International Journal of Mathematics and
Computer Science, **17**(2022), no. 3, 1451–1461

Novel public-key cryptosystem based on the problem of performing sequence of local complementations on the Paley graphs

Oumazouz Zhour

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

email: oumazouzzhour@gmail.com

(Received March 8, 2022, Accepted May 9, 2022)

Abstract

The security and robustness of the existing cryptographic models are ensured, thanks to algebraic or arithmetic problems such as the factorization problem, the discrete logarithm, and the quadratic residues. In this article, we consider the problem of performing sequence of local complementations on the Paley graphs. We then propose an effective novel public-key cryptosystem based on this problem.

1 Introduction

Cryptography deals with the study and the practice of how to encode and hide sensitive information from say, enemies, hackers. The security and robustness of the existing data encryption algorithms are ensured, thanks to algebraic or arithmetic problems such as the factorization problem, the discrete logarithm. Generally, data encryption can be done by choosing a key which can be a number, word, graph, etc.
Using some graph problems to introduce a new contribution in coding theory and cryptography is an interesting topic. To locally complement a graph

Key words and phrases: Quadratic residues, Paley graphs, Encryption algorithm, Decryption algorithm, Sequence of Local complementations.
AMS (MOS) Subject Classifications: 11T71.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

$G = (V, A)$ at its vertex v is to replace the subgraph induced by G on the set $N_V(v)$ of the neighborhood of v by the complementary subgraph. The resulting graph is denoted by $G*V$ and the operation used here is called local complementation and which was first introduced by Bouchet [1]. Danielsen and Parker [5] showed that by representing a binary linear code as a bipartite graph, the edge local complementation (ELC) on this graph provides a simple way of jumping between equivalent codes, and that the orbit of a bipartite graph under ELC corresponds to the complete equivalence class of the corresponding code. Javelle [3] proved that the family of Paley graphs is the constructive family whose minimum degree by local complementation is the highest until now. This allows us to say that these graphs can be used as a good support for sharing a quantum secret, thus realizing qQSS * protocol of quantum sharing secret. Bouchet [1] proposed an efficient algorithm to recognize locally equivalent graphs for simple undirected graphs. Fon-Der-Flaass [2] generalized some results in [1] to the directed simple graphs.
We pose the following questions:
What is the minimum degree up to local complementation of the Paley graph of order p? How can we identify in function of G the graph induced by a sequence of local complementations of Paley graphs G at its vertices? The answer to the first question is unknown for the moment [7]. Javelle, Mhalla, and Perdrix [7] showed that the local minimum degree of the Paley graph of order p is greater than $\sqrt{p} - 3/2$. As far as we know, this degree is the highest known bound on an explicit family of graphs.
The second question is very difficult because the study of the problem is related to the characterization of the type of the induced graph after such operation of local complementation. After introducing a new symmetric encryption algorithm using Paley graphs [6], we show that performing sequence of local complementations of Paley graphs at its vertices is a difficult problem. By exploiting this problem, we introduce a new effective asymmetric key cryptographic algorithm. To achieve this goal, we propose a solution of this problem to one Paley graph family under some particular conditions. As for the second section, we propose a new effective algorithm of encryption and decryption based on our proposed problem. We then give reasons why this algorithm is powerful.
In this work, we have exploited the problem of realizing sequence of local complementations of Paley graphs at its vertices to introduce a new asymmetric encryption and decryption algorithm. We conjecture that the study of this problem is equivalent to the behavior study of quadratic residues. Hence, no information is given to the cryptanalysis part. Therefore, we present this

cryptographic model in order to discuss its power and compare it to the already existing cryptographic systems.

