УДК 681.3.06

СТРАТЕГІЯ ВИБОРУ S-БЛОКІВ ДЛЯ НЕЛІНІЙНОГО ПЕРЕТВОРЕННЯ ШИФРУ СТРУМОК

Костянтин Лисицький

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна
lisickiy@ukr.net

Рецензент: Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна
kuznetsov@karazin.ua

Надійшло в квітні 2018

Анотація: *Обговорюються особливості побудування S-перетворення шифру Струмок. Зокрема увага зосереджується на виборі S-блоків для цього перетворення. Оцінюються показники його випадковості, зокрема визначається мінімальне число циклів повторного використання цього перетворення, після котрого результат зашифрування приходить до показників стаціонарного стану випадкової підстановки. Розглядається можливість використання в S перетворенні випадкових S-блоків. Робиться висновок, що випадкові S-блоки не погіршують показників його випадковості. Пропонується удосконалення цієї конструкції S-перетворення, яке дозволяє покращити показники його випадковості. Воно будується на використанні замість паралельного набору S-блоків ланцюжка з керованих підстановок з додатним змішуючим лінійним перетворенням сегментів блоків даних на вході шару керованих підстановок. Показується, що ця конструкція дозволяє вже при однократному проході активізувати мінімум чотири S-блоки, замість одного S-блоку в вихідній конструкції. Запропонована удосконалена конструкція S-перетворення представляється більш швидкодіючою і дозволяє за три цикли активізувати мінімум 20-ть S-блоків замість 16-ти в вихідній конструкції, що додатково покращує показники випадковості удосконалення.*

Ключові слова: *потоковий шифр; показники випадковості; випадкові S-блоки; активні S-блоки; керовані підстановки.*

1 Вступ

В даній роботі розглянемо модифікований потоковий SNOW-подібний шифр Струмок, який був розроблений з метою підвищення швидкодії вихідної конструкції [1]. Ця мета досягається тим, що в шифрі використовується лінійний рекурентний регістр над полем GF(264). Уся інша частина шифру повторює оригінальну конструкцію, за виключенням того, що S-перетворення тепер береться не 32-ох бітним а 64-ох бітним. У представленій роботі зосереджується увага саме на конструкції S-перетворення. Відповідно до пропозиції розробників, воно повторює 64-х бітну «цеглинку» шифру Калина.

Відомо, що розробники шифру Калина при виборі S-блоків однією з основних вимог взяли, вимогу, щоб показники нелінійності булевих функцій, які входять в S-блоки, були не менше ніж 104 [2]. В своїх дослідженнях [3] вони довели, що ймовірність знайти підстановку з таким показником нелінійності дорівнює 0,0000007. В цій же роботі підкреслено, що для породження оптимального S-блоку необхідно в середньому перебрати 1.100.000 підстановок.

Аналогічним шляхом пішли і при виборі S-блоків в шифрах “Кузнечик” та білоруському шифрі. Але, якщо це було важливо для великих шифрів (*для забезпечення мінімізації числа циклів їх приходу до стану випадкової підстановки* [4]), то в даному випадку для 64-х бітного блоку даних, відкривається можливість без втрати стійкості використати S-блоки без такого жорстокого їх відбору, про котрий було зазначене вище.

В першій частині статті буде показано, що показники випадковості цього перетворення зберігаються і при використанні в ньому випадкових S-блоків, а в другій частині пропонується удосконалена конструкція S-перетворення для шифру Струмок.

2 Опис S перетворення шифру Струмок

Нелінійне перетворення шифру Струмок будується на основі 64-х бітної конструкції шифру Калина, наведеної на рис. 1 [2].

Вхідне 64-бітове значення ділиться на 8-м байтів, кожен з яких замінюється відповідно до заданої таблиці підстановки. У перетворенні використовується 8-м різних таблиць, по одній на кожен байт.

Таблиці підстановок перетворення повторюють таблиці підстановок шифру Калина.

Операція лінійного розсіювання (перемішування в колонці) використовує поліноміальний уявлення байтів в поле GF (28), утвореному неприводимим поліномом

$$m(x)=x^8+x^4+x^3+x^2+1,$$

або $\{01\}\{1d\}$ в шістнадцятковому представленні.

