адаптивного метода защиты с обнаружением и нейтрализацией всех атак НСД - если мы не можем построить абсолютно защищенную корпоративную сеть Интранет, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом (адаптивно) реагировать на них.

Список литературы

1.2000 CSI/FBI Computer and Security Survey.Computer Security Institue. Federal Bureau Investigation's Computer Intrusion Squad.

2. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л.Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах ОВС Уаїни. Видавництво НАВСУ, 2003. С.316.

3. Пакет из пяти нормативных документов по вопросам защиты информации от несанкционированного доступа Департамента СТСЗИ СБ Украины, К., 1999.

4. В.В.Шорошев. Базовая модель экспертной системы оценки безопасности информации в компьютерных системах. // Научно-технический сборник КПИ, Минобразования и науки Украины, ДСТСЗИ СБ Украины. Выпуск 3. - 2001.

5. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. С.624.

6. Richard Power. Crrent and Future Danger: A CSI Primer on Computer Crime and Information Warfare. Computer Sequrity Institute. 1995.

Поступила 25.04.2007 г.

УДК 681.3.06

Дирда О.В., Скрипник Л.В.

УДОСКОНАЛЕННЯ МЕТОДУ КОРЕЛЯЦІЙНОГО КРИПТОАНАЛІЗУ ДЛЯ ОДНОГО ТИПУ КОМБІНАЦІЙНОГО ГЕНЕРАТОРА

Одним із потужних методів криптографічного аналізу, який може бути застосовано проти потокових шифрів, є кореляційний метод криптоаналізу [1, 2]. Цей метод засновано на обчисленні кореляції вихідних значень двійкових (булевих) функцій з їх вхідними значеннями. Для двійкової функції $f = f(x_1, x_2, ...x_n)$ від n змінних кореляція між i-им "входом" та значенням функції обчислюється за формулою

$$c_i = p\left(x_i = 1 \middle/ f = 1\right).$$

Розглянемо випадок, коли у потоковому шифрі використовується S-блок розміру $n \times n$ (або $n \times n$ S-блок), який являє собою функцію $S : V_n \to V_n$, де V_n – лінійний простір бітових векторів довжини n. S-блок розміру $n \times n$ може бути поданий як система з n булевих функцій $f_j : V_n \to \{0,1\}$, $j = \overline{1,n}$, які носять назву координатних функцій S-блоку.

Для $n \times n$ S-блоку вводять так звану матрицю кореляційних коефіцієнтів, яка визначає кореляцію між i-им "входом" та j-им "виходом". Елемент $c_{i,j}$ цієї матриці носить назву кореляційного коефіцієнту та обчислюється за формулою

$$c_{i,j} = p\left(x_i = 1 \middle/ f_j = 1\right),$$

де $i, j = \overline{1,n}$.

Для координатної функції f_j S-блоку максимальне відхилення від 0.5 кореляційних коефіцієнтів позначимо через Δ_j. Очевидно, що Δ_j обчислюється за формулою

$$\Delta_j = \max_{i=\overline{1,n}}(|c_{i,j} - 0.5|).$$

Кореляційну "усталеність" S-блоку характеризує параметр

$$\Delta = \max_{j=\overline{1,n}} \Delta_j = \left|0.5 - \max_{i,j=\overline{1,n}} c_{i,j}\right|.$$

У роботі [2] розглядається застосування кореляційного методу криптоаналізу проти "класичного" комбінаційного генератора гами, який містить декілька лінійних рекурентних регістрів (ЛРР) на нелінійну функцію ускладнення, яка носить назву комбінуючої функції. Розглянемо випадок, коли комбінаційний генератор містить n ЛРР довжини m кожний, а вихідна функція являє собою $n \times n$ S-блок. Структурна схема такого генератора зображена на рис. 1.