2 The operation of local complementation of Paley graphs

Let $G = (V_G, A_G)$ be a directed graph without loops and let v be a vertex of G.
We use the following notations:
$N^+_{V_G}(v) = \{x \in V_G/(v,x) \in A_G\}$, $N^-_{V_G}(v) = \{x \in V_G/(x,v) \in A_G\}$.
$X_1 + X_2 = \{X_1 \cup X_2\} - \{X_1 \cap X_2\}$; the symmetric difference of X_1 and X_2.
$N_{V_G}(v) = N^+_{V_G}(v) + N^-_{V_G}(v)$ is a neighborhood of v.
We identify the graph G with its adjacency matrix (g_{ij}) over the field $\mathbb{Z}_2$ defined as follows:

$$g_{ij} = \begin{cases} 1 & \text{if } (j,i) \in A_G \\ 0 & \text{if } (i,j) \in A_G \end{cases}$$

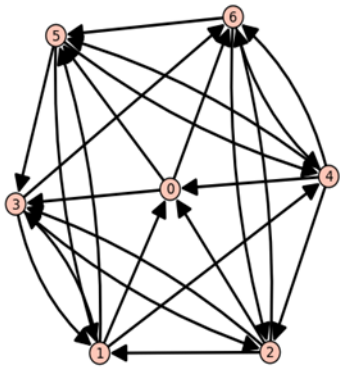
and we write $G = (g_{ij})$. A local complementation of G at a vertex v consists of replacing the subgraph induced by G on a neighborhood of v by the complementary graph. The resulting graph is denoted by $G * v$, and is defined in the following way:

Definition 2.1. *([4]) The local complementation of a graph $G = (g_{ij})$ at its vertex v is the graph $G * v = (g^{(1)}_{ij})$ with the adjacency matrix given by the following formula:*

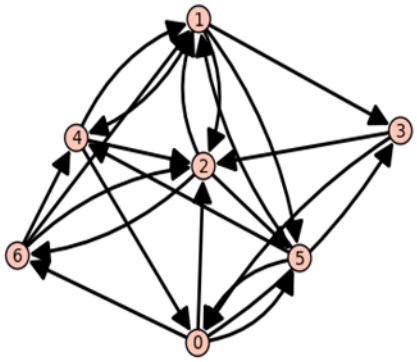
$$g^{(1)}_{ij} = \begin{cases} g_{ij} + g_{iv}g_{vj} & \text{if } i \neq j \\ 0 & \text{if } i = j \end{cases}$$

Property 2.2. *The operation of local complementation is an equivalence relation.*

Example 2.3. *Example of some graphs induced by the operation of local complementation of Paley Tournaments.*



The graph induced by the local complementation of T_7 at 0



The graph induced by the local complementation of T_7 at 0,1,2,3

The following proposition gives another characterization of $G * v$.

Proposition 2.4. *Let $G = (V_G, A_G)$ be the Paley graph of size p with the adjacency matrix (g_{ij}). The adjacency matrix $(g_{ij}^{(1)})$ of $G * v$ is given by the following formula:*

$$g_{ij}^{(1)} = \begin{cases} g_{ij} + 1 & \text{if } i \in N_{V_G}^+(v), j \in N_{V_G}^-(v), i \neq j \\ g_{ij} & \text{otherwise} \end{cases}$$

Proof. This proposition follows from the fact that the only case in which $g_{iv}g_{vj} = 1$ is when $i \in N_{V_G}^+(v)$ and $j \in N_{V_G}^-(v)$. □

Remark 2.5. *If G is an undirected Paley graph, then $N_{V_G}^+(v) = N_{V_G}^-(v) = N_{V_G}(v)$*

As we know that the local complementation is an operation which acts on the neighborhood set of such vertex v, we can ask for the relationship that exists between the following sets $N_G(u)$ and $N_{G*v}(u)$, where u is a vertex of V_G.
The following property answers this question.

Property 2.6. *Let $G = (V_G, A_G)$ be the Paley graphs of size p and let $G * v$ be the graph induced by the local complementation of G at its vertex v. If $(u, v) \in A_G$, Then*

$$N_{V_{G*v}}^-(u) = N_{V_G}^-(u) \ , \ N_{V_{G*v}}^+(u) = N_{V_G}^+(u) + N_{V_G}^+(v)$$

.

