S E N S ' 2 0 0 6
Second Scientific Conference with International Participation
SPACE, ECOLOGY, NANOTECHNOLOGY, SAFETY
14 – 16 June 2006, Varna, Bulgaria

АНАЛИЗ НА ЧЕТИРИРАЗРЯДЕН ЛИНЕЕН ПРЕМЕСТВАЩ РЕГИСТЪР С ОБРАТНА ВРЪЗКА, ИЗПОЛЗВАН КАТО ГЕНЕРАТОР НА КЛЮЧ В КРИПТОСИСТЕМИ С ПОТОЧНО ШИФРИРАНЕ

Адриана Бороджиева

Русе 7017, ул. „Студентска" № 8, Русенски университет „Ангел Кънчев",
Катедра „Комуникационна техника и технологии", тел.: (00359 82) 888 734,
e-mail: aborodjieva@ecs.ru.acad.bg

Ключови думи: криптосистеми, поточно шифриране, линейни преместващи регистри с обратна връзка.

Резюме. *Статията описва разработен програмен модул на MS Excel, който позволява да се определи състоянието на четириразряден линеен преместващ регистър, използван като генератор на псевдослучайна ключова последователност в системи с поточно шифриране, в няколко последователни такта, при зададено начално състояние, както и шифрирания текст с използване на генерирания ключов поток, при зададен открит текст. С помощта на създадения програмен модул може да се открият и съединенията в обратната връзка на регистъра, като по този начин се демонстрира уязвимостта му към атака на известния открит текст. Разработеният модул може да се използва от студенти, изучаващи дисциплините „Комуникационни системи" (по-специално криптосистемите) и „Анализ и синтез на логически схеми".*

ВЪВЕДЕНИЕ

Като *генератор на ключ* в системите за поточно шифриране се използват най-често *линейни преместващи регистри с обратна връзка*. Тези регистри се прилагат широко и в теорията на кодирането, в частност при реализацията на шумоустойчиви циклични кодове, и често се наричат *линейни превключващи схеми* или *линейни последователностни машини*. Много потокови шифри от този тип са засекретени и се използват активно във военните криптографски системи. Известни са и редица комерсиални приложения, като например, на френския потоков шифър A5 в GSM, където се използват три линейни преместващи регистъра с обратна връзка, с дължини съответно 19, 22 и 23 бита, т.е. използва се 64-битов секретен ключ, от който се генерира ключовия поток [1]. В статията се описва разработен програмен модул на MS Excel, който разглежда само четириразряден преместващ регистър с обратна връзка, свързваща чрез логически елемент от типа „сума по модул 2" (известен още и с наименованието си „изключващо ИЛИ") произволни два или три тригера на регистъра. Възможните варианти са девет – обратна връзка, съединяваща съответно тригери 1 и 2; 1 и 3; 1 и 4; 2 и 3; 2 и 4; 3 и 4; 1, 2 и 3; 1, 2 и 4; 2, 3 и 4. Създаденият модул обхваща за демонстрация само три от тях и съдържа следните работни листа:

1) 4SR_1_2 – за демонстрация на действието на регистър с обратна връзка от първи и втори елемент;

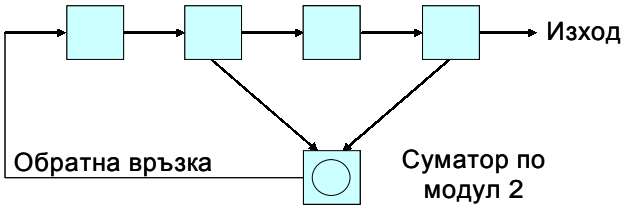
2) 4SR_1_3 – с обратна връзка от първи и трети елемент;

3) 4SR_1_2_3 – с обратна връзка от първи, втори и трети елемент;

4) 4SR_A – с негова помощ, при захванати от криптоаналитика открит текст и неговия шифриран еквивалент, се определят съединенията в обратната връзка на регистъра.

