A New Symmetric Key Cryptographic Algorithm using Paley Graphs and ASCII Values.

Zhour Oumazouz$^{1,2,\ast}$ and Driss Karim$^{2,\ast\ast}$

$^1$Department of Mathematics, FST Mohammedia, Hassan II university, Casablanca, Morocco.

$^2$Department of Mathematics, FST Mohammedia, Hassan II University, Casablanca, Morocco.

Abstract. The main objective of the study conducted in this article is to introduce a new algorithm of encryption and decryption of a sensitive message after transforming it into a binary message. Our proposed encryption algorithm is based on the study of a particular graph constructed algebraically from the quadratic residues. We have exploited the Paley graph to introduce an abstract way of encryption of such message bit according to the other message bits by the intermediate study of the neighborhood of a graph vertex. The strong regularity of the Paley graphs and the unknown behavior of the quadratic residues will play a very important role in the cryptanalysis part which allows to say that the brute force attack remains for the moment the only way to obtain the set of possible messages.

1 Introduction

Any one who seriously studies algebraic graph theory, sooner or later, come across the Paley graphs and its applications in cryptography and coding theory due to its dependence on quadratic residues and its particular property of strong regularity.

As we know that the Paley graphs have a several applications in coding and cryptography such its application in quantum secret sharing domain [1] and its application in construction of codes from its incidence matrices and its line graphs [2], we decided to propose a new application of these graphs in the field of cryptography by introducing a new effective algorithm of encryption and decryption that we will describe later.

Nowadays, the use of internet are growing increasingly across the world and the network security becomes a prime concern of issue for the society in order to ensure confidentiality and authencity on the web.

For providing data security, cryptography which is the practice and the study of how to encode and hide information from enemies, hackers or the public employs many techniques to ensures that the sensitive information should be sent without any alterations and only the authorized person can be able to open and read the ciphertext. To ensure security, there are various cryptography techniques to employed both symmetric and asymmetric in order to create an encryption algorithm(one of the principal means to guarantee security) which performs various substitutions and transformations on the plaintext and transforms it into ciphertext. The sender encrypts message to the receiver.

The receiver decrypts the encrypted message by the exact decryption algorithm using a piece of secret information(the key that is the same or different from the key used by the sender) and recovers the original message. People who don’t have the right key would not be able to read the message even if they steal a copy of the decrypted version.

In this paper, we will introduce a new effective symmetric key algorithm using the Paley graph induced by the field $\mathbb{Z}_p$. To achieve this goal, we will first give some definitions from graph theory, then we introduce the notion of Paley graphs and Paley digraphs or tournaments. In the second section, we will describe the new algorithm of encryption and decryption of binary message using Paley graphs and illustrate this by an example.

2 The directed and undirected Paley graphs.

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 $(a_{ij})_{0\leq i,j < n}$, where $a_{ij} = 1$ if $(i,j) \in A$, and $a_{ij} = 0$ otherwise. The neighborhood of $v \in V$, is a set of all vertices that have a shared edge with $v$.

From the finite field $\mathbb{Z}_p$ of size $p$, we can construct the Paley graph which is strongly regular graph if $p = 1 \mod 4$, and the Paley tournament otherwise.

Throughout this paper, matrix computations will be over $\mathbb{Z}_2$, and $p$ be a prime number.

Definition 2.1 An undirected graph $G$ is a set of vertices that are connected together, where all the edges are bidirectional.
Definition 2.2 A directed graph $G$ is a graph having no symmetric pair of directed edges. In the case of complete directed graph, $G$ is called tournament.

Definition 2.3 The Paley graph $P_{p} = (V,A)$ where $p = 1 \mod 4$ and $n \in \mathbb{N}$, is an undirected graph of order $p$, has a vertex set $V = \mathbb{Z}_p$ (The finite field of size $p$), with two vertices $x$ and $y$ are adjacent if and only if $x - y$ is a non-zero square in $\mathbb{Z}_p$.

Definition 2.4 The Paley tournament $T_{p} = (V,A)$ where $p = 3 \mod 4$ and $n \in \mathbb{N}$, is a directed graph, has a vertex set $V = \mathbb{Z}_p$ (The finite field of size $p$), and such directed arc of $A$ goes from $x$ to $y$ (x $\neq$ y) if and only if $x - y$ is a non-zero square in $\mathbb{Z}_p$.

Example 2.5 The following graphs are constructed using SageMath.
Property 2.6 If $T_p = (V, A)$ is the Paley tournament of size $p$, then every vertex $u \in V$ has exactly $\frac{p-1}{2}$ directed arcs of tail $u$.

This follows from the fact that $-1$ is not square in $\mathbb{Z}_p$, and the number of quadratic residues in $\mathbb{Z}_p$ is exactly $\frac{p-1}{2}$.

3 The New Symmetric Key Cryptographic Algorithm using Paley Graphs.

Cryptography is used to achieve a few goals like Confidentiality, Data integrity, Authentication etc. of the send data. Now, in order to achieve these goals, various cryptographic algorithms like DES, AES, RSA etc. are developed by various people to ensure security of an important amount of data.