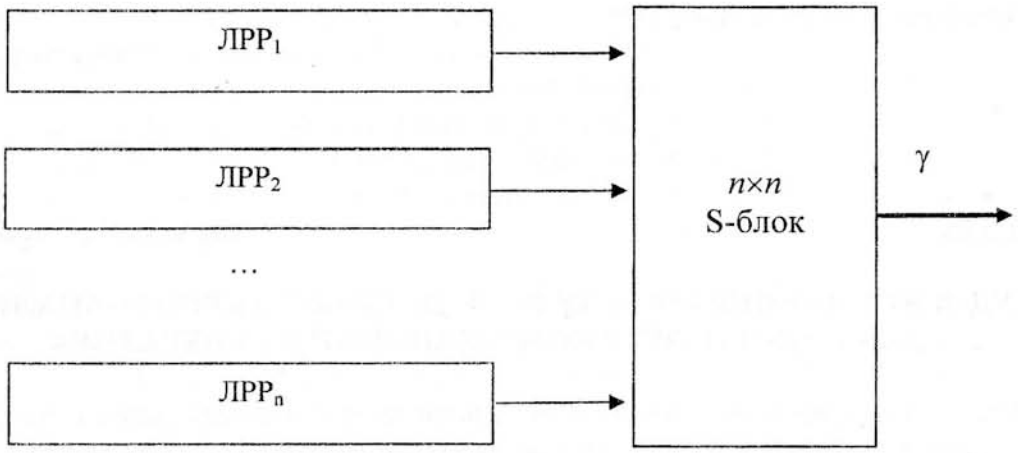

Рис. 1. Структурна схема комбінаційного генератора

За кожен такт роботи генератора з ЛРР здійснюється знімання n бітів, які поступають на вхід S-блоку. Вихідним знаком гами генератора є n-бітове число γ.

Особливістю такого генератора, у порівнянні з "класичним", є те, що вихідні послідовності ЛРР поступають на вхід n двійкових функцій, замість одної. Як наслідок цього, метод кореляційного криптоаналізу може бути удосконалено за рахунок розгляду кореляції послідовностей з виходу окремих ЛРР з декількома бітами послідовності $\{\gamma\}$.

Позначимо i-ий ЛРР генератора через $L^{(i)}$, де $i = \overline{1,n}$, а вихідний біт ЛРР у такті з номером t через $l^{(i)}(t)$. Знак гами у такті з номером t позначимо через $\gamma(t)$, а i-ий біт числа $\gamma(t)$ – через $\gamma^{(i)}(t)$. У введених позначеннях у такті з номером t виконується система рівнянь

$$\begin{cases} \gamma^{(1)}(t) = f_1(l^{(1)}(t),...,l^{(n)}(t)) \\ \quad ... \\ \gamma^{(n)}(t) = f_n(l^{(1)}(t),...,l^{(n)}(t)) \end{cases}$$

Нехай зі змінною x_i найбільшу кореляцію мають функції f_{i_1}, f_{i_2},..., $f_{i_{k(i)}}$, де $k(i) \geq 2$.

Для кожного з $2^m - 1$ ненульових початкових значень регістра $L^{(i)}$ обчислюємо $k(i)$ функцій

$$G_i^{(i_j)} = \sum_{t=1}^{N} (\gamma^{(i_j)}(t) \oplus l^{(i)}(t)),$$

де $j = \overline{1,k(i)}$, N – кількість тактів роботи генератора. Функція $G_i^{(i_j)}$, яка носить назву функції нев'язки, визначає кореляцію між i-им "входом" та i_j-им "виходом" S-блоку.

Для кожного $j = \overline{1,k(i)}$ якщо $c_{i,i_j} > 0.5$, то вибираємо t значень регістру $L^{(i)}$, які мають найменші значення функції нев'язки $G_i^{(i_j)}$, а якщо $c_{i,i_j} < 0.5$, то вибираємо t значень, які мають найбільші значення функції нев'язки $G_i^{(i_j)}$. Множину відібраних значень позначимо через $X_t^{(i,i_j)}$. Число t є параметром алгоритму, який залежить від значення $\max_{j=\overline{1,k(i)}}(\Delta_{i_j})$.