ОПИСАНИЕ НА ПРОГРАМНИЯ МОДУЛ И РЕЗУЛТАТИ ОТ АНАЛИЗА

Действие на четириразряден линеен преместващ регистър с обратна връзка, обхващаща първи и трети елемент

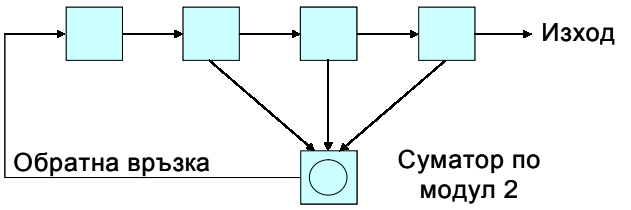


№ такт	x_4	x_3	x_2	x_1	Открит текст	Шифро-текст
1	1	0	1	0	1	1
2	0	1	0	1	0	1
3	0	0	1	0	1	1
4	0	0	0	1	0	1
5	1	0	0	0	1	1
6	0	1	0	0	0	0
7	1	0	1	0	1	1
8	0	1	0	1	0	1

Предаван ключов поток	**01010001**
Открит текст (нешифриран)	**10101010**
Шифриран текст	**11111011**

Фиг.1. Демонстрация на действието на четириразряден линеен преместващ регистър с обратна връзка, обхващаща първия и третия елемент

Действие на четириразряден линеен преместващ регистър с обратна връзка, обхващаща първи, втори и трети елемент



№ такт	x_4	x_3	x_2	x_1	Открит текст	Шифро-текст
1	1	0	1	0	1	1
2	1	1	0	1	0	1
3	0	1	1	0	1	1
4	0	0	1	1	0	1
5	0	0	0	1	1	0
6	1	0	0	0	0	0
7	0	1	0	0	1	1
8	1	0	1	0	0	0

Предаван ключов поток	**01011000**
Открит текст (нешифриран)	**10101010**
Шифриран текст	**11110010**

На фиг.1 е показано действието във времето на четириразряден *линеен преместващ регистър с обратна връзка*, която обхваща първи и трети елемент, а на фиг.2 – съответно първи, втори и трети елемент. Началното състояние на регистъра и в двата случая е прието 1010 $(x_4 x_3 x_2 x_1)$, като то може да се избере произволно от потребителя в създадения с помощта на MS Excel програмен модул. Действието на регистъра за следващите седем такта се изчислява чрез формулите, заложени във всяка една от клетките, а именно (за регистъра от фиг.1):

$$(1)\qquad \begin{aligned} x_1^{t+1} &= x_2^{t} \\ x_2^{t+1} &= x_3^{t} \\ x_3^{t+1} &= x_4^{t} \\ x_4^{t+1} &= x_1^{t} \oplus x_3^{t} \end{aligned} \quad .$$

За регистъра от фиг.2 последната зависимост ще има вида:

$$(2)\qquad x_4^{t+1} = x_1^{t} \oplus x_2^{t} \oplus x_3^{t} .$$

Поради отсъствието на функцията *XOR* (сума по модул 2) в MS Excel, се налага изразяването ѝ чрез логическите функции от базис 1 (*AND*, *OR* и *NOT*), известни от булевата алгебра: $a \oplus b = a.\overline{b} \vee \overline{a}.b$ и $a \oplus b \oplus c = \overline{a}.\overline{b}.c \vee \overline{a}.b.\overline{c} \vee a.\overline{b}.\overline{c} \vee a.b.c$. Освен състоянието на регистъра за осем последователни такта, създаденият програмен модул позволява определянето на шифрирания текст чрез сумиране по модул 2 на зададения от потребителя открит текст и ключовия поток, който се получава в колонката за x_1. В демонстрационните примери е избран следният открит текст 10101010. И

Фиг.2. Демонстрация на действието на четириразряден линеен преместващ регистър с обратна връзка, обхващаща първия, втория и третия елемент

накрая, посредством вградената в MS Excel функция *CONCATENATE*, се извеждат разрядите на предавания ключов поток, на открития и на шифрирания текст.

На фиг.3 е показан пример за определяне на съединенията с обратната връзка на четириразряден линеен преместващ регистър. Единствените клетки, които се попълват от потребителя, или се изчисляват като сума по модул 2 на прихванатите от криптоаналитика открит текст и неговия шифриран еквивалент, са стойностите на битовете на ключовия поток, означени като $x_8, x_7, x_6, x_5, x_4, x_3, x_2, x_1$. Чрез тези стойности се попълва програмно матрицата $\mathbf{X}$ и вектора-стълб $\mathbf{x}$ [2], като:

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_5 \\ x_3 & x_4 & x_5 & x_6 \\ x_4 & x_5 & x_6 & x_7 \end{bmatrix} \text{ и } \mathbf{x} = \begin{bmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}. \quad (3)$$