The aim of this work is to design and implement a new effective algorithms of encryption and decryption of big data using an interaction between algebraic and graph field. The new encryption algorithm is based on quadratic residues to construct the Paley graph $\mathbb{Z}_p$, then by making some operations that we will describe them in the rest of the work, we will encode our sensitive informations.

The new decryption algorithm is based on solving some systems of linear equations over $\mathbb{Z}_2$.

To describe this algorithms, we need the following notations:

Let $G = (V, A)$ be a Paley graph without loops, and let $v$ be a vertex of $G$. $N^+(v) = \{x \in V \mid (v, x) \in A\}$, $N^-(v) = \{x \in V \mid (x, v) \in A\}$, $X_1 + X_2 = \{X_1 \cup X_2\} - \{X_1 \cap X_2\}$; the symmetric difference of $X_1$ and $X_2$.

Remark 3.1 If $G$ is an undirected Paley graph, then $N^-_{G_0}(v) = N^+_{G_0}(v)$.

3.1 Encryption algorithm

step 1: Generate the ASCII value of each letter $C_i$ in the message $C = C_0C_1...C_{x-1}$.

Step 2: Generate the corresponding binary value of it, then let $B = b_0b_1...b_{2x-1}$ be the binary message corresponding to $C$ with respecting of the same order of $C_i$ in $C$.

Step 3: Choose a prime number $p$(secret key), then consider the Paley graph of order $p$.

Step 4: The encrypted binary message of $B$ is $B' = b'_0b'_1...b'_{2x-1}$ where $b'_i = b_i + \sum_{u \in N^-_{G_0}(u), u \geq 7x-1} b_u + \sum_{u \in N^+(u), u \leq 7x-1} b_u$ for $0 \leq i \leq 7x-1$.

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 to send is $C' = C_0'C_1'...C_{x-1}'$.

Example 3.2 Let $C = \begin{bmatrix} C_0 & C_1 & C_2 & C_3 \end{bmatrix}$ be the plaintext to encrypt and let $p = 29$ the secret key. The binary message $B \in \mathbb{Z}_2^7$ corresponding to ASCII code of $C$ is

$B_0 = 0 b_0 \ b_1 \ b_2 \ b_3 \ b_4 \ b_5 \ b_6$

$B_1 = 0 b_7 \ b_8 \ b_9 \ b_{10} \ b_{11} \ b_{12} \ b_{13}$

$B_2 = 0 b_{14} \ b_{15} \ b_{16} \ b_{17} \ b_{18} \ b_{19} \ b_{20}$

$B_3 = 0 b_{21} \ b_{22} \ b_{23} \ b_{24} \ b_{25} \ b_{26} \ b_{27}$

The encrypted binary message $B'$ is

$B'_0 = 0 b'_0 \ b'_1 \ b'_2 \ b'_3 \ b'_4 \ b'_5 \ b'_6$

$B'_1 = 0 b'_7 \ b'_8 \ b'_9 \ b'_{10} \ b'_{11} \ b'_{12} \ b'_{13}$

$B'_2 = 0 b'_{14} \ b'_{15} \ b'_{16} \ b'_{17} \ b'_{18} \ b'_{19} \ b'_{20}$

$B'_3 = 0 b'_{21} \ b'_{22} \ b'_{23} \ b'_{24} \ b'_{25} \ b'_{26} \ b'_{27}$

The encrypted message to send is

$C' = \begin{bmatrix} C'_0 & C'_1 & C'_2 & C'_3 \end{bmatrix}$

CAN is the control character cancel.

HT is the control character horizontal tab.
3.2 Decryption algorithm

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 $B' = b'_0b'_1...b'_{7s-1}$ be the binary message corresponding to $C'$ with respecting of the same order of $C'_i$ in $C'$.

Step 3: For $0 \leq i \leq 7s - 1$, use the symmetric key to solve over the field $\mathbb{Z}_2$ the linear algebraic equations $b'_i = b_i + \sum_{u \in N(i), mod p}(c) = a(7s-1) b_u + \sum_{u \in N(i), mod p}(c) = a(7s-1) u$, then take the binary decrypted message $B = b_0b_1...b_{7s-1}$.

Step 4: Determine the ASCII code which corresponds to the binary message $b_i$, then the character corresponding to this ASCII code.

**Example 3.3** Let $C' = \begin{bmatrix} C_0 & C_1 & C_2 & C_3 \\ n & CAN & \# & HT \end{bmatrix}$ be the ciphertext to decrypt.