Слід зазначити, що цей незвідний поліном в шифрі Калина не збігається з утворюючим поліномом шифру Rijndael/AES.

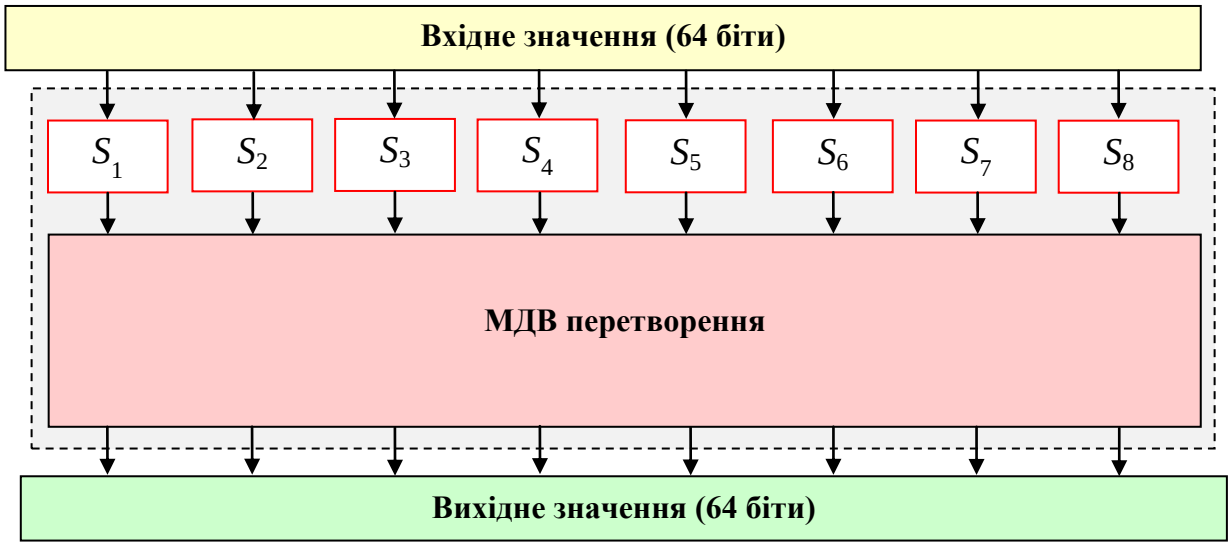

Рис. 1 – S перетворення шифру Струмок

Перемішування в колонках (MixColumns)

В ході перетворення MixColumns виконується послідовна обробка всіх колонок поточного стану. Кожна 8-байтна колонка розглядається як поліном над полем GF(28) с 8-ма термами, а в ході перетворення виконується множення цього поліному за модулем x^8+1 на фіксований поліном $c(x)$, де $c(x)=\{01\}x^7+\{05\}x^6+\{01\}x^5+\{08\}x^4+\{06\}x^3+\{07\}x^2+\{04\}x+\{01\}$.

Ця операція еквівалентна матричному множенню над GF(28) вихідного 8-байтного вектору на фіксовану матрицю, результат заноситься в 8-байтний вектор b (див. рис. 2).

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix}$$

Рис. 2 – Матричне множення над GF(28) вихідного 8-байтного вектору

Порядок обчислення елементів підсумкового вектору b пояснює рис. 3, де всі операції множення виконуються над полем GF(2^8).