Proof. 1) Let (g_{ij}) be the adjacency matrix of G and let $(g_{ij}^{(1)})$ be that of $G * v$.

$$\begin{aligned} i \in N^-_{V_{G*v}}(u) &\iff (i,u) \in A_{G*v} \\ &\iff g_{ui}^{(1)} = 1 \\ &\iff g_{ui} + g_{uv}g_{vi} = 1 \\ &\iff g_{ui} = 1 \ since (u,v) \in A_G \\ &\iff (i,u) \in A_G \\ &\iff i \in N^-_{V_G}(u) \end{aligned}$$

2) Assume that $(u,v) \in A_G$. By applying the previous proposition, we have:

$$\begin{aligned} i \in N^+_{V_{G*v}}(u) &\iff (u,i) \in A_{G*v} \\ &\iff g_{iu}^{(1)} = 1 \\ &\iff \begin{cases} g_{iu} + 1 = 1 & \text{if } i \in N^+_{V_G}(v) \\ g_{iu} = 1 & \text{otherwise} \end{cases} \\ &\iff \begin{cases} g_{iu} = 0 & \text{if } i \in N^+_{V_G}(v) \\ g_{iu} = 1 & \text{otherwise} \end{cases} \\ &\iff i \in N^+_{V_G}(u) + N^+_{V_G}(v) \end{aligned}$$

□

Characterizing the graph $G * u_1 * .. * u_n$ induced by sequence of local complementations of a Paley graph G at its vertices $u_1, .., u_n$ is a difficult problem. Since the operation of local complementation is an equivalence relation, identifying the graph $G * u_1 * .. * u_n$ as a function of G amounts to studying this problem for a number of families of graph. In this work, we will try to solve this problem for a family of graphs which satisfies the following condition: $u_i \in \cap_{k=2}^{i-1} N^-_{V_G}(u_k) - \{N^-_{V_G}(u_1)\}$, where $3 \leq i \leq n$ and $u_2 \in N^-_{V_G}(u_1)$.

Proposition 2.7. *Let $G = (V_G, A_G)$ be the Paley graph of size p with adjacency matrix (g_{ij}) and let n be an integer such that $n > 3$.*
For all $3 \leq i \leq n$, $u_i \in \cap_{k=2}^{i-1} N^-_{V_G}(u_k) - \{N^-_{V_G}(u_1)\}$ and $u_2 \in N^-_{V_G}(u_1)$, the adjacency matrix $(g_{ij}^{(n)})$ of the graph induced by sequence of local complementations of G at its vertices u_1,..., u_n is given by the following formula:
$g_{ij}^{(n)} = g_{ij} + g_{iu_1}g_{u_nj} + g_{iu_2}(g_{u_1j} + g_{u_nj}) + g_{iu_3}(g_{u_1j} + g_{u_2j} + g_{u_3j}) + \sum_{k>3}^{n} g_{iu_k}(g_{u_kj} + g_{u_{k-1}j})$.

Proof. For $n = 4$ we have:

$$\begin{aligned}
g_{ij}^{(4)} &= g_{ij}^{(3)} + g_{iu_4}^{(3)} g_{u_4j}^{(3)} \\
&= g_{ij}^{(3)} + [g_{iu_4} + g_{iu_1} g_{u_3u_4} + g_{iu_2}(g_{u_1u_4} + g_{u_3u_4}) \\
&+ g_{iu_3}(g_{u_1u_4} + g_{u_2u_4} + g_{u_3u_4})][g_{u_4j} + g_{u_4u_1} g_{u_3j} \\
&+ g_{u_4u_2}(g_{u_1j} + g_{u_3j}) + g_{u_4u_3}(g_{u_1j} + g_{u_2j} + g_{u_3j})] \\
&= g_{ij}^{(3)} + (g_{iu_1} + g_{iu_2} + g_{u_4})(g_{u_4j} + g_{u_3j}) \\
&= g_{ij} + g_{iu_1} g_{u_4j} + g_{iu_2}(g_{u_1j} + g_{u_4j}) + g_{iu_3}(g_{u_1j} + g_{u_2j} + g_{u_3j}).
\end{aligned}$$

