Algebraic coding theory using Pell equation $x^2 - 8y^2 = 1$

Janaki G[*]
Gowri Shankari A[†]

Abstract

An interdisciplinary field with significant practical use is cryptography. The difficulty of specific mathematical computing tasks affects a public key cryptosystem's security. The technique for coding and decoding the messages was described in this work, utilising the solutions of Pell equation $x^2 - 8y^2 = 1$ and matrix Q^{8^*}. It was noted that messages can be turned into an even size that is then divided into slabs. Considering the information security has become a more serious issue in recent years, coding and decoding algorithms are essential in order to improve information security. In this article, a new matrix Q8* and a decryption system based on the solutions of the Pell Equation $x^2 - 8y^2 = 1$ are devised. The messages can be divided into even-sized slabs during encryption. This algorithm will not only improve information security but also has a high degree of accuracy.

Keywords: Pell equation; Encryption-decryption algorithm; Q^{8^*} matrix; Cryptography
2020 AMS subject classifications: 11B37, 11C20, 11D09, 11T71.
[1]

[*] Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli-18, Tamil Nadu, India. janakikarun@rediffmail.com.

[†] Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli-18, Tamil Nadu, India. gowrirajinikanth@gmail.com.

[1] Received on September 15, 2022. Accepted on December 15, 2022. Published on March 20, 2023. DOI: 10.23755/rm.v46i0.1062. ISSN: 1592-7415. eISSN: 2282-8214. ©Janaki G et al. This paper is published under the CC-BY licence agreement.

1 Introduction

Currently, almost all current coding methods can be supported by number theory Carmichael [1950], Disckson [1952], Trappe and Washington [2006]. Samuel F.B. Morse, an American inventor, developed the first coding technique that used just two symbols—a dot and a comma—to transmit the first cypher message in 1844 through an electric telegraph. He called it Morse code. Later, binary code encoding improved as a more secure method for encrypting messages, and it is still in use today Saranya and Janaki [2019], Janaki and Saranya [2020]. Binary code encoding divides each coded word into blocks of ones and zeros. The twentieth century saw important advancements in coding. It is common knowledge that the Fibonacci sequences are defined as $Fn + 1 = Fn + Fn - 1$ with the initial parameters F0=0and F1=1. The definition of the Fibonacci Q-matrix is $Q = [(11@10)]$, and its nth power is of the form Carmichael [1950], Disckson [1952], Trappe and Washington [2006]. Several approaches were used to study the Fibonacci coding principle. For instance, utilising the key variability notion in symmetric key algorithm and the Fibonacci Q-matrix, a novel method for safe information transmission through communication channels was developed. By using blocking matrices and Fibonacci numbers, a new cryptography algorithm was recently described in Berges [1981], Gould [1981]. Using the help of the Pell equation's solutions $x^2 8y^2 = 1$ that were found in Tas et al. [2018], Sumeyra et al. [2019] and the new matrix Q8*, we present new coding and decoding algorithms in this work. Also, this method's fundamental principle hinges on subdividing the message into a 2x2 slab matrix. The security of information will be improved by using this technology, which also has a high degree of accuracy in data transmission via communication channels Saranya and Janaki [2019], Janaki and Saranya [2020].

The connection of recurrence for the Pell equation $x^2 - 8y^2 = 1$ is

$$\begin{aligned} x_{n+1} &= 3x_n + 8y_n \\ y_{n+1} &= x_n + 3y_n \end{aligned}$$

For $n \geq 1$, where $x_1 = 3, y_1 = 1$.
It is noted that $Q^{8^*} = \begin{pmatrix} x_j & 8y_j \\ y_j & x_j \end{pmatrix}$
The primary concept is to turn the messages into order 2×2 block matrices. The number of blocks and letter positions must be determined based on this. Then encrypted matrix P is obtained and Q^{8^*} utilized for decryption.

2 Main results

2.1 Representations:

1. $G-$ a message-to-be-sent matrix constituted by an even order.

2. $G_j - j^{th}$ block of G whose size is 2.

3. $g-$ Number of slabs G_j of G.

4. $m = \begin{cases} 3 \text{ if } & g \geq 3 \\ g \text{ if } & g > 3 \end{cases}$

5. $D_j = |G_j|$.