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01\cdot a_0 \oplus 01\cdot a_1 \oplus 05\cdot a_2 \oplus 01\cdot a_3 \oplus 08\cdot a_4 \oplus 06\cdot a_5 \oplus 07\cdot a_6 \oplus 04\cdot a_7 \\ 04\cdot a_0 \oplus 01\cdot a_1 \oplus 01\cdot a_2 \oplus 05\cdot a_3 \oplus 01\cdot a_4 \oplus 08\cdot a_5 \oplus 06\cdot a_6 \oplus 07\cdot a_7 \\ 07\cdot a_0 \oplus 04\cdot a_1 \oplus 01\cdot a_2 \oplus 01\cdot a_3 \oplus 05\cdot a_4 \oplus 01\cdot a_5 \oplus 08\cdot a_6 \oplus 06\cdot a_7 \\ 06\cdot a_0 \oplus 07\cdot a_1 \oplus 04\cdot a_2 \oplus 01\cdot a_3 \oplus 01\cdot a_4 \oplus 05\cdot a_5 \oplus 01\cdot a_6 \oplus 08\cdot a_7 \\ 08\cdot a_0 \oplus 06\cdot a_1 \oplus 07\cdot a_2 \oplus 04\cdot a_3 \oplus 01\cdot a_4 \oplus 01\cdot a_5 \oplus 05\cdot a_6 \oplus 01\cdot a_7 \\ 01\cdot a_0 \oplus 08\cdot a_1 \oplus 06\cdot a_2 \oplus 07\cdot a_3 \oplus 04\cdot a_4 \oplus 01\cdot a_5 \oplus 01\cdot a_6 \oplus 05\cdot a_7 \\ 05\cdot a_0 \oplus 01\cdot a_1 \oplus 08\cdot a_2 \oplus 06\cdot a_3 \oplus 07\cdot a_4 \oplus 04\cdot a_5 \oplus 01\cdot a_6 \oplus 01\cdot a_7 \\ 01\cdot a_0 \oplus 05\cdot a_1 \oplus 01\cdot a_2 \oplus 08\cdot a_3 \oplus 06\cdot a_4 \oplus 07\cdot a_5 \oplus 04\cdot a_6 \oplus 01\cdot a_7 \end{bmatrix}.$$

Рис. 3 – Порядок обчислення елементів підсумкового вектору b

3 Показники випадковості S перетворення

Наведемо результати оцінки очікуваних параметрів переходу модифікованого S перетворення шифру SNOW до стану випадкової підстановки. Будемо оцінювати показники його випадковості як циклової функції ітеративного шифру.

Відповідно до [5] необхідно виконати оцінку мінімального числа активних (*задіяних S-блоків*), після проходження яких S перетворення стає випадковою підстановкою. Це мінімальне число визначається диференціальними і лінійними показниками самих S-блоків, що застосовуються в S перетворенні, конструкціями і властивостями подальшого лінійного перетворення, а також значеннями показників доказової стійкості перетворення в цілому, які залежать від розміру його бітового входу. В роботі [5] цей зв'язок між зазначеними показниками визначений у вигляді двох співвідношень:

$$IPS_D=(DP^{\pi}_{\max})^k,\ IPS_L = 2^{k-1}\cdot\left(LP^{\pi}_{\max}\right)^k, \quad (1)$$

де: – $DP^{\pi}_{\max}$ і $LP^{\pi}_{\max}$ – максимальні значення диференціальної і лінійної ймовірностей підстановлювальних перетворень $\pi(x)$; – *IPSD* (*Differential Indicator of Provable Security*) – диференційний показник доказовою безпеки; – *IPSL* (*Linear Indicator of Provable Security*) – лінійний показник доказовою безпеки; – $k = k_{\min}$ – мінімальне число активних S-блоків, що беруть участь у формуванні переходу шифру до випадкової підстановці.

Користуючись розрахунковими співвідношеннями, встановленими в роботі [6], можна прийти до висновку, що очікуване значення максимуму диференціального переходу для шифру з 64-*х* бітовим входом (*S перетворення*) виявляється близьким до 68, а очікуване значення максимуму зміщення лінійного корпусу для шифру з 64-*х* бітовим входом виявляється близьким до 2^{65}. Відповідно отримаємо, що максимальні значення лінійної і диференціальної ймовірності для багатоциклового перетворення з 64-*х* бітовим входом виходять близькими один до одного і рівними приблизно 2^{-58}.

Виходячи з наведених вище співвідношень можна зробити висновок, що для перетворення з 64-*х* бітовим входом потрібно для приходу до стану випадкової підстановки за диференціальними показниками при використанні S-блоків з граничними показниками δ-рівномірності рівними $DP^{\pi}_{\max}= 2^{-6}$, (у відповідності з рівністю $2^{-58} = (2^{-6})^k$) $k_{\min}$=10 S-блоків.

Аналогічно, для приходу до стану випадкової підстановки за лінійними показниками при використанні S-блоків з граничними показниками нелінійності рівними $LP^{\pi}_{\max}=2^{-4,8}$ буде потрібно $(2^{-58} = 2^{k-1}\cdot\left(2^{-4,8}\right)^k)$ $k_{\min}$=15 S-блоків.