Тъй като стълбовете на квадратната матрица $\mathbf{X}$ са линейно независими, то матрицата $\mathbf{X}$ е *неособена*, т.е. детерминантата ѝ е различна от нула [2]. От математиката е известно [3], че неособеността на една матрица е необходимо и достатъчно условие, за да има тя точно една обратна матрица $\mathbf{X}^{-1}$, за която $\mathbf{X}.\mathbf{X}^{-1} = \mathbf{X}^{-1}.\mathbf{X} = \mathbf{E}$ (с $\mathbf{E}$ е означена единичната матрица). Обратната матрица може да се пресметне чрез израза:

$$\mathbf{X}^{-1} = \left(A_{ji}\right) / \det \mathbf{X}, \quad (4)$$

където $\det \mathbf{X} = \sum_{i=1}^{n} x_{ji} A_{ji}$ е детерминантата на матрица $\mathbf{X}$, а A_{ji} са адюнгираните количества на елементите x_{ji}, поместени в матрицата $\mathbf{X}$ в j-ти ред, i-ти стълб. Тъй като $\det \mathbf{X} \neq 0$, а при определянето ѝ се извършва сумиране по модул 2, то винаги ще се получава, че $\det \mathbf{X} = 1$. Тогава зависимостта (4) може да се запише във вида:

$$\mathbf{X}^{-1} = \begin{bmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{bmatrix}. \quad (5)$$

Известно е, че адюнгираното количество (алгебричното допълнение) A_{ji} на елемента x_{ji} се определя от поддетерминантата D_{ji}, получена от детерминантата на матрица $\mathbf{X}$ след задраскване на j-тия ред и i-тия стълб. Тъй като в случая матрицата $\mathbf{X}$ е с размерност 4×4, то всички поддетерминанти D_{ji} ще са от трети ред и за изчисляването им може да се използва правилото на Сарус [3]. Тогава всяко от адюнгираните количества ще се определя по следния начин:

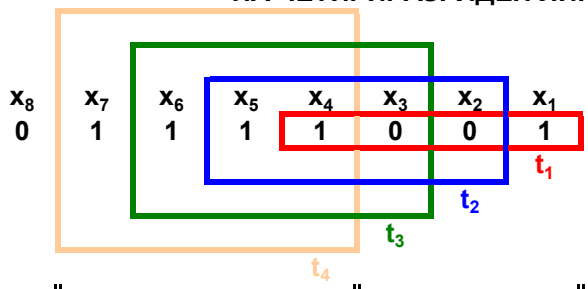
$$A_{ji} = \begin{vmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{vmatrix} = a_{11}.a_{22}.a_{33} \oplus a_{12}.a_{23}.a_{31} \oplus a_{13}.a_{21}.a_{32} \oplus$$

$$\oplus a_{13}.a_{22}.a_{31} \oplus a_{11}.a_{23}.a_{32} \oplus a_{12}.a_{21}.a_{33} = \quad (6)$$

$$= S_1 \oplus S_2 \oplus S_3 \oplus S_4 \oplus S_5 \oplus S_6.$$

В зависимост (6) всяко едно от тези трибуквени произведения е означено с S_i, $i = 1 \div 6$. Поради отсъствието на функцията *XOR* (сума по модул 2) в MS Excel, и тук се налага изразяването ѝ чрез логическите функции от базис 1 (*AND*, *OR* и *NOT*), но този път за шестте члена S_i, което е доста сложно. По тази причина е предпочетено създаденият модул да изчислява произведенията S_i ($i = 1 \div 6$) и да определя сумата им S. Ако сумата S е нечетно число (1, 3 или 5), като стойност на

ПРИМЕР ЗА ОПРЕДЕЛЯНЕ НА СЪЕДИНЕНИЯТА С ОБРАТНАТА ВРЪЗКА НА ЧЕТИРИРАЗРЯДЕН ЛИНЕЕН ПРЕМЕСТВАЩ РЕГИСТЪР



Ключов поток, определен чрез сумиране по модул 2 на прихванатите от криптоаналитика открит текст и неговия шифриран еквивалент

$$X = \begin{Vmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{Vmatrix} \qquad X^{-1} = \begin{Vmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{Vmatrix}$$

$A_{11} = \begin{Vmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{Vmatrix} = 0$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	1	1	1	1	0	4

$A_{12} = \begin{Vmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{Vmatrix} = 0$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	1	0	1	0	0	2

$A_{13} = \begin{Vmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{Vmatrix} = 1$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	0	0	1	0	0	1