У якості вірного початкового значення регістру $L^{(i)}$ вибираємо значення, яке належить множині

$$\bigcap_{j=\overline{1,k(i)}} X_t^{(i,i_j)}.$$

Алгоритмічна складність запропонованого методу оцінюється величиною $O(n2^m)$.

Далі розглянемо приклад застосування удосконаленого методу кореляційного криптоаналізу для комбінаційного генератора, в якому використовується S-блок криптографічного алгоритму Twofish. Блоковий шифр Twofish розроблено у 1998 році групою з шести криптографів на чолі з Б.Шнайером.

У шістнадцятковому форматі S-блок алгоритму Twofish має наступний вид:

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

Транспонована матриця кореляційних коефіцієнтів даного S-блоку дорівнює:

```
0.453125 0.515625 0.453125 0.484375 0.500000 0.546875 0.484375 0.453125
0.484375 0.515625 0.515625 0.546875 0.515625 0.515625 0.453125 0.531250
0.562500 0.437500 0.531250 0.484375 0.578125 0.484375 0.515625 0.515625
0.515625 0.500000 0.484375 0.484375 0.468750 0.562500 0.515625 0.531250
0.546875 0.484375 0.546875 0.531250 0.500000 0.421875 0.500000 0.515625
0.484375 0.593750 0.484375 0.453125 0.437500 0.500000 0.500000 0.453125
0.578125 0.421875 0.531250 0.500000 0.515625 0.546875 0.531250 0.484375
0.437500 0.484375 0.500000 0.453125 0.484375 0.515625 0.500000 0.437500
```

У матриці ті значення кореляційних коефіцієнтів, які мають найбільші відхилення від 0.5, виділені жирним шрифтом для кожної з координатних функцій. Транспонована матриця модулів відхилень кореляційних коефіцієнтів від 0.5 дорівнює:

```
0.046875 0.015625 0.046875 0.015625 0.000000 0.046875 0.015625 0.046875
0.015625 0.015625 0.015625 0.046875 0.015625 0.015625 0.046875 0.031250
0.062500 0.062500 0.031250 0.015625 0.078125 0.015625 0.015625 0.015625
0.015625 0.000000 0.015625 0.015625 0.031250 0.062500 0.015625 0.031250
0.046875 0.015625 0.046875 0.031250 0.000000 0.078125 0.000000 0.015625
0.015625 0.093750 0.015625 0.046875 0.062500 0.000000 0.000000 0.046875
0.078125 0.078125 0.031250 0.000000 0.015625 0.046875 0.031250 0.015625
0.062500 0.015625 0.000000 0.046875 0.015625 0.015625 0.000000 0.062500
```

Значення Δ_j та номери вхідних змінних функції, які відповідає найбільшому відхиленню, наведені у таблиці 1.

Таблиця 1.

Функція	Δ	Вхід
f_1	0.046875	1, 3, 6, 8
f_2	0.046875	4, 7
f_3	0.078125	5
f_4	0.0625	6
f_5	0.078125	6
f_6	0.09375	2
f_7	0.078125	1, 2
f_8	0.0625	1, 8

Таблиця 2.

ЛРР	Початковий стан ЛРР	
	bin	hex
1	000011000011000	0x0C30
2	011010001100011	**0x6316**
3	010111000000011	0x603A
4	000100011001111	0x7988
5	110111011111011	0x6FBB
6	000110010001011	**0x6898**
7	001011101100110	0x3374
8	000000001100001	0x4300

Як видно з таблиці 1, з одним й тим же вхідним значенням корелюють декілька вихідних значень, зокрема з другою змінною корелюють вихідні значення координатних функцій f_6 та f_7, а з шостою змінною – функцій f_4 та f_5.

Нехай довжина ЛРР дорівнює 15, а поліном зворотного зв'язку регістрів дорівнює $x^{15}+x+1$. З використанням програмної моделі комбінаційного генератора було згенеровано 100 Кбайт гами. Початковий стан ЛРР наведений у таблиці 2.

