Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Лабораторна робота

із Криптографії №4

Побудова регістрів зсуву з лінійним зворотним зв’язком та дослідження їх властивостей

Виконали:

Нестеров Назар ФБ – 74

Христиченко Дмитро ФБ-72

Перевірено_____

Київ 2019

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4
Побудова регістрів зсуву з лінійним зворотним зв'язком та дослідження їх властивостей

Мета роботи
Ознайомлення з принципами побудови регістрів зсуву з лінійним зворотним зв'язком; практичне освоєння їх програмної реалізації; дослідження властивостей лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.

Порядок виконання роботи
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму. 1. Вибрати свій варіант завдання згідно зі списком. Варіанти завдань містяться у файлі Crypto_CP4 LFSR_Var.
2. За даними характеристичними многочленами $p_1(x)$, $p_2(x)$ скласти лінійні рекурентні співвідношення для ЛРЗ, що задаються цими характеристичними многочленами.
3. Написати програми роботи кожного з ЛРЗ L_1 , L_2 .
4. За допомогою цих програм згенерувати імпульсні функції для кожного з ЛРЗ і підрахувати їх періоди.
5. За отриманими результатами зробити висновки щодо влавствостей кожного з характеристичних многочленів $p_1(x)$, $p_2(x)$: многочлен примітивний над F_2 ; не примітивний, але може бути незвідним; звідний.
6. Для кожної з двох імпульсних функцій обчислити розподіл k-грам на періоді, $k \le n_i$, де n_i - степінь полінома $f_i(x)$, $i=1,2$ а також значення функції автокореляції $A(d)$ для $0 \le d \le 10$. За результатами зробити висновки.

Варіант 18:

$P_1(X)= X_{23}+X_{20}+X_{19}+X_{18}+X_{17}+X_{13}+X_{12}+X_{11}+X_7+X+1$
$P_2(X)= X_{22}+X_{20}+X_{19}+X_{17}+X_{16}+X_{15}+X_{12}+X_9+X_7+X_5+X_4+X_3+X_2+X+1$

Довжини періодів:
L_1: $2^{23}-1 = 8\ 388\ 607$ => $P_1(x)$ – примітивний поліном поля F_2
L_2: 35 805 => $P_2(x)$ – не примітивний та звідний

Розподіл К-грам полінома Р1:

2 – грами		3 - грами		4 - грами		5 - грами	
00	0.249949	000	0.124989	0000	0.0624681	00000	0.031235
01	0.249968	001	0.124960	0001	0.062521	00001	0.0312331
10	0.249968	010	0.124937	0010	0.0624426	00010	0.0312233
11	0.250114	011	0.125031	0011	0.0625178	00011	0.0312977
		100	0.124960	0100	0.0624685	00100	0.0312139
		101	0.125007	0101	0.0624686	00101	0.0312287
		110	0.125031	0110	0.062493	00110	0.031232
		111	0.125083	0111	0.062538	00111	0.0312858
				1000	0.0625209	01000	0.0312635
				1001	0.0624394	01001	0.031205
				1010	0.0624945	01010	0.0312346
				1011	0.0625133	01011	0.031234
				1100	0.0624918	01100	0.03124
				1101	0.0625392	01101	0.031253
				1110	0.062538	01110	0.0312654
				1111	0.062545	01111	0.0312726
						10000	0.031233
						10001	0.0312879
						10010	0.0312193
						10011	0.0312201
						10100	0.0312546
						10101	0.0312399
						10110	0.031261
						10111	0.0312522
						11000	0.0312574
						11001	0.0312344
						11010	0.0312599
						11011	0.0312793
						11100	0.0312518
						11101	0.0312862
						11110	0.0312726
						11111	0.0312724

Розподіл К-грам полінома Р2:

2 – грами		3 - грами		4 - грами		5 - грами	
00	0.249156	000	0.1258165	0000	0.0638725	00000	0.0322595
01	0.249462	001	0.123339	0001	0.0619435	00001	0.031613
10	0.249462	010	0.1241155	0010	0.061949	00010	0.0314185
11	0.251918	011	0.125347	0011	0.06139	00011	0.030525
		100	0.123339	0100	0.0607675	00100	0.02994
		101	0.1261235	0101	0.063348	00101	0.032009
		110	0.125347	0110	0.0625615	00110	0.03064
		111	0.1265715	0111	0.0627855	00111	0.03075
				1000	0.0619435	01000	0.030522
				1001	0.0613955	01001	0.0302455
				1010	0.0621665	01010	0.03162
				1011	0.063957	01011	0.031728
				1100	0.0625715	01100	0.0315405
				1101	0.0627755	01101	0.031021
				1110	0.0627855	01110	0.031225
				1111	0.063786	01111	0.0315605
						10000	0.0316125
						10001	0.0303305
						10010	0.0305305
						10011	0.030865
						10100	0.0308275
						10101	0.031339
						10110	0.0319215
						10111	0.0320355
						11000	0.0314215
						11001	0.03115
						11010	0.0305465
						11011	0.032229
						11100	0.031031
						11101	0.0317545
						11110	0.0315605
						11111	0.0322255