У нашому випадку число активних S-блоків одноциклового перетворення дорівнює одному (на вході першого циклу перетворення активізується мінімум один S-блок і далі через те, що S перетворення містить 8-м S-блоків для двоциклового перетворення число S-блоків, що активізуються буде вже рівним 9-ти). Це означає, що для S-блоків з граничними диференціальними і лінійними показниками (для S-блоків з $DP^{\pi}_{\max}=LP^{\pi}_{\max}=2^{-6}$) S перетворення буде приходити до випадкової підстановці з запасом за три цикли.

4 Перспективи використання випадкових S-блоків

Методика виконання розрахунків представлена в роботі [7]. Нижче, у табл. 1 представлені результати розрахунків числа переходів різного типу в 17-ти рядках диференціальної таблиці випадкової байтової підстановки.

Таблиця 1 – Розрахунок числа переходів різного типу

Значення переходу таблиці	Число переходів диференціальної Таблиці	Число переходів в рядку	Число переходів в 17-ти рядках
12	1	0,003906	0,0664
10	10	0,039065	0,664
8	104	0,40625	6,906
6	830	3,24218	55,117

З представлених результатів випливає, що для 17-ти активних S-блоків при виборі в рядках максимально можливих переходів можна очікувати при випадкових входах в S-блоки:

- один перехід зі значенням 10;
- сім переходів зі значенням 8;
- дев'ять переходів зі значенням 6.

Всього 17-ть переходів (17-ть активних S-блоків). У припущенні, що вхід в перший S-блок (вхід в перший цикл) може бути обраний максимально можливим, обчислення в цьому випадку призводять до результату:

$$\left(\frac{12}{256}\right)\times\left(\frac{10}{256}\right)\times\left(\frac{8}{256}\right)^{7}\times\left(\frac{6}{256}\right)^{8}=2^{-87,4}.$$

Це означає, що випадкові S-блоки для цього шифру з великим запасом забезпечують за три цикли його прихід до стану випадкової підстановки.

Зауважимо, що для двох циклів маємо 9-ть активних S-блоків, і розрахунки для цього випадку представлені в табл. 2.

Таблиця 2 – Число переходів різного типу

Значення переходу таблиці	Число переходів диференціальної Таблиці	Число переходів в рядку	Число переходів в 9-ти рядках
12	1	0,003906	0,035154
10	10	0,039065	0,35158
8	104	0,40625	3,656
6	830	3,24218	29,17

З аналізу даних табл. 2 випливає, що для 9-ти активних S-блоків при виборі в рядках максимально можливих переходів можна очікувати при випадкових входах в S-блоки:

- нуль переходів зі значенням 10;
- чотири переходи зі значенням 8;

- п'ять переходів зі значенням 9.

У припущенні, що вхід в перший S-блок (вхід в перший цикл) може бути обраний максимально можливим, обчислення в цьому випадку призводять до результату:

$$\left(\frac{12}{256}\right)\times\left(\frac{8}{256}\right)^4\times\left(\frac{6}{256}\right)^4=2^{-46},$$

тобто двох циклів в цьому разі не вистачає для приходу до випадкової підстановки.

Будемо вважати, що процедура проходження S-блоків є випадковою і статистично незалежною. Методика розрахунків для цього випадку представлена в роботі [7].

У таблиці 3 представлені результати оцінки числа переходів і їх значень в 17 випадково взятих рядках таблиці ЛАТ. З результатів випливає, що для 17 активних S-блоків при використанні максимально можливих переходів можна очікувати при випадкових входах в випадкові S-блоки:

Таблиця 3 – Число переходів різного типу в 17-ти рядках лінійної таблиці

Значення переходу	Число переходів в таблиці ЛАТ	Число переходів в рядку таблиці ЛАТ	Число переходів в 17 випадково взятих рядках таблиці ЛАТ
±34	1,998	0,0078	0,1326
±32	4	0,0156	0,2652
±30	10	0,0392	0,6664
±28	28	0,1098	1,8666
±26	65	0,2588	4,3996
±24	146	0,572	9,724
±22	298	1,164	19,788

- один перехід зі значенням 30;
- два переходи зі значенням 28;
- чотири переходи зі значенням 26;
- дев'ять переходів зі значенням 24.

