International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 2, (2025), 465–468
DOI: https://doi.org/10.69793/ijmcs/02.2025/zhour

A proposed public-key cryptosystem constructed using Paley graphs

Oumazouz Zhour

Faculty of Science and Technology
Hassan II University
Mohammedia, Morocco

email: oumazouzzhour@gmail.com

(Received October 31, 2024, Revised December 3, 2024,
Accepted December 9, 2024, Published January 4, 2025)

Abstract

The aim of this work is to clearly describe the cryptosystem based on Paley graphs and pose some open problems on which the cryptanalysis part of this cryptosystem is based.

1 Introduction

Any public key cryptosystem depends on some difficult mathematical problem. The Goldwasser–Micali (GM) cryptosystem is the first probabilistic public-key encryption scheme introduced which is based on the problem of quadratic residuosity. In [2] and [4], a symmetric key cryptographic algorithm using Paley graphs is introduced and analyzed. In this paper, we have exploited the problem of quadratic residuosity and the chaotic behavior of the operation $*$ of local complementation to introduce a new relevant application in cryptography. Before starting the description of this cryptosystem, we will cite some important results used in this paper.

Definition 1.1. *Let $G = (g_{ij})_{0\leq i,j\leq n-1}$ be the adjacency matrix corresponding to a graph G of degree n. The graph $G * u = (g_{ij}^{(1)})$ where u is a vertex of G is defined in the following way: $g_{ij}^{(1)} = g_{ij} + g_{iu}g_{uj}$ if $i \neq j$, else* 0.

Key words and phrases: Quadratic residues, Paley graphs, Cryptographic systems, Encryption algorithm, Decryption algorithm, Sequence of Local complementations.
AMS (MOS) Subject Classifications: 11T71.
ISSN 1814-0432, 2025, https://future-in-tech.net

Definition 1.2. *The local minimum degree $\delta_{loc}(G)$ of a graph G is the minimum degree obtained after SLC sequence of local complementations of this graph.*

Let P be a Paley graph whose degree is a prime number $p \equiv 1 \ mod \ 4$.

Theorem 1.3. *[5] The local minimum degree $\delta_{loc}(P) \geq \sqrt{p} - \frac{3}{2}$.*

Theorem 1.4. *[3] The number of the graphs induced by SLC of P is equal to 2^p.*

2 Main results

Let $N_V^+(i)$ be the neighborhood set of a graph $G = (V, A)$ on the right at its vertex i and $\mathbb{Z}_2$ the finite field with two elements.

2.1 Exchange of keys

In this subsection, we will propose a new method allowing how to make secretly an exchange of keys between two interlocutors Alice and Bob. Indeed, they will secretly choose respectively $(s_1, s_2..., s_t)$ and $(s'_1, s'_2..., s'_{t'})$ where $s_i, s'_i, t, t' \in \mathbb{N}$, then Alice will send the graph $G' = G * s_1 * s_2... * s_t$ to Bob. Bob will receive G', then he will send the graph $G'' = G' * s'_1 * s'_2... * s'_{t'}$ to her. The fact that the operation of local complementation is an equivalence relation allows us to say that the secret graph shared between these two interlocutors will be $G = G' * s_1 * s_2... * s_t$. To obtain the secret keys, a spy must solve the following problem: given a graph F, determine a t-tuple $(s_1, s_2..., s_t)$ of vertices of F that verify $F = P * s_1 * s_2... * s_t$. In this case, we say that F is locally parallel to the Paley graph P. Bouchet [1] succeeded in introducing a polynomial complexity algorithm that allows us to decide whether a graph is locally parallel to a specific simple directed graph. The general case is no longer easy to study, especially for Paley graphs which are strongly regular having the highest minimum degree by local complementation.

2.2 Description of the proposed public-key cryptosystem constructed using the Paley graphs

The cryptosystem based on Paley graphs and the local complementation operation was previously introduced in [3]. We noticed that in the key generation part, the interlocutors use the same secret key. This is in contradiction with the key asymmetry property. The previous subsection describes a way to exchange two secret keys between two interlocutors. We describe our proposed cryptosystem in the following table:

Bob	**Alice**
Key creation	
- Choose $p = q^r$ - Choose $\{s_1, s_2, ..., s_t\}$ a secret numbers such that $1 \leq s_i \leq p$ $(\forall i \in [\|1, t\|])$ - Publish p.	
Key exchange	
	- Choose $\{s'_1, s'_2, ..., s'_{t'}\}$ a secret numbers such that $1 \leq s'_i \leq p$ $(\forall i \in [\|1, t\|])$ - Use the Bob's public key p, then consider P_p the Paley graph of degree p. - Send $G' = P_p * s'_1 * s'_2 * ...s'_{t'}$ to Bob
Compute $G'' = G' * s_1 * s_2 * ...s_t$, then send G'' to Alice	
Encryption	
	- Take the binary message $B_M = B_0B_1...B_k$ corresponding to the plain message M - Compute $G = G'' * s'_1 * s'_2 * ...s'_{t'} = P_p * s_1 * s_2 * ...s_t$, then consider G - The encrypted binary message of B_M is $B'_{M'} = b'_0b'_1...b'_k$ where $b'_i \equiv b_i + \sum_{u \in N_V^+(i \bmod p), u \leq k} b_u + \sum_{u \in N_V^+(i), u > k} u \pmod 2$ for $0 \leq i \leq k$. - Send the message M' corresponding to the binary message $B'_{M'}$ to Bob.
Decryption	
- Take the binary message $B'_{M'} = b'_0b'_1...b'_k$ received from Alice. - Let $G = P_p * s_1 * ...s_t$, then consider G to be the graph induced by sequence of local complementations of the Paley graph P_p of degree p (p is the public key) at $s_1, s_2, .., s_t$; that are secret - For $0 \leq i \leq k$, use the symmetric key to solve over $\mathbb{Z}_2$ the linear algebraic equations $b'_i = b_i + \sum_{u \in N_V^+(i \bmod p), u \leq k} b_u + \sum_{u \in N_V^+(i), u > k} u$ - The decrypted message is $B_M = b_0b_1...b_k$. Hence, the decrypted message is M.	

Example 2.1. *Let* $P_{13} = (V, A)$ *be the Paley graph of degree* 13 *which is public and let* $B_M = 10011011111001$ *be the binary message corresponding to*

$M = My$. Alice and Bob first choose a triplet of secret vertices $s' = (3, 5, 6)$ and $s = (1, 3, 6)$, respectively. Then Alice sends $G' = P_{13} * 3 * 5 * 6$ to Bob and he tries to compute $G'' = G' * 1 * 3 * 6$. Let
$N_V^+(0) = \{2, 3, 5, 6, 8, 10, 12\}$, $N_V^+(1) = \{2, 4, 5, 6, 8, 9\}$,
$N_V^+(2) = \{0, 1, 3, 4, 6, 12\}$, $N_V^+(3) = \{0, 2, 4, 6, 7, 12\}$,
$N_V^+(4) = \{1, 2, 3, 7, 8, 10, 11\}$, $N_V^+(5) = \{0, 1, 6, 8, 9, 10, 11\}$,
$N_V^+(6) = \{0, 1, 2, 3, 5, 7, 11\}$, $N_V^+(7) = \{3, 4, 6, 8, 10, 11\}$,
$N_V^+(8) = \{0, 1, 4, 5, 6, 7, 10, 12\}$, $N_V^+(9) = \{1, 5, 11, 12\}$,
$N_V^+(10) = \{1, 3, 5, 6, 8, 9, 11\}$, $N_V^+(11) = \{4, 5, 6, 7, 9, 10, 12\}$,
$N_V^+(12) = \{0, 2, 3, 8, 9, 11\}$.
Using the formula cited in the part of encryption, $B'_{M'} = 10011100011101$.

3 Conclusion and open problems

The proposed cryptosystem is based on several difficult problems in graph theory such as the classification in terms of degree of the graph induced by SLC of Paley graphs and the local equivalence problem. Without giving any information on the problems mentioned above, we can say that this cryptosystem is powerful because it also relies on the problem of quadratic residuosity which is equivalent to the factorization problem on which the RSA cryptosystem is based.

References

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

[2] Z. Oumazouz, D. Karim, *A new symmetric key cryptographic algorithm using Paley graphs and ASCII values,* Proceeding E3S Web of Conf., **297,** (2021), 01046. https://doi.org/10.1051/e3sconf/202129701046

[3] Z. Oumazouz, *Novel public-key cryptosystem based on the problem of performing sequence of local complementations on the Paley graphs,* Int. J. Math. Comput. Sci., **17,** no. 3, (2022), 1451–1461.

[4] Z. Oumazouz, D. Karim, *The analysis and implementation of the symmetric key cryptographic algorithm based on the algebraic Paley graphs,* Int. J. Math. Comput. Sci., **17,** no. 4, (2022), 1563–1567.

[5] J. Javelle, M. Mhalla, S. Perdrix *On the minimum degree up to local complementation: Bounds and complexity,* Int. Workshop on Graph-Theoretic Concepts in Computer Science, (2012), 138-147.