Нехай t=5. Значення $X_5^{(2,6)}$ та $X_5^{(2,7)}$ наведені у таблицях 3 та 4 відповідно.

Таблиця 3.

№	ЛРР2	$G_2^{(6)}$
1	0x7e36	37509
2	**0x6316**	40635
3	0x51a1	42201
4	0x55ae	43729
5	0x4d42	43735

Таблиця 4.

№	ЛРР2	$G_2^{(7)}$
1	0x53d3	59369
2	**0x6316**	57836
3	0x6dc9	57833
4	0x6f26	57819
5	0x22f9	57803

$X_5^{(2,6)} \cap X_5^{(2,7)}$={0x6316}. Як видно з таблиці 2, це є істиним значенням ЛРР2.

Нехай t=10. Значення $X_{10}^{(6,4)}$ та $X_{10}^{(6,5)}$ наведені у таблицях 5 та 6 відповідно.

$X_{10}^{(6,4)} \cap X_{10}^{(6,5)}$={0x6898}, що є істиним значенням ЛРР6 (див. табл. 2).

Наведений приклад свідчать про можливість застосування удосконаленого методу кореляційного криптоаналізу для відновлення початкових станів лінійних рекурентних регістрів комбінаційних генераторів гами, вихідна функція яких являє собою S-блок.

Таблиця 5.

№	ЛРР6	$G_6^{(4)}$
1	0x1a9e	39056
2	0x5ccf	40614
3	0x0b13	40642
4	0x123c	42142
5	0x5533	42173
6	0x33e9	42188
7	0x319b	43723
8	**0x6898**	43726
9	0x176d	43727
10	0x5f7e	43741

Таблиця 6.

№	ЛРР6	$G_6^{(5)}$
1	0x21d5	57848
2	**0x6898**	57797
3	0x377b	56286
4	0x439d	56280
5	0x74e6	56268
6	0x4c81	56253
7	0x0e42	56242
8	0x322a	56239
9	0x7609	56236
10	0x5fe3	56203

Далі розглянемо кореляційні характеристики S-блоків 22 сучасних криптографічних алгоритмів. Назви алгоритмів, їх типи та країни, де вони були розроблені, наведені у таблиці 7. Результати детального аналізу криптографічних властивостей S-блоків більшості з цих алгоритмів наведені у роботі [3].

Таблиця 7.

Алгоритм	**Країна**	**Тип алгоритму**
Rijndael	Бельгія	Блоковий шифр
Skipjack	США	Блоковий шифр
Whirlpool	Бельгія, Бразилія	Геш-функція
Twofish	США	Блоковий шифр
Crypton	Південна Корея	Блоковий шифр
Snow 1.0	Швеція	Потоковий шифр
E2	Японія	Блоковий шифр
Square	Бельгія	Блоковий шифр
Safer+	США	Блоковий шифр
MD2	США	Геш-функція
Turing	Австралія	Потоковий шифр
RC2	США	Блоковий шифр
Hierocrypt-3	Японія	Блоковий шифр
Camellia	Японія	Блоковий шифр
Q	США	Блоковий шифр
CS	Франція	Блоковий шифр
Anubis	Бельгія, Бразилія	Блоковий шифр
Торнадо	Україна	Блоковий шифр
BelT	Білорусія	Блоковий шифр
DESX	США	Блоковий шифр
SEED	Південна Корея	Блоковий шифр
PY	Ізраїль	Потоковий шифр

Серед розглянутих алгоритмів блокові шифри Rijndael, Twofish, Crypton, E2, Square, Safer+ розглядались у проекті Advanced Encryption Standard (AES), алгоритми Whirlpool, Camellia, SNOW 1.0, Q, CS, Anubis, Hierocrypt-3 – у проекті New European Schemes for Signatures, Integrity, and Encryption (NESSIE), а алгоритм PY – у проекті eSTREAM. Алгоритм Skipjack розроблено Агенцією національної безпеки США, алгоритм "Торнадо" – АТ "Інститут інформаційних технологій" (м. Харків), алгоритм "BelT" – Національним науково-дослідним центром прикладних проблем математики і інформатики Білоруського державного університету та Державним центром безпеки інформації при Президенті Республіки Білорусь.