Найперший (один) S-блок береться з максимально можливим значенням переходу 34.

Вважаючи далі, що рядки в S-блок вибираються зі всієї безлічі 256-ти рядків, при цьому переходи по S-блокам йдуть в довільному порядку і здійснюються за найбільш ймовірного шляху, можемо виконати оцінку ймовірності приходу шифру до стану випадкової підстановки з випадковими S-блоками. Обчислення для значення $k = 17$ призводять до результату

$$2^{16}\times\left(\frac{34}{128}\right)^2\times\left(\frac{30}{128}\right)^2\left(\left(\frac{28}{128}\right)^2\right)^2\times\left(\left(\frac{26}{128}\right)^2\right)^4\times\left(\left(\frac{24}{128}\right)^2\right)^9=2^{16-74}=2^{-58}.$$

Таким чином, і в цьому випадку мінімальне число S-блоків, що активізуються задовольняє граничному значенню $k_{min}=17$. При цьому слід нагадати, що шифр Калина приходить до стану випадкової підстановки, як за диференціальним, так і за лінійними показниками на третьому-четвертому циклі.

5 Альтернативна конструкція S перетворення

Сама конструкція, що пропонується представлена на рис. 4. У своєї основі вона повторює конструкцію першого циклу шифру ШУП [7], тільки в цьому випадку замість SL перетворень тут виступають байтові S-блоки (*керовані підстановки*), а замість підсумування за модулем 2 сегментів на вході першого SL перетворення, використовується інша, більш ефективна схема змішування, яка заснована на багатошаровому підсумуванні за модулем 2 сегмен-

тів 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 і формується новий 64-*х* бітний блок даних. Він складається з нового лівого 32-*х* бітного підблоку (*який одержується за допомогою підсумування за модулем 2, лівого і правого 32-х бітних підблоків вихідного блоку даних*) та 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 він зводиться до байтового розміру.

