International Journal of Mathematics and
Computer Science, **17**(2022), no. 4, 1563–1567

The analysis and implementation of the symmetric key cryptographic algorithm based on the algebraic Paley graphs

Zhour Oumazouz, Driss Karim

Department of Mathematics and Applications
Faculty of Science and Technology
Hassan II University
Mohammedia, Morocco

email: oumazouzzhour@gmail.com, dkariim@gmail.com

(Received May 12, 2022, Accepted June 14, 2022)

Abstract

Using pari gp, we analyze and give an implementation of the symmetric key cryptographic algorithm using the Paley graphs and binary codes.

Introduction

Generally, cryptographic schemes are based on mathematical problems like factorization problems, discrete logarithms, elliptic curves, quadratic residues. Some graph problems are exploited in coding theory due to their difficulty and computing complexity. Coding using algebraic graphs is an important topic. In [1], the authors introduced a new symmetric key cryptographic algorithm using Paley graphs and ASCII values. In [2], the author introduced a Novel public-key cryptosystem based on the problem of performing a sequence of local complementations on the Paley graphs. The cryptanalysis of these two cryptosystems is very difficult. The first difficulty is related to the anonymous behavior of quadratic residues and the second is related to the

Key words and phrases: Quadratic residues, Paley graphs, Encryption algorithm, Decryption algorithm.
AMS (MOS) Subject Classifications: 05-XX, 11T71.
Oumazouz Zhour is the corresponding author.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

problem of identification of the graph induced by a sequence of local complementations of the Paley graph of order p. Using pari gp, we will give an implementation of the secret key cryptosystem of the algorithm proposed in [1]. This implementation is used to determine the binary codes transformed by this encryption algorithm using secret keys varying between 37 and 500. The analysis of the set of possible messages shows that this proposed cryptosystem is powerful.

1 Analysis and implementation of the symmetric key cryptographic algorithm using Paley graphs

In this section, we will describe the symmetric key cryptographic algorithm which was introduced in [1] and discuss its robustness.
A graph is a pair $G = (V, A)$ where V is a set of vertices, and $A \subset V \times V$ is a set of arcs or edges. A graph with n vertices can be represented by an $n \times n$ adjacency matrix $(g_{ij})_{0 \leq i,j \leq n-1}$, where $g_{ij} = 0$ if $(j, i) \in A$, and $g_{ij} = 1$ otherwise. The neighborhood of $v \in V$, is a set of all vertices that have a shared edge with v.
To encrypt our message, we need to use the neighborhood set of a vertex v defined as $N_V^+(v) = \{x \in V/(v, x) \in A\}$.
The symmetric key cryptographic algorithm using Paley graphs is described in [1] in the following way:

Step 1: Generate the ASCII value of each letter C_i in the message $C = C_0C_1...C_{s-1}$.
Step 2: Generate the corresponding binary value of it, then Let $B_m = b_0b_1...b_{7s-1}$ be the binary message corresponding to C with respecting of the same order of C_i in C.
Step 3: Let $G_p = (V, A)$ be a choosen Plaey graph of order p.
Step 4: The encrypted binary message of B_m is $B'_m = b'_0b'_1...b'_{7s-1}$ where $b'_i = b_i + \sum_{u \in N_V^+(i \bmod p), u \leq 7s-1} b_u + \sum_{u \in N_V^+(i), u > 7s-1} u$ for $0 \leq i \leq 7s - 1$.
Step 5: Determine the ASCII code which corresponds to the binary message b'_i, then the character corresponding to this ASCII code. The encrypted message is $C' = C'_0C'_1...C'_{s-1}$.

We describe the decryption scheme introduced in [1] as follows:

Step 1: For each $0 \leq i \leq 7s-1$, generate the ASCII value of the letter C'_i in the received message $C' = C'_0C'_1...C'_{s-1}$.
Step 2: Generate the corresponding binary value of it, then Let $B'_m = b'_0b'_1...b'_{7s-1}$ be the binary message corresponding to C' with respecting of the same order of C'_i in C'.
Step 3: Let $G_p = (V, A)$ be the Paley graph of order p(p is the secret key)
Step 4: For $0 \leq i \leq 7s-1$, use the symetric key to solve over the field $\mathbb{Z}_2$ the linear algebraic equations $b'_i = b_i + \sum_{u \in N_V^+(i \bmod p), u \leq 7s-1} b_u + \sum_{u \in N_V^+(i), u > 7s-1} u$, then take the binary decripted message $B_m = b_0b_1...b_{7s-1}$.
Step 5: Determine the ASCII code which corresponds to the binary message b_i, then the character corresponding to this ASCII code.

Using pari gp, the following program gives all positions i of b_i where we have a change of the message bit corresponding to the message bit of "Hello"

```
*************Encryption of the message: Hello******************
*************p: is the secret key*******************************
*************B: The binary message corresponding to Hello*******
*************G: corresponds to Paley graph of order p***********
EncryptionWithSecretKey(p)=
{s=35;B=[1,0,0,1,0,0,0,1,1,0,0,1,0,1,1,1,0,1,1,0,0,1,1,0,1,1,0,0,1,1,0,1,1,1,1];
G=matrix(p,p);
B2=vector(s);
if(p>s,
for(i=1,s,B1=B;
for(j=1,s,
if(j!=i && (i-j)^((p-1)/2)%p==1,G[i,j]=1;
if(G[i,j]==1,B1[i]=B1[i]+B[j];)));
for(j=s+1,p,
if((i-j)^((p-1)/2)%p==1,G[i,j]=1;
if(G[i,j]==1,B2[i]=B2[i]+j;)));
B1[i]=(B1[i]+B2[i])%2;
if(B1[i]!=B[i],
printf(" %d,",i);)))
}
EncryptionWithSecretKey(p);
```

To analyze this cryptosystem, we will try to give the number of repetition E_i of each bit b_i transformed after each encryption step. The encryption is done by choosing a secret key p varying between $p = 37$ and $p = 500$. After running the program described above, We obtain the following results:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

E_i	45	27	29	38	40	34	41	38	41	46	39	39	33	45	45	33	40	43

i	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
E_i	34	39	44	44	40	35	42	44	39	46	43	45	34	39	37	23	40

To illustrate the difficulty of the cryptanalysis of this cryptosystem, we will redo the same study for another clear message. Take, for example, the message "looks". The results obtained are given in the following table:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
E_i	47	24	30	42	43	62	40	45	45	35	33	41	42	46	41	46	45	38

i	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
E_i	36	49	45	38	49	40	37	29	35	38	36	39	41	40	37	14	41

2 Conclusion

The difficulty produced during the cryptanalysis part of this cryptosystem is due to the following problems:

- The behavior of quadratic residues is anonymous.
- The encryption of a bit of message is done according to the other plain message bits.

We have tried to show that this cryptanalysis is difficult. This allowed us to say that brute force attack remains, for the moment, the only way to the decryption phase.

We conjecture that the cryptanalysis part will depend on probabilistic methods that need study in order to give information on the power part of the proposed encryption technique.

References

[1] Zhour Oumazouz, Driss Karim, A New Symmetric Key Cryptographic Algorithm using Paley Graphs and ASCII Values, E3S Web of Conferences, **297,** EDP Sciences, 2021.

[2] Zhour Oumazouz, Novel public-key cryptosystem based on the problem of performing sequence of local complementations on the Paley graphs, International Journal of Mathematics and Computer Science, **17,** no. 3, (2022), 1451–1461.