Слід відзначити, що S-блоки ряду з розглянутих алгоритмів використовуються в інших алгоритмах. Наприклад, S-блок алгоритму Skipjack використовується в потокових

шифрах Sober-t8, Sober-t16, Sober-t32, Sober-t128, NLS, а S-блок алгоритму Rijndael – в алгоритмах Scream, HBB, Squafer, Mir-1, Grand Cru, Snow 2.0, MUGI, Hermes8-80, Polar Bear.

У таблиці 8 наведені значення параметра Δ для S-блоків даних алгоритмів, а у таблиці 9 – значення параметрів Δ_j, де $j = \overline{1,8}$.

Таблиця 8.

Алгоритм	Δ	**Алгоритм**	Δ
Rijndael	0.0625	Торнадо	0.046875
Crypton	0.125	Camellia	0.0546875
E2	0.0546875	Q	0.0625
MD2	0.0625	CS	0.125
RC2	0.101562	Anubis	0.0703125
Safer+	0.09375	Hierocrypt-3	0.0625
Skipjack	0.0625	Turing	0.0859375
Snow 1.0	0.0625	BelT	0.0625
Square	0.0546875	DESX	0.0859375
Twofish	0.09375	SEED	0.0546875
Whirlpool	0.101562	PY	0.0625

Таблиця 9.

Алгоритм	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	Δ_8
Rijndael	0.046875	0.046875	0.0625	0.0625	0.046875	0.0625	0.0625	0.046875
Торнадо	0.046875	0.046875	0.046875	0.046875	0.0390625	0.046875	0.046875	0.046875
Whirlpool	0.046875	0.0703125	0.046875	0.101562	0.0546875	0.0390625	0.0546875	0.0703125
Square	0.046875	0.0546875	0.046875	0.0546875	0.0546875	0.046875	0.046875	0.046875
Snow 1.0	0.03125	0.0625	0.0625	0.0625	0.03125	0.0625	0.0625	0.0625
Skipjack	0.0546875	0.03125	0.0625	0.0625	0.046875	0.046875	0.0390625	0.046875
Crypton	0.0625	0.0625	0.0625	0.0625	0.125	0.0625	0.03125	0.125
E2	0.0390625	0.046875	0.0546875	0.0234375	0.0390625	0.046875	0.0234375	0.046875
MD2	0.0546875	0.0546875	0.0546875	0.03125	0.0625	0.03125	0.0546875	0.0390625
RC2	0.101562	0.078125	0.046875	0.0546875	0.0625	0.0546875	0.0390625	0.0546875
Safer+	0.015625	0.0625	0.046875	0.03125	0.0546875	0.0234375	0.078125	0.09375
Twofish	0.046875	0.046875	0.078125	0.0625	0.078125	0.09375	0.078125	0.0625
Camellia	0.046875	0.0546875	0.0390625	0.03125	0.046875	0.0546875	0.0546875	0.0546875
Q	0.046875	0.046875	0.0625	0.0625	0.046875	0.0625	0.0625	0.046875
CS	0.125	0.0625	0.125	0	0.125	0.125	0.125	0.125
Anubis	0.0625	0.0625	0.0390625	0.0703125	0.0390625	0.0546875	0.0703125	0.0625
Hierocrypt-3	0.0546875	0.046875	0.0625	0.0625	0.046875	0.0546875	0.0546875	0.0546875
Turing	0.0234375	0.0703125	0.0703125	0.0859375	0.046875	0.046875	0.0703125	0.0546875
DESX	0.0625	0.0859375	0.046875	0.0625	0.0625	0.046875	0.046875	0.046875
BelT	0.0546875	0.0390625	0.046875	0.0390625	0.0625	0.03125	0.03125	0.0546875
PY	0.0390625	0.03125	0.0625	0.0546875	0.0546875	0.046875	0.046875	0.0546875
SEED	0.046875	0.0546875	0.0390625	0.046875	0.0546875	0.0546875	0.046875	0.046875

Відсортировані у порядку збільшення параметра Δ алгоритми наведені у таблиці 10.