Значення автокореляції:

L_1:	L_2:
d = 1 : 4194304 d = 2 : 4194304 d = 3 : 4194304 d = 4 : 4194304 d = 5 : 4194304 d = 6 : 4194304 d = 7 : 4194304 d = 8 : 4194304 d = 9 : 4194304 d = 10 : 4194304	d = 1 : 17864 d = 2 : 17808 d = 3 : 17864 d = 4 : 17864 d = 5 : 17864 d = 6 : 17864 d = 7 : 17808 d = 8 : 17976 d = 9 : 17976 d = 10 : 17976

Висновок:

В даному комп'ютерному практикумі було набуто навичок роботи з лінійними регістрами зсуву, а саме: їх програмна реалізація, дослідження властивостей характеристичного полінома регістра. Окрім цього було досліджено властивості лінійних рекурентних послідовностей

Програмний код:

```
a = [1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0]
b = [1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0]
def linear_relation(poly, n, f, c, power): # power of the first polynom is 23 and of the other one is 22
s = [0] * f
for i in range(0, n): # n is 22 for the sirst polynom or 20 for the second one
s[i] = 0
s[c] = 1 #c is 23 for the first one and 21 for the second polynom
j = c
for i in range(0, f - power):
s[i + power] = (sum(poly[j] * s[i + j] for j in range(0, power - 1))) % 2
# print(s)
for k in range(power, f - power):
if any(s[k + i] for i in range(0, n)) == 0 and s[k + c] == 1:
        a = k
        break
print("The period of your polynom with the power " + str(power) + " equals to: " + str(a))
for d in range(1, 11):
autocorellation = 0
for i in range(0, a):
        autocorellation += (s[i] + s[(i + d) % a]) % 2
print("Autocorellation data for your polynom with the power " + str(power) + " and d being equal to " + str(d) +" is: " +
str(autocorellation))
text = ""
for i in s:
text += str(i)
dictionary = {}
dictionary_second = {}
dictionary_third = {}
dictionary_fourth = {}
array = "0011"
for i in array:
for j in array:
        dictionary[i + j] = 0
for i in range(f - 1):
dictionary[text[i] + text[i + 1]] += 1
for frequency in dictionary:
dictionary[frequency] /= f
print("2-grams sequences are here: " + str(dictionary))
array_second = "000111"
for i in array_second:
for j in array_second:
```

```
        for p in array_second:
                dictionary_second[i + j + p] = 0
for i in range(f - 2):
dictionary_second[text[i] + text[i + 1] + text[i + 2]] += 1
for frequency in dictionary_second:
dictionary_second[frequency] /= f
print("3-grams sequences are here: " + str(dictionary_second))
array_third = "00001111"
for i in array_third:
for j in array_third:
        for p in array_third:
                for z in array_third:
                        dictionary_third[i + j + p + z] = 0
for i in range(f - 3):
dictionary_third[text[i] + text[i + 1] + text[i + 2] + text[i + 3]] += 1
for frequency in dictionary_third:
dictionary_third[frequency] /= f
print("4-grams sequences are here: " + str(dictionary_third))
array_fourth = "0000011111"
for i in array_fourth:
for j in array_fourth:
        for p in array_fourth:
                for z in array_fourth:
                        for q in array_fourth:
                                dictionary_fourth[i + j + p + z + q] = 0
for i in range(f - 4):
dictionary_fourth[text[i] + text[i + 1] + text[i + 2] + text[i + 3] + text[i + 4]] += 1
for frequency in dictionary_fourth:
dictionary_fourth[frequency] /= f
print("5-grams sequences are here: " + str(dictionary_fourth))
return "--------------------------------------------------------------------------------"


print(linear_relation(a, 22, 10000000, 22, 23))
print(linear_relation(b, 21, 2000000, 21, 22))
```