$A_{14} = \begin{Vmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{Vmatrix} = 1$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	0	0	1	0	0	1

$A_{41} = \begin{Vmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{Vmatrix} = 1$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	0	0	1	0	0	1

$A_{42} = \begin{Vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{Vmatrix} = 0$

S_1	S_2	S_3	S_4	S_5	S_6	S
1	0	0	0	0	1	2

$A_{43} = \begin{Vmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{Vmatrix} = 1$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	0	0	0	0	1	1

$A_{44} = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{Vmatrix} = 1$

S_1	S_2	S_3	S_4	S_5	S_6	S
0	0	0	0	0	1	1

Определяне на съединенията с обратната връзка на регистъра: $g = X^{-1}x$

$$\begin{Vmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{Vmatrix} = \begin{Vmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{Vmatrix} \cdot \begin{Vmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{Vmatrix}$$

$$\begin{Vmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 1 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

R_1	R_2	R_3	R_4	R
0	0	1	0	1
0	1	1	0	2
1	1	1	0	3
1	0	1	0	2

$\Rightarrow \quad g_1 = 1 \qquad g_2 = 0 \qquad g_3 = 1 \qquad g_4 = 0$

Фиг.3. Пример за определяне на съединенията с обратната връзка на регистъра

адюнгираното количество се извежда „1”, а в случай на четно число (0, 2, 4 или 6) се извежда съответно „0”. На фиг.3 са „скрити” изчисленията на част от адюнгираните количества, поради еднотипност на визуализираните резултати. След определяне на обратната матрица $\mathbf{X}^{-1}$, съгласно израза (5), се пристъпва към изчисляването на вектора-стълб $\mathbf{g}$, използвайки зависимостта:

(6) $\mathbf{g} = \mathbf{X}^{-1}\mathbf{x}$.

Векторът-стълб $\mathbf{g}$ съдържа стойностите на g_i, дефиниращи наличието на съединение на i-тия елемент на регистъра с обратната връзка при $g_i = 1$ или отсъствието на такова съединение при $g_i = 0$.

Зависимост (6) може да се запише за случая на четириразряден регистър във вида:

(7) $$\begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} = \begin{bmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{bmatrix} . \begin{bmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} .$$

Следователно, $g_i = \sum_{j=1}^{4} A_{ji}.x_{j+4}$ за $i = 1 \div 4$, като сумирането е по модул 2. И тук всяко едно от произведенията $A_{ji}x_{j+4}$ е означено с R_j ($j = 1 \div 4$), а изчисляването на $R_1 \oplus R_2 \oplus R_3 \oplus R_4$ се свежда отново до определяне на броя на единиците R (четен или нечетен) при обикновеното събиране на R_j ($j = 1 \div 4$). В случай, че сумата $R = R_1 + R_2 + R_3 + R_4$ е четно число (0, 2 или 4) съответното g_i има стойност „0”, а в случай на нечетно число (1 или 3) – $g_i = 1$.

ЗАКЛЮЧЕНИЕ

В статията е описан разработеният чрез MS Excel програмен модул, който позволява да се определи състоянието на четириразряден линеен преместващ регистър, използван като генератор на псевдослучайна ключова последователност в системи с поточно шифриране, в няколко последователни такта от абстрактното време, при зададено от потребителя начално състояние на регистъра (в първия такт). С помощта на създадения програмен модул може да се определи и шифрирания текст с използване на генерирания ключов поток, при произволно зададен от потребителя открит текст, както и да се открият съединенията в обратната връзка на регистъра, ако са известни само по 8 бита от откритият текст и от шифрирания му еквивалент. По този начин се демонстрира уязвимостта на линейните преместващи регистри с обратна връзка към атака на известния открит текст. Избран е продуктът MS Excel, тъй като е най-достъпен, а и позволява много удобно таблично представяне на решаваната задача. Разбира се, при необходимост да се изследват тези съединения за регистър с повече разряди, е по-удачно да се използва програмният продукт MATLAB, предназначен специално за работа с матрици. Разработеният модул може да се използва от студенти, изучаващи дисциплините „Комуникационни системи” (по-специално криптосистемите) и „Анализ и синтез на логически схеми”.

ЛИТЕРАТУРА

[1] Антонов, П., С. Малчев. Криптография в компютърните комуникации. Варна, 2000.

[2] Гелерт, В., Х. Кестнер, З. Нойбер. Математически енциклопедичен речник. София, Наука и изкуство, 1983.

[3] Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. Москва, Вильямс, 2003.