Таблиця 10.

Δ	**Алгоритми**
0.046875	Торнадо
0.0546875	E2, Square, Camellia, SEED
0.0625	Rijndael, MD2, Skipjack, Q, SNOW 1.0, Hierocrypt-3, BelT, PY
0.0703125	Anubis
0.0859375	Turing, DESX
0.09375	Safer+, Twofish
0.101562	RC2, Whirlpool
0.125	Crypton, CS

У таблиці 11 наведені номери змінних, від яких статистично залежать координатні функції S-блоків.

Таблиця 11.

Алгоритм	i_1	i_2	i_3	i_4	i_5	i_6	i_7	i_8
Rijndael	1, 5, 8	8	8	7	3, 4	3	2	1, 6
Торнадо	6	4	1,2, 6	3	4	5, 7	1,2, 7	3
Whirlpool	6	8	2, 4	8	2	1	7	4
Square	4, 5	2	7	6, 8	7	8	4	1
Snow 1.0	1, 2, 4, 5, 8	4	7	2	3, 4, 6	2	6	2, 5
Skipjack	4	6	2, 8	5, 6	1, 8	6	2, 4, 5, 7	8
Crypton	8	5	5, 6	8	4	3, 8	5, 6, 8	2, 3
E2	1	4	2	6	3, 8	8	1, 6	6
MD2	8	6, 8	1, 6	5	7, 8	1, 6, 7	3	5, 6
RC2	6	4	7	5	1	3	3, 4	4
Safer+	8	1, 3, 4, 5	2	2, 6	8	7	8	8
Twofish	1, 3, 6, 8	4, 7	5	6	6	2	1, 2	1, 8
Camellia	3, 5, 7	7	4, 7, 8	5	3, 6	7	5	8
Q	1, 5, 8	8	8	7	3, 4	3	2	1, 6
CS	5	6	8	-	1, 5	6	7	3, 8
Anubis	2	1	7	7	6	2, 7	4	8
Hierocrypt-3	3	8	7	8	3	8	4	7
Turing	5, 8	8	6	8	1, 8	3	2	2
DESX	8	1	5	6	8	6	2	5, 8
BelT	5	4	5	8	6	2, 4, 7	5, 7	6
PY	5	3, 4, 7	5	2, 6	1	1, 7	7	7
SEED	1	2	1	1, 6, 7	2	2, 7	1	7

Як видно з таблиць 8 та 10, найгірші показники параметра Δ мають S-блоки алгоритмів CS та Crypton, найкращий показник – S-блок алгоритму Торнадо. Варто зауважити, що в алгоритмі Торнадо використовуються три S-блоки, для яких значення параметру Δ дорівнює 0.046875, 0.0625, 0.0546875 відповідно.

З таблиці 9 видно, що властивості кореляційної імунності першого порядку задовольняє тільки четверта координатна функція S-блоку алгоритму CS, алгебраїчна нормальна форма (многочлен Жегалкіна) якої дорівнює $x_4x_2 + x_8x_5x_2 + x_5x_2 + x_2 + x_4x_3 + x_8x_5x_3 + x_5x_3 + x_7x_6x_4 + x_8x_7x_4 + x_7x_4 + x_8x_4 + x_4 + x_8x_7x_6x_5 + x_7x_6x_5 + x_8x_7x_5 + x_7x_5 + x_8x_5 + x_7x_6 + x_7 + 1$. Слід зазначити, що функція суттєво залежить тільки від 7 змінних.

