.39% 5 - 12 - 4.68% 6 - 242 - 94.53%	5 - 9 - 3.51% 6 - 245 - 95.70% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_8 \neq 0$	7	4 - 175 - 68.35% 5 - 80 - 31.25%	6 - 13 - 5.08% 7 - 242 - 94.53%	6 - 24 - 9.37% 7 - 231 - 90.23%	4 - 162 - 63.28% 5 - 93 - 36.33%	3 - 4 - 1.56% 4 - 247 - 96.48% 5 - 4 - 1.56%	6 - 21 - 8.20% 7 - 233 - 91.01% 8 - 1 - 0.39%	6 - 150 - 58.59% 7 - 105 - 41.02%	5 - 12 - 4.68% 6 - 242 - 94.53% 7 - 1 - 0.39%	5 - 9 - 3.51% 6 - 245 - 95.70% 7 - 1 - 0.39%
$\Delta X_3 = \Delta X_4 \neq 0$	7	2 - 145 - 56.64% 6 - 40 - 15.62% 7 - 70 - 27.34%	2 - 1 - 0.39% 6 - 25 - 9.76% 7 - 229 - 89.45%	6 - 19 - 7.42% 7 - 236 - 92.18%	2 - 164 - 64.06% 6 - 36 - 14.06% 7 - 55 - 21.48%	5 - 6 - 2.34% 6 - 249 - 97.26%	6 - 25 - 9.76% 7 - 228 - 89.06% 8 - 2 - 0.78%	6 - 163 - 63.67%	4 - 3 - 1.17% 5 - 250 - 97.65% 6 - 2 - 0.78%	4 - 5 - 1.95% 5 - 248 - 96.87% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_5 \neq 0$	6	2 - 167 - 65.23% 6 - 88 - 34.37%	3 - 1 - 0.39% 6 - 23 - 8.98% 7 - 231 - 90.23%	6 - 28 - 10.93% 7 - 227 - 88.67%	2 - 151 - 58.98% 6 - 104 - 40.62%	4 - 7 - 2.73% 5 - 246 - 96.09% 6 - 2 - 0.78%	6 - 32 - 12.5% 7 - 223 - 87.1094%	2 - 157 - 61.32% 6 - 98 - 38.28%	1 - 2 - 0.78% 4 - 6 - 2.34% 5 - 244 - 95.31% 6 - 3 - 1.17%	4 - 9 - 3.51% 5 - 245 - 95.70% 6 - 1 - 0.39%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_3 = \Delta X_6 \neq 0$	6	4 - 197 - 76.95% 7 - 58 - 22.66%	6 - 31 - 12.10% 7 - 224 - 87.5%	6 - 32 - 12.5% 7 - 222 - 86.72%	4 - 199 - 77.73% 7 - 56 - 21.87%	3 - 1 - 0.39% 5 - 8 - 3.12% 6 - 245 - 95.70% 7 - 1 - 0.39%	6 - 22 - 8.59% 7 - 233 - 91.01%	3 - 159 - 62.1094% 6 - 96 - 37.5%	4 - 5 - 1.95% 5 - 249 - 97.27% 6 - 1 - 0.39%	4 - 17 - 6.64% 5 - 236 - 92.19% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_7 \neq 0$	2	2 - 255 - 99.61%	4 - 1 - 0.39% 5 - 167 - 65.23% 7 - 85 - 33.20% 8 - 2 - 0.78%	5 - 2 - 0.78% 6 - 21 - 8.20% 7 - 231 - 90.23% 8 - 1 - 0.39%	2 - 255 - 99.6%	1 - 160 - 62.5% 2 - 95 - 37.10%	4 - 4 - 1.56% 5 - 166 - 64.84% 6 - 3 - 1.17% 7 - 81 - 31.64% 8 - 1 - 0.39%	4 - 163 - 63.67% 6 - 92 - 35.93%	3 - 2 - 0.78% 4 - 4 - 1.56% 5 - 247 - 96.48% 6 - 2 - 0.78%	4 - 6 - 2.34% 5 - 247 - 96.48% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_8 \neq 0$	7	3 - 169 - 66.01% 6 - 64 - 25% 7 - 22 - 8.59%	6 - 25 - 9.78% 7 - 230 - 89.84%	6 - 23 - 8.98% 7 - 232 - 90.62%	3 - 161 - 62.89% 6 - 74 - 28.90% 7 - 20 - 7.81%	5 - 11 - 4.3% 6 - 243 - 94.92% 7 - 1 - 0.39%	6 - 27 - 10.54% 7 - 228 - 89.06%	5 - 169 - 66.01% 6 - 86 - 33.59%	4 - 7 - 2.73438% 5 - 248 - 96.87%	4 - 12 - 4.68% 5 - 242 - 94.53% 6 - 1 - 0.39 %