**Step 1 and 2:** The binary message $B'$ corresponding to ASCII code of $C'$ is

$B'_0 = \begin{bmatrix} b'_0 & b'_1 & b'_2 & b'_3 & b'_4 & b'_5 & b'_6 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$

$B'_1 = \begin{bmatrix} b'_7 & b'_8 & b'_9 & b'_{10} & b'_{11} & b'_{12} & b'_{13} \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$

$B'_2 = \begin{bmatrix} b'_{14} & b'_{15} & b'_{16} & b'_{17} & b'_{18} & b'_{19} & b'_{20} \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

$B'_3 = \begin{bmatrix} b'_{21} & b'_{22} & b'_{23} & b'_{24} & b'_{25} & b'_{26} & b'_{27} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

**Step 3:** Let $p = 29$ be the common secret key.

To decrypt the binary message $B'$ corresponding to $\mathbb{Z}_2$ the linear algebraic equations $b'_i = b_i + \sum_{u \in N(i), mod p}(c) = a(7s-1) b_u + \sum_{u \in N(i), mod p}(c) = a(7s-1) u$, where $0 \leq i \leq 7s - 1$.

Indeed, let $G = (g_{ij})$ be the adjacency matrix of the Paley graph of order $p$ and $N = (n_i)_{0\leq i \leq 7s-1}$ the vector of $\mathbb{Z}_2$ defined in the following way: $n_i = \sum_{u \in N(i), mod p}(c) = a(7s-1) u$ for $0 \leq i \leq 7s - 1$.

We have to solve the equation $(A + I)B = B' - N$ over $\mathbb{Z}_2$ after reducing the matrix $(A + I)$ to triangular form.

**Step 4:** The decrypted binary message $B$ is

$B_0 = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$

$B_1 = \begin{bmatrix} b_7 & b_8 & b_9 & b_{10} & b_{11} & b_{12} & b_{13} \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$

$B_2 = \begin{bmatrix} b_{14} & b_{15} & b_{16} & b_{17} & b_{18} & b_{19} & b_{20} \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

$B_3 = \begin{bmatrix} b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} & b_{27} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$

Therefore, the decrypted message is

$C = \begin{bmatrix} C_0 & C_1 & C_2 & C_3 \\ p & u & i & \# \end{bmatrix}$

3.3 security information

Our proposed algorithm is an effective algorithm because of the following reasons:

1. If $p = 1 \mod 4$, then we have to use the undirected Paley graph according to the following property:
   if $a$ is a quadratic residue, then $-a$ still remains a quadratic residue.

2. If $p = 3 \mod 4$, then we have to use the directed Paley graph.

3. The behavior of the quadratic residues remains unknown.

4. The behavior of prime numbers is unknown.

5. The encryption of a such message bit is done in function of other messages bits by the neighborhood of the associate vertex of this bit.

6. The decryption part is based on solving over $\mathbb{Z}_2$ a large linear systems.

To ensure security, the sender must choose a very large prime number $p$.

The cryptanalysis of this algorithm is mainly based on The unknown behavior of quadratic residues. Therefore, brute-force attack remains for the moment the only way to discover the possible clear message set that matches the encrypted message by iterating through all the prime numbers. However this is theoretically going to take an enormous amount of time to solve over $\mathbb{Z}_2$ an important number of linear systems.

References

[1] J. Javelle, Cryptographie Quantique: Protocoles et Graphes. Algèbres quantiques [math.QA].Université de Grenoble (2014).

[2] D. Ghinelli, Jennifer D.Key, Codes from incidence matrices and line graphs of Paley graphs, Advances in Mathematics of Communications. 5. 10.3934/amc.2011.5.93. (2011).

[3] Joseph B. Dence and Thomas P. Dence, Cubic and Quartic Residues Modulo A Prime, Missouri J. Math. Sci. 7(1): 24-31 (Winter 1995).

[4] A. Ayushi, A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications (0975 - 8887) Volume 1 - No. 15(2010).
To decrypt the binary message $B$, we have to solve the equation $\sum Z$.

**Step 1 and 2:** The binary message $B$ takes the binary decripted message $Z$ defined in the following way: for $n \leq 7$, generate the ASCII value $Z_i$ from $b_i$.

**Step 3:** For $0 \leq n \leq 7$, $Z_i$ is the common secret key.

**Step 4:** The decrypted binary message $B$ is after reducing the matrix $(3.2)$ to triangular form.

**Decryption Algorithm**

1. If $\text{det}(A) \neq 0$, then we have to use the undirected Paley graph according to the following property: $\text{det}(A) = 0$.
2. If $\text{det}(A) = 0$, then we have to use the directed Paley graph.

The cryptanalysis of this algorithm is mainly based on the following reasons:

1. The behavior of prime numbers is unknown.
2. The behavior of the quadratic residues remains enormous amount of time to solve over a general prime.
3. If $p$ is a prime of $p \equiv 3 \pmod{16}$, then we have to use the undirected Paley graph.
4. If $p \equiv 1 \pmod{16}$, then we have to use the directed Paley graph.
5. The enormous amount of time to solve over a general prime.
6. The decryption part is based on solving over a general prime.

Therefore, the decrypted message is $B$.

**Example 3.3**

Let $A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ \end{pmatrix}$.

The behavior of prime numbers is unknown.

Therefore, the decrypted message is $B$.

**References**

[5] M. Azhar Mushtaq, A. Sultan, M. Afrasayab, New Cryptographic Algorithm Using ASCII Values and Gray Code (AGC). ICBDC 2019: Proceedings of the 2019 4th International Conference on Big Data and Computing May Pages 242-246(2019).