Матриця кореляційних коефіцієнтів S-блоку алгоритму CS наведена нижче

$$\begin{pmatrix} 0.5 & 0.5 & 0.5 & 0.5 & 0.625 & 0.5625 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5625 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.625 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 \\ 0.625 & 0.5 & 0.5 & 0.5 & 0.375 & 0.46875 & 0.5 & 0.5 \\ 0.5625 & 0.5625 & 0.5 & 0.5 & 0.46875 & 0.375 & 0.53125 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.53125 & 0.375 & 0.5 \\ 0.5 & 0.5 & 0.625 & 0.5 & 0.5 & 0.5 & 0.5 & 0.375 \end{pmatrix}.$$

Як видно з таблиці 11, для всіх розглянутих S-блоків кілька координатних функцій статистично залежать від одної змінної. Саме цю властивість використовується в удосконаленому методі кореляційного криптоаналізу у випадку, якщо у потоковому шифрі в якості вихідної функції використовується S-блок.

З метою визначення розподілу значення параметра Δ були проведені емпіричні дослідження, а саме, згенеровано 10^6 псевдовипадкових 8×8 S-блоків та обчислено значення параметра Δ з точністю 4 десяткових знаки після коми. Числові значення, які отримані у результаті експерименту, наведені у таблиці 12, а графік імовірності значень параметра Δ наведено на рис. 2.

Таблиця 12.

Δ	*p*	Δ	*p*	Δ	*p*
0.039	0.000004	0.0859	0.199976	0.1328	0.001472
0.0468	0.000750	0.0937	0.119803	0.1406	0.000492
0.0546	0.016626	0.1015	0.060519	0.1484	0.000145
0.0625	0.092877	0.1093	0.026999	0.1562	0.000044
0.0703	0.210913	0.1171	0.011141	0.164	0.000010
0.0781	0.253915	0.125	0.004313	0.1718	0.000001

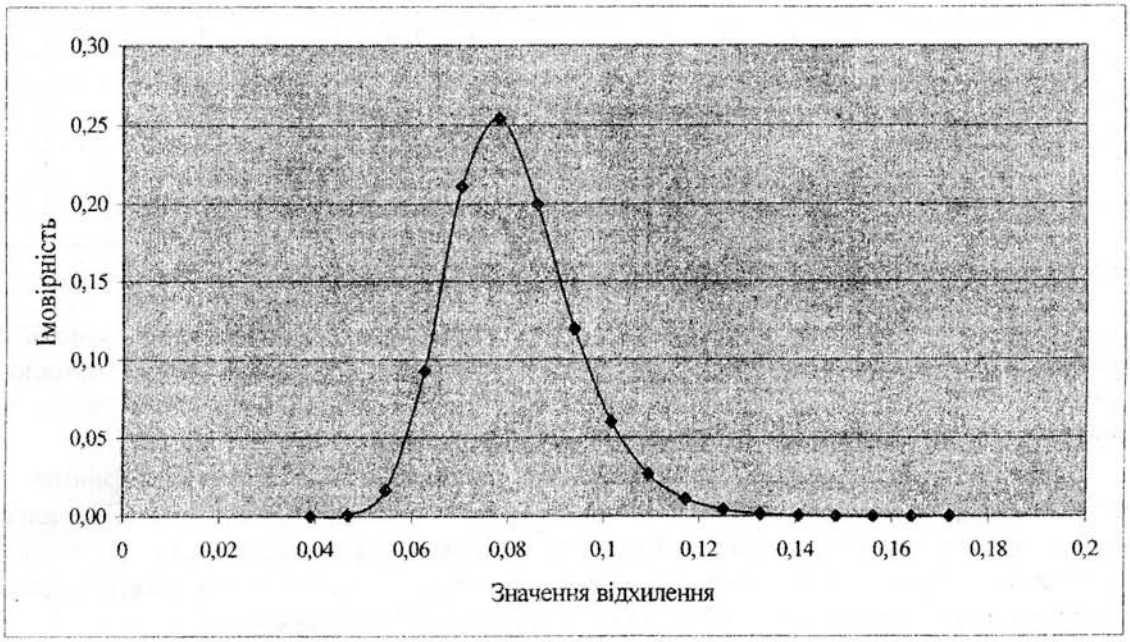

Рис. 2. Імовірність значень параметра Δ для 8×8 S-блоків

Математичне очікування параметра Δ для 8×8 S-блоків приблизно дорівнює 0.08.