$\Delta X_4 = \Delta X_5 \neq 0$	7	3 - 163 - 63.68% 6 - 61 - 23.83% 7 - 31 - 12.11%	6 - 19 - 7.42% 7 - 236 - 92.19%	6 - 22 - 8.59% 7 - 233 - 91.02%	3 - 169 - 66.02% 6 - 54 - 21.09% 7 - 32 - 12.5%	5 - 11 - 4.29% 6 - 243 - 94.92% 7 - 1 - 0.39%	5 - 1 - 0.39% 6 - 31 - 12.11% 7 - 223 - 87.11%	1 - 97 - 37.89% 5 - 158 - 61.71%	3 - 3 - 1.17% 4 - 246 - 96.09% 5 - 6 - 2.34%	3 - 8 - 3.12% 4 - 241 - 94.14% 5 - 6 - 2.34%
$\Delta X_4 = \Delta X_6 \neq 0$	5	2 - 160 - 62.5% 5 - 95 - 37.11%	6 - 26 - 10.15% 7 - 229 - 89.45%	6 - 19 - 7.42% 7 - 236 - 92.18%	2 - 145 - 56.64% 5 - 110 - 42.97%	1 - 1 - 0.39% 3 - 3 - 1.17% 4 - 246 - 96.09% 5 - 5 - 1.95%	5 - 1 - 0.39% 6 - 25 - 9.76% 7 - 229 - 89.45%	2 - 153 - 59.76% 5 - 102 - 39.84%	3 - 1 - 0.39% 4 - 249 - 97.27% 5 - 5 - 1.95%	3 - 11 - 4.297% 4 - 239 - 93.35% 5 - 5 - 1.95%
$\Delta X_4 = \Delta X_7 \neq 0$	7	4 - 154 - 60.15% 5 - 66 - 25.78% 6 - 16 - 6.25% 7 - 19 - 7.42%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	5 - 1 - 0.39% 6 - 22 - 8.59% 7 - 232 - 90.62%	4 - 149 - 58.20% 5 - 70 - 27.34% 6 - 14 - 5.47% 7 - 22 - 8.59%	4 - 2 - 0.78% 5 - 11 - 4.29% 6 - 242 - 94.53%	6 - 26 - 10.15% 7 - 229 - 89.45%	3 - 164 - 64.06% 5 - 91 - 35.54%	2 - 1 - 0.39% 3 - 4 - 1.56% 4 - 247 - 96.48% 5 - 3 - 1.17%	3 - 9 - 3.52% 4 - 244 - 95.31% 5 - 2 - 0.78%
$\Delta X_4 = \Delta X_8 \neq 0$	1	1 - 255 - 99.6%	4 - 146 - 57.03% 6 - 69 - 26.95% 7 - 26 - 10.15% 8 - 14 - 5.47%	4 - 2 - 0.78% 6 - 18 - 7.03% 7 - 235 - 91.8%	1 - 255 - 99.60%	1 - 255 - 99.60%	4 - 150 - 58.59% 5 - 1 - 0.39% 6 - 65 - 25.39% 7 - 29 - 11.32% 8 - 10 - 3.90%	4 - 156 - 60.93% 5 - 99 - 38.67%	3 - 3 - 1.17% 4 - 249 - 97.26% 5 - 3 - 1.17%	3 - 2 - 0.78% 4 - 245 - 95.70% 5 - 8 - 3.12%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_5 = \Delta X_6 \neq 0$	7	4 - 170 - 66.40% 6 - 48 - 18.75% 7 - 37 - 14.45%	6 - 17 - 6.64% 7 - 238 - 92.99%	6 - 27 - 10.55% 7 - 228 - 89.06%	4 - 158 - 61.71% 5 - 0 - 0% 6 - 63 - 24.61% 7 - 34 - 13.28%	3 - 1 - 0.39% 5 - 11 - 4.29% 6 - 243 - 94.9%	6 - 29 - 11.32% 7 - 226 - 88.28%	1 - 102 - 39.84% 4 - 153 - 59.76%	3 - 247 - 96.48% 4 - 8 - 3.13%	2 - 5 - 1.95% 3 - 235 - 91.8% 4 - 15 - 5.86%