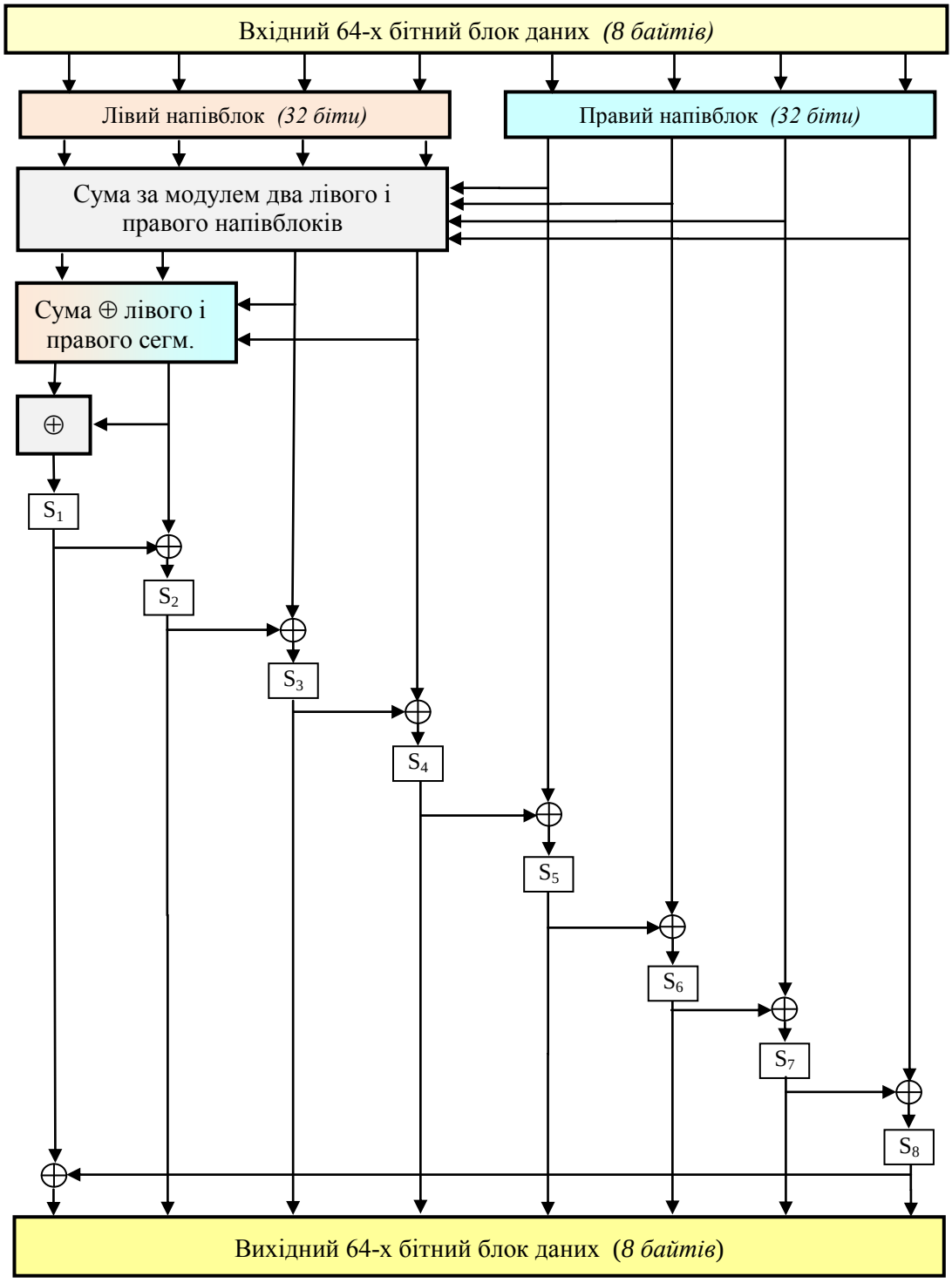

Рис. 4 – Альтернативна схема S перетворення на керованих підстановках

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

$$X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8$$

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

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

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

В гіршому випадку буде мати ненульову різницю байт X_5 ($X_1 \oplus X_5 = 0$, $X_1 = X_5 \neq 0$, $X_3 = X_7 = X_2 = X_6 = X_4 = X_8 = 0$, котрий буде активізувати на першому циклі 4-ри S-блоки.

Зауважимо, що для 256-бітного шифру с 4-и байтовими SL перетвореннями маємо активізацію на першому циклі в гіршому випадку 13-ти S-блоків.

Природно, що при трьох циклах у S перетворення буде активізуватися 20 S-блоків, і воно з великим запасом буде становитися випадковою підстановкою і при випадково згенерованих S-блоках.

Ця додатна операція потребує для свого виконання три XOR-и (*для 32-ох бітної платформи*). Всього в конструкції, що наведена на рис. 4 виконується 11-ть XOR-ів. Для виконання 64-*х* бітного перетворення шифру Калина потрібно буде використати (*при програмному виконанні*) 56 XOR-ів, не кажучи вже про операції множення байтів.

7 Висновки

Показано, що перетворення, яке складається з 8-ми паралельних S-блоків з наступним множенням виходів S-блоків на МДВ матрицю розміру 8×8 забезпечує граничні показники випадковості і при використанні випадкових S-блоків. Тобто в якості S-блоків в такому перетворенні можна використовувати практично підстановки з виходу генератора випадкових підстановок.

В статті запропонована та розглянута удосконалена конструкція S перетворення, в котрому для 64-х бітного вхідного блоку даних активізується (*вже на першому циклі*) мінімум чотири S-блоки, чого не дозволяють відомі конструкції циклових перетворень сучасних шифрів (*за виключенням шифру Лабіринт, в котрому на вході першого циклу використовується додаткове нелінійне перетворення*).

Посилання

[1] Opys potochnogo shyfru Strumok.

[2] Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – K.: Derzhspozhyvstandart Ukrai'ny, 2015. – 238 s. – (Nacional'nyj standart Ukrai'ny).

[3] Rodinko M.Yu. Improvement of the method for optimal S-boxes generation / M.Yu. Rodinko, R.V. Oliynykov, T.O. Hrinenko // Applied Radio Electronics. – 2015. – V.14. – No.4. – pp. 315-320.