Проведений аналіз кореляційних властивостей S-блоків 26 криптографічних алгоритмів свідчить про потенційну можливість застосування удосконаленого методу криптоаналізу у випадку використання S-блоків цих алгоритмів в комбінаційних генераторах гами потокових шифрів. Емпіричні дослідження свідчать про те, що "випадкові" 8×8 S-блоки також не мають прийнятних кореляційних характеристик.

Висновки

Запропонований у статті удосконалений метод кореляційного криптоаналізу може бути використано проти одного типу комбінаційного генератора, в якому в якості вихідної функції використовується S-блок. Метод дозволяє відновити початковий стан лінійних рекурентних регістрів комбінаційного генератора навіть при невеликих відхиленнях кореляційних коефіцієнтів від 0.5.

Для запобігання застосування цього методу в комбінаційних генераторах такого типу S-блоки необхідно вибирати таким чином, щоб усі їх координатні функції задовольняли

властивості кореляційної імунності першого порядку. Приклад такого S-блоку наведено у роботі [3]. У цьому випадку усі кореляційні коефіцієнти дорівнюють 0.5, отже, буд-який "вихід" статистично не залежить від "входу", що унеможливлює застосування запропонованого методу.

Список літератури

1. *Siegenthaler T.* Correlation immunity of non-linear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. –1984. –V.30. –P.776-780.

2. *Siegenthaler T.* Decrypting a class of stream ciphers using ciphertext only // IEEE Trans. Comput. –1985. – V.34.

3. *Л.Скрипник, О.Дирда.* Порівняльний аналіз методів побудови та властивостей S-блоків ряду сучасних криптографічних алгоритмів. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, –К.: 2005. –Вип.10. –С.85–98.

Надійшла 17.05.2007 р.

УДК 681.3.07

Жердєв М.К., Лєнков С.В., Пампуха І.В.

СПОСІБ ЗАШИФРУВАННЯ - РОЗШИФРУВАННЯ ІНФОРМАЦІЇ З ВИПАДКОВИМ, ВІДКРИТИМ І АДАПТИВНИМ КЛЮЧЕМ

Спосіб зашифрування – розшифрування інформації з випадковим, відкритим і адаптивним ключем (ВВАК) призначений для криптографічного перетворення інформації в мережі, захисту від атак вірусів і несанкціонованого доступу (хакерів) в комп'ютери через цю мережу. Він може бути реалізований програмно, апаратно і програмно-апаратно.

Кращим захистом від способів криптоаналізу є вибір ключового слова по довжині, рівного довжині відкритих даних (ВД), яке відрізняється від відкритих даних за статистичними показниками. Таку схему було запропоновано інженером компанії AT&T Гілбертом Вернамом в 1918 р., у якій оперують не буквами, а двійковими числами. Коротко це можна виразити формулою [1]:

$$C_i = p_i \oplus k_i,$$

де:

p_i – *i-е* двійкове значення ВД;

k_i – *i-е* двійкове значення ключа;

C_i – *i*-е двійкове значення закритих даних (ЗД);

$\oplus$ – операція «виключення АБО».

Таким чином, ЗД генеруються шляхом побітового виконання операції виключення «АБО» для ВД й ключа.

Основною проблемою при цьому є спосіб генерування ключа, який за статистичними показниками відрізнявся б від ВД. Вернам запропонував використовувати закільцьовану стрічку, тобто циклічне повторення ключового слова, тому насправді виконувалась операція зашифрування ВД, хоч і з дуже довгим, але все-таки ключем, який повторюється. Незважаючи на те, що така схема, в силу дуже великої довжини ключа, значно ускладнює завдання криптоаналізу, схему можна «зламати», маючи в розпорядженні досить довгий фрагмент ЗД, відомі або ймовірно відомі фрагменти ВД або й те, і інше відразу.