$\Delta X_5 = \Delta X_7 \neq 0$	6	4 - 219 - 85.54% 6 - 36 - 14.06%	5 - 2 - 0.78% 6 - 22 - 8.59% 7 - 231 - 90.23%	6 - 25 - 9.76% 7 - 229 - 89.45% 8 - 1 - 0.39%	4 - 228 - 89.06% 6 - 27 - 10.54%	3 - 1 - 0.39% 4 - 4 - 1.56% 5 - 246 - 96.09% 6 - 4 - 1.56%	6 - 21 - 8.20% 7 - 234 - 91.40%	2 - 148 - 57.81% 4 - 107 - 41.8%	1 - 2 - 0.78% 2 - 1 - 0.39% 3 - 237 - 92.58% 4 - 15 - 5.9%	2 - 4 - 1.56% 3 - 242 - 94.53% 4 - 9 - 3.52%
$\Delta X_5 = \Delta X_8 \neq 0$	4	4 - 157 - 61.33% 6 - 86 - 33.59% 7 - 12 - 4.68%	3 - 1 - 0.39% 4 - 1 - 0.39% 6 - 28 - 10.94% 7 - 225 - 87.89%	5 - 1 - 0.39% 6 - 27 - 10.55% 7 - 227 - 88.67%	4 - 167 - 65.23% 5 - 1 - 0.39% 6 - 72 - 28.12% 7 - 15 - 5.86%	3 - 1 - 0.39% 5 - 12 - 4.69% 6 - 242 - 94.53%	6 - 24 - 9.37% 7 - 231 - 90.23%	3 - 158 - 61.72% 4 - 97 - 37.89%	2 - 1 - 0.39% 3 - 248 - 96.87% 4 - 6 - 2.34%	2 - 1 - 0.39% 3 - 241 - 94.14% 4 - 13 - 5.078%
$\Delta X_6 = \Delta X_7 \neq 0$	7	2 - 1 - 0.39% 4 - 102 - 39.84% 5 - 99 - 38.67% 6 - 32 - 12.5% 7 - 21 - 8.20%	3 - 1 - 0.39% 5 - 3 - 1.17% 6 - 28 - 10.94% 7 - 223 - 87.11%	6 - 33 - 12.89% 7 - 222 - 86.72%	2 - 4 - 1.56% 4 - 103 - 40.23% 5 - 94 - 36.71% 6 - 41 - 16.02% 7 - 13 - 5.08%	5 - 6 - 2.34% 6 - 247 - 96.48% 7 - 2 - 0.78%	6 - 23 - 8.98% 7 - 232 - 90.62%	1 - 101 - 39.45% 3 - 154 - 60.15%	2 - 222 - 86.71% 3 - 33 - 12.89%	1 - 2 - 0.78% 2 - 215 - 83.98% 3 - 38 - 14.84%
$\Delta X_6 = \Delta X_8 \neq 0$	5	3 - 161 - 62.89% 4 - 64 - 25% 5 - 30 - 11.71%	6 - 32 - 12.5% 7 - 223 - 87.10%	6 - 22 - 8.59% 7 - 233 - 91.02%	3 - 166 - 64.84% 4 - 55 - 21.48% 5 - 34 - 13.28%	3 - 5 - 1.95% 4 - 246 - 96.0% 5 - 4 - 1.56%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	2 - 162 - 63.28% 3 - 93 - 36.32%	2 - 222 - 86.72% 3 - 33 - 12.89%	1 - 1 - 0.39% 2 - 227 - 88.67% 3 - 27 - 10.54%
$\Delta X_7 = \Delta X_8 \neq 0$	7	4 - 154 - 60.15+5 6 - 87 - 33.98% 7 - 14 - 5.46%	5 - 1 - 0.39% 6 - 18 - 7.03% 7 - 236 - 92.19%	6 - 27 - 10.54% 7 - 228 - 89.06%	3 - 1 - 0.39% 4 - 165 - 64.45% 5 - 2 - 0.78% 6 - 78 - 30.47% 7 - 9 - 3.52%	5 - 11 - 4.3% 6 - 244 - 95.31%	6 - 22 - 8.6% 7 - 233 - 91.02%	1 - 95 - 37.11% 2 - 160 - 62.5%	1 - 147 - 57.42% 2 - 108 - 42.19%	1 - 163 - 63.67% 2 - 92 - 35.93%