[4] Gorbenko I. D. O dinamike prikhoda blochnykh simmetrichnykh shifrov k sluchainoi podstanovke / I. D. Gorbenko, K. E. Lisitskii // Radiotekhnika – Vseukr. mezhved. nauchn.-tekhn. sb. – 2014. – Vip. 176. – S. 27-39.

[5] Gorbenko I.D. On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov // Universal Journal of Electrical and Electronic Engineering, 2, 2014 – pp. 206-215. doi: 10.13189/ujeee.2014.020409.

[6] Lisitskii K. E. Maksimal'nye znacheniya polnykh differentsialov i lineinykh korpusov blochnykh simmetrichnykh shifrov / K. E. Lisitskii // Tekhnologicheskii audit i rezervy proizvodstva. – 2014. – № 1/1 (15) – S. 47-52.

[7] Dolgov V. I. The new concept of block symmetric ciphers design / V.I. Dolgov, I.V. Lisitska, K.Ye. Lisitskyi // doi: 10.1615 / TelecomRadEng. v. 76. i. 2. pp. 157-184.

Reviewer: Alexandr Kuznetsov, Doctor of Technical Sciences, Prof., Academician of the Academy of Sciences of Applied Radio Electronics, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine.
E-mail: kuznetsov@karazin.ua

Received: April 2018.

Authors:
Konstantin Lisitzky, postgraduate student of the Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine.

E-mail: lisickiy@ukr.net

Strategy of selection of S-blocks for nonlinear transformation of cipher Strumok.

Abstract. The peculiarities of the construction of the S-transform of the Stream cipher "Strumok" are discussed. In particular, attention is focused on the choice of S-blocks for this transformation. The rates of its randomness are estimated, in particular, the minimum number of cycles of reuse of this transformation is determined, after which the result of encryption comes to the indicators of the stationary state of random substitution. Consideration of the possibility of using in the S transformation of random S-blocks. It is concluded that random S-blocks do not worsen the indicators of its randomness. It is proposed to improve this S-conversion design, which allows to improve its randomness. It is built on using instead of a parallel set of S-blocks of a managed substitution chain with a positive blended linear transformation of segments of data blocks at the input of a layer of controlled substitutions. It is shown that this design allows, at a single pass, to activate at least four S-blocks, instead of one S-block in the original design. The proposed enhanced S-conversion design appears to be more efficient and allows for at least 20 cycles of S-blocks to be activated in three cycles in the original design, which further improves the chance of improvement.

Keywords: stream cipher; random indices; random S-blocks; active S-blocks; controlled substitutions.

Рецензент: Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, площадь Свободы 6, г. Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Поступила: Апрель 2018.

Авторы:
Константин Лисицкий, аспирант кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, площадь Свободы 6, г. Харьков, 61022, Украина.
E-mail: lisickiy@ukr.net

Стратегия выбора S-блоков для нелинейного преобразования шифра Струмок.

Аннотация. Обсуждаются особенности построения S-преобразования шифра "Струмок". В частности внимание сосредотачивается на выборе S-блоков для этого преобразования. Оцениваются показатели его случайности, в частности определяется минимальное число циклов повторного использования этого преобразования, после которого результат зашифрования приходит к показателям стационарного состояния случайной подстановки. Рассматривается возможность использования в S преобразовании случайных S-блоков. Делается вывод, что случайные S-блоки не ухудшают показателей его случайности. Предлагается усовершенствование этой конструкции S-преобразование, которое позволяет улучшить показатели его случайности. Оно строится на использовании вместо параллельного набора S-блоков цепочки из управляемых подстановок с положительным смешивающим линейным преобразованием сегментов блоков данных на входе слоя управляемых подстановок. Показывается, что эта конструкция позволяет уже при однократном проходе активизировать минимум четыре S-блоки, вместо одного S-блока в исходной конструкции. Предложенная усовершенствованная конструкция S-преобразования представляется более быстродействующей и позволяет за три цикла активизировать минимум 20-ть S-блоков вместо 16-ти в исходной конструкции, дополнительно улучшает показатели случайности совершенствования.

Ключевые слова: потоковый шифр; показатели случайности; случайные S-блоки; активные S-блоки; управляемые подстановки.