If we suppose that the formula (1) is true for $n \in \mathbb{N}$, then

$$\begin{aligned}
g_{ij}^{(n+1)} &= g_{ij}^{(n)} + g_{iu_{n+1}}^{(n)} g_{u_{n+1}j}^{(n)} \\
&= g_{ij}^{(n)} + [g_{iu_{n+1}} + g_{iu_1} g_{u_n u_{n+1}} \\
&+ g_{iu_2}(g_{u_1u_{n+1}} + g_{u_n u_{n+1}}) + g_{iu_3}(g_{u_1u_{n+1}} + g_{u_2u_{n+1}} \\
&+ g_{u_3u_{n+1}}) + \sum_{k>3}^{n+1} g_{iu_k}(g_{u_k u_{n+1}} + g_{u_{k-1}u_{n+1}})] \\
&[g_{u_{n+1}j} + g_{u_{n+1}u_1} g_{u_nj} + g_{u_{n+1}u_2}(g_{u_1j} + g_{u_nj}) + \\
&g_{u_{n+1}u_3}(g_{u_1j} + g_{u_2j} + g_{u_3j}) + \sum_{k>3}^{n+1} g_{u_{n+1}u_k}(g_{u_kj} + g_{u_{k-1}j})] \\
&= g_{ij}^{(n)} + (g_{iu_{n+1}} + g_{iu_1} + g_{u_2})(g_{u_{n+1}j} + g_{u_nj}) \\
&= g_{ij} + g_{iu_1} g_{u_{n+1}j} + g_{iu_2}(g_{u_1j} + g_{u_{n+1}j}) + g_{iu_3}(g_{u_1j} \\
&+ g_{u_2j} + g_{u_3j}) + \sum_{k>3}^{n+1} g_{iu_k}(g_{u_kj} + g_{u_{k-1}j}).
\end{aligned}$$

Hence, if $u_i \in \cup_{k=2}^{i-1} N_{V_G}^-(u_k) - \{N_{V_G}^-(u_1)\}$ for $2 \leq i \leq n$ and $n > 3$, then: $g_{ij}^{(n)} = g_{ij} + g_{iu_1} g_{u_nj} + g_{iu_2}(g_{u_1j} + g_{u_nj}) + g_{iu_3}(g_{u_1j} + g_{u_2j} + g_{u_3j}) + \sum_{k>3}^{n} g_{iu_k}(g_{u_kj} + g_{u_{k-1}j})$. □

The problem proposed in this work is to identify the graph induced by a sequence of local complementations of a Paley graph. This problem is not obvious because it is based on the following problem:
each time we go to the i-th complementation $G * u_1 * u_2 ... u_i$, we need to know the structure of the graph induced by the $(i-1)$-th complementation. Consequently, studying this problem requires the cryptanalysis part of the encryption algorithm that we will try to propose in the next section.

3 The new asymmetric key cryptographic algorithm using binary codes and sequence of local complementations of Paley Graphs

Cryptography is used to achieve a few goals like Confidentiality, Data integrity, Authentication of sent data, among others. Now, in order to achieve these goals, various cryptographic algorithms like DES, AES, RSA are developed by various people to ensure security of an important amount of data.
We design and implement a new effective algorithms of encryption and decryption of information data using an interaction between algebraic and graph field.
The new encryption algorithm is based on performing a sequence of local complementations of such Paley graph G constructed from quadratic residues, By making some operations that we will describe later, we will encode our sensitive information.
Since the operation of local complementation is an equivalence relation, the new decryption algorithm is based on performing a sequence of local complementations and solving some systems of linear equations over $\mathbb{Z}_2$.