4 Висновки

Пропозиція стосовно можливостей удосконалення шифру Струмок, що була висунута раніше автором роботі [1], виявляється помилковою. Так, раніше запропоноване рішення практично поступається за своїми показниками випадковості відповідному рішенню представленому у специфікації до шифру Струмок [3].

Наступний висновок, який має принципове значення, міститься в тому, що залишається справедливим раніше висловлене в роботі [2] загальне положення, згідно до якого мінімальне число активованих S-блоків перших циклів SPN шифрів дорівнює одному! Виключенням є лише шифр Лабіринт [4], в котрому використовується нелінійне доциклове перетворення (*перетворення з шару S-блоків на вході першого циклу*). Фактично це додаткове циклове перетворення.

Посилання

[1] Lisitzky, K. Stratehiia vyboru S-blokiv dlia neliniinoho peretvorennia shyfru Strumok. Kompiuterni nauky ta kiberbezpeka. 2018. № 2. P.4–11. URL: https://periodicals.karazin.ua/cscs/article/view/12025
[2] Dolgov V. I., Lisitska I. V., Lisitskyi K. Ye. The new concept of block symmetric ciphers design. TelecomRadEng. Vol. 76. Issue 2. P. 157–184.
[3] Matematychna struktura potokovoho shyfru Strumok / Gorbenko I.D., Kuznetsov O.O., Oleksyichuk A.M., V.A. Tymchenko. Radyotekhnyka. Kharkiv: KhTURE, 2018. Vyp. 193. P. 17–27.
[4] Golovashych S. A. Spetsyfykatsyia alhorytma blochnoho symmetrychnoho shyfrovanyia «Labyrynt». Prykladnaia radyoэlektronyka. Kharkiv: KhTURE, 2007. Vol. 6, №2. P. 230–240.

Reviewer: Roman Oliynikov, Doctor of Sciences (Eng.), Full Professor, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: roliynykov@gmail.com

Received: October 2018.

Authors:
Konstantin Lisitzky, postgraduate student of the Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: lisickiy@ukr.net

Katerina Kuznetsova, computer science student**,** V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: kate.kuznetsova.2000@gmail.com

On the weakness S of the transformation of the cipher Strumok from the chain of controllable S-blocks.

Abstract. The peculiarities of the construction of the S-transform of the Stream cipher “Strumok” are discussed. In particular, an analysis of the preposition for constructing S-transformation of the stream cipher “Strumok” using controlled S-blocks is underway. His randomness scores are evaluated. It is shown that it is inferior to the effectiveness of the original proposal. The reasons of such circumstances turn out.

Keywords: current cipher; random substitution; differential probability; S-transformation; linear mixing scheme.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина. Украина. E-mail: roliynykov@gmail.com

Поступила: Октябрь 2018.

Авторы:
Константин Лисицкий, аспирант кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 4, Харьков, 61022, Украина.
E-mail: lisickiy@ukr.net

Екатерина Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 4, Харьков, 61022, Украина. E-mail: kate.kuznetsova.2000@gmail.com

О слабости S-преобразования шифра Струмок из цепочки управляемых S-блоков.

Аннотация. Обсуждаются особенности построения S-преобразования шифра “Струмок”. Выполнен анализ предложения по построению S-преобразования поточного шифра “Струмок” с использованием управляемых S-блоков. Оцениваются показатели его случайности. Показывается, что оно по своей эффективности уступает соответствующему оригинальному решению. Выясняются причины таких обстоятельств.

Ключевые слова: поточный шифр; случайная подстановка; дифференциальная вероятность; S-преобразование; линейная смешивающая схема.