3.1 Encryption algorithm

In [6], we have proposed a symmetric key cryptographic algorithm using Paley graphs and the vertex neighborhood notion. From this encryption scheme, we propose an asymmetric key cryptographic algorithm that will bear the name of the public-key cryptosystem of ZO based on the problem of performing a sequence of local complementations of Paley graphs at its vertices. The new proposed encryption scheme is described as follows:
Step 1: Generate the binary value of each letter C_i in the message $C = C_0C_1...C_{s-1}$, and let $B_m = b_0b_1...b_{7s-1}$ be the binary message corresponding to C respecting of the same order of C_i in C.
Step 2: Let $G = (V_G, A_G)$ be the graph induced by sequence of local complementations of Paley graph of order p at its vertices $u_1, u_2, .., u_n$, where u_i are secret and p is the public key.
Step 3: The encrypted binary message of B_m is $B'_m = b'_0b'_1...b'_{7s-1}$ where $b'_i = b_i + \sum_{u\in N^+_{V_G}(i \ mod \ p), u\leq 7s-1} b_u + \sum_{u\in N^+_{V_G}(i), u>7s-1} u$ for $0 \leq i \leq 7s-1$.
Step 4: Determine the character C'_0 which corresponds to the binary code of b'_i. The encrypted message to send is $C' = C'_0C'_1...C'_{s-1}$.

Example 3.1. *Let* $C =$

C_0	C_1	C_2	C_3	C_4	C_5
P	u	t	”	t	”

be the plain text to encrypt.

The binary message B_m *corresponding to* C *is*

$$B_m = 101000010101010101010010001001000110100010$$

Let P *be the Paley graph of order* 13. *We identify the graph* P *by its adjacency matrix* M_P.

$$M_P = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Let $G = P * 1 * 2 * 6$ *be the graph induced by sequence of local complementations of* P *at its vertices* $1, 2$ *and* 6. *The adjacency matrix of* M_G *of* $G = P * 1 * 2 * 6$ *is:*

$$M_G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The encrypted binary message B'_m *is*
$B'_m = 000000001001100001011100010011000001101111$

The encrypted message to send is $C' =$

C'_0	C'_1	C'_2	C'_3	C'_4	C'_5
x	ACK	U	D	7	o

(ACK is the Acknowledge character).

3.2 Decryption algorithm

The decryption algorithm is based on solving over $\mathbb{Z}_2$ a system of linear equations. We describe the decryption scheme as follows:
Step 1: For each $0 \leq i \leq 7s-1$, generate the binary value of each letter C'_i in the received message $C' = C'_0C'_1...C'_{s-1}$. 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 2: Let $G = (V_G, A_G)$ be the graph induced by sequence of local complementations of Paley graph of order p(p is the public key) at its vertices $u_1, u_2, .., u_n$(u_i are secret)
Step 3: For $0 \leq i \leq 7s-1$, use the symmetric key to solve over the field $\mathbb{Z}_2$ the linear algebraic equations $b'_i = b_i + \sum_{u \in N^+_{V_G}(i \ mod \ p), u \leq 7s-1} b_u + \sum_{u \in N^+_{V_G}(i), u > 7s-1} u$, then take the binary decrypted message $B_m = b_0b_1...b_{7s-1}$.
Step 4: Determine the character which corresponds to the binary message b_i and then conclude the decrypted message.

Example 3.2. *Let* $C' =$

C'_0	C'_1	C'_2	C'_3	C'_4	C'_5
x	ACK	U	D	7	o

be the cipher text to decrypt.
Step 1: The binary message B'_m *corresponding to* C' *is*
$B'_m = 000000001001100001011100010011000001101111$
Steps 2 and 3: Let $G = (V_G, A_G)$ *be the graph induced by sequence of local complementations of Paley graph of secret order* 13 *at its secret vertices* $1, 2, 6$.
To decrypt the binary message B'_m*, we have to solve the linear algebraic equations* $b'_i = b_i + \sum_{u \in N^+(i \ mod \ p), u \leq 7s-1} b_u + \sum_{u \in N^+(i), u > 7s-1} u$ *over* $\mathbb{Z}_2$*, where* $0 \leq i \leq 7s-1$.
Indeed, let M_G *be the adjacency matrix of* G *and* $N = (n_i)_{0 \leq i \leq 7s-1}$ *the vector of* $\mathbb{Z}_2^{7s-1}$ *defined in the following way:*
$n_i = \sum_{u \in N^+(i), u > 7s-1} u$ *for* $0 \leq i \leq 7s-1$.

Let $B = \begin{pmatrix} b_0 \\ b_1 \\ . \\ . \\ b_{7s-1} \end{pmatrix}$ *and* $B' = \left(b'_0, b'_1, .., b'_{7s-1}\right)$. *Since* $p < 7s-1$, $N = O_{\mathbb{R}^{7s-1}}$.
After reducing the matrix $M_G + I$ *to a triangular form, we have to solve the following equations* $(M_G + I)\begin{pmatrix} b_0 \\ b_1 \\ . \\ . \\ b_{12} \end{pmatrix} = \begin{pmatrix} b'_0 \\ b'_1 \\ . \\ . \\ b'_{12} \end{pmatrix}$, $(M_G + I)\begin{pmatrix} b_{13} \\ b_{14} \\ . \\ . \\ b_{25} \end{pmatrix} = \begin{pmatrix} b'_{13} \\ b'_{14} \\ . \\ . \\ b'_{25} \end{pmatrix}$, $(M_G+I)\begin{pmatrix} b_{26} \\ b_{27} \\ . \\ . \\ b_{38} \end{pmatrix} = \begin{pmatrix} b'_{26} \\ b'_{27} \\ . \\ . \\ b'_{38} \end{pmatrix}$ *over* $\mathbb{Z}_2$ *and then conclude the values of* b_{39}, b_{40}, b_{41}

The decrypted binary message B_m *is*

$$B_m = 10100001010101010101001000100100011010001 0$$

3.3 Algorithm power

If p is a very large prime, then this algorithm is not obvious to break for the following reasons:

1. The encryption of a message bit is done in an abstract way as a function of the other bits of this message by using the quadratic residues of $\mathbb{Z}_p$ (p is secret) that have a difficult behavior to understand.

2. Generally, performing sequence of local complementations of Paley graphs is a complicated subject.

3. If the message is very large, then the decryption algorithm relies on solving over a large linear systems $\mathbb{Z}_2$.

4. As we know that the operation $(*)$ is an equivalence relation, to get the set of possible messages that match the cipher text, the hacker must solve $\sum_{k=1}^{p-1} C_{p-1}^k = 2^{p-1}$ linear systems over $\mathbb{Z}_2$.

Remark 3.3. *The only way for the moment for the crypt-analysis part is the brute force attack by performing the sequence of local complementations of a Paley graph of degree p.*

References

[1] A. Bouchet, *An efficient algorithm to recognize locally equivalent graphs,* Combinatorica, **11,** no. 4, (1991), 315–329.

[2] D. G. Fon-Der-Flaass, *Local complementations of simple and directed graphs.* In Discrete Analysis and Operations Research, A. D. Korshunov (ed.), Mathematics and its Applications, **355,** Springer, Dordrecht, 1996.

[3] J. Javelle, *Cryptographie quantique: protocoles et graphes. Algèbres quantiques,*[math.QA], Université de Grenoble, (2014).

[4] Joseph B. Dence, Thomas P. Dence, *Cubic and Quartic Residues Modulo A Prime,* Missouri J. Math. Sci., **7,** no. 1,(1995), 24–31.

[5] L. E. Danielsen, M. G. Parker, *Edge local complementation and equivalence of binary linear codes,* Designs, Codes and Cryptography, **49,** nos. 1-3, (2008), 161–170.

[6] Oumazouz Zhour, Driss Karim, *A new symmetric key cryptographic algorithm using Paley graphs and ASCII values,* Proceeding E3S Web of Conference 297, 01046, (2021), ICCSRE'2021, https://doi.org/10.1051/e3sconf/202129701046

[7] J. Javelle, M. Mhalla, S. Perdrix, On the Minimum Degree Up to Local Complementation: Bounds and Complexity. In Graph-Theoretic Concepts in Computer Science, M. C. Golumbic, M. Stern, A. Levy, G. Morgenstern (eds.), WG 2012, Lecture Notes in Computer Science, **7551,** Springer, Berlin, Heidelberg,