6. $G_j = \begin{pmatrix} g_{j1} & g_{j2} \\ g_{j3} & g_{j4} \end{pmatrix}$

7. $P-$ encrypted matrix defined by $P = \begin{pmatrix} d_j & g_{jk} \end{pmatrix}_{k \in \{1,2,4\}}$

8. $\left(Q^{8^*}\right)^m = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$

9. $*-$ denotes the space between the words.

2.2 Assignment of alphabets:

A	B	C	D	E	F	G	H	I
m	m+1	m+2	m+3	m+4	m+5	m+6	m+7	m+8
J	K	L	M	N	O	P	Q	R
m+9	m+10	m+11	m+12	m+13	m+14	m+15	m+16	m+17
S	T	U	V	W	X	Y	Z	*
m+18	m+19	m+20	m+21	m+22	m+23	m+24	m+25	m-1

2.3 Algorithm for encryption:

1. Create an even order matrix G for the provided message.

2. Separate G_j into slabs of size 2 and calculate g.

3. Selecting m using g.

4. Replace the alphabets with the provided numbers to get the elements of G_j.
5. Find D_j.
6. Create P.

2.4 Algorithm for decryption:

Using P, one must find G. The goal is to locate g_{j3} as P contains g_{j1}, g_{j2}, g_{j4}.

1. Identify $\left(Q^{8^*}\right)^m$
2. Identify its constituents as q_{ij}'s.
3. Explore $p_{j1} = q_{11}g_{j1} + q_{21}g_{j2}$
4. Explore $p_{j2} = q_{12}g_{j1} + q_{22}g_{j2}$
5. Solve $D_j = p_{j1}(q_{12}s_j + q_{22}g_{j4}) - p_{j2}(q_{11}s_j + q_{21}g_{j4})$ for s_j.
6. Replace $s_j = g_{j3}$
7. Establish G_j
8. Establish G

2.5 Encryption decryption algorithm using (x, y) such that $x^2 - 8y^2 = 1$

The following are a few Pell equation $x^2 - 8y^2 = 1$ solutions:

j	1	2	3	4	5	6	7	8
x_j	3	17	99	577	3363	19601	114243	665857
y_j	1	6	35	204	1189	6930	40391	235416

Case (i): g=1

Example: 1 Take "ARMY" as the encrypted message.

Encryption:

$$G = \begin{pmatrix} A & R \\ M & Y \end{pmatrix}$$

Here there is only one block so $g = 1$.

This implies $m = 3$.

Thus $G_1 = \begin{pmatrix} 3 & 20 \\ 15 & 27 \end{pmatrix}$ and so $g_{11} = 3, g_{12} = 20, g_{13} = 15, g_{14} = 27$.

$\therefore D_1 = -219$

$P = \begin{pmatrix} -219 & 3 & 20 & 27 \end{pmatrix}$

Decryption:

$$\left(Q^{8^*}\right)^3 = \begin{pmatrix} x_3 & 8y_3 \\ y_3 & x_3 \end{pmatrix} = \begin{pmatrix} 99 & 280 \\ 35 & 99 \end{pmatrix}$$

$\Rightarrow q_{11} = 99, q_{12} = 280, q_{21} = 35, q_{22} = 99$.

Apply p_{j1} and p_{j2}, one can get $p_{11} = 997$ and $p_{12} = 2820$.

$$\begin{aligned} D_1 &= p_{11}(q_{12}s_1 + q_{22}g_{14}) - p_{12}(q_{11}s_1 + q_{21}g_{14}) \\ -219 &= 997(280s_1 + 2673) - 2820(99s_1 + 945) \\ \Rightarrow s_1 &= 15 \end{aligned}$$

Thus $g_{13} = s_1 = 15$.

$$\therefore G_1 = \begin{pmatrix} 3 & 20 \\ 15 & 27 \end{pmatrix} \text{ from } P$$

Hence $G = \begin{pmatrix} A & R \\ M & Y \end{pmatrix}$.

Case (ii): g=4

Example: 2 Take “AMOUNT RECEIVED” as the encrypted message.

Encryption:

$$G = \begin{pmatrix} A & M & O & U \\ N & T & * & R \\ E & C & E & I \\ V & E & D & * \end{pmatrix}$$

Here there are four blocks so $g = 4$.

$$\therefore G_1 = \begin{pmatrix} A & M \\ N & T \end{pmatrix}, G_2 = \begin{pmatrix} O & U \\ * & R \end{pmatrix}, G_3 = \begin{pmatrix} E & C \\ V & E \end{pmatrix}, G_4 = \begin{pmatrix} E & I \\ D & * \end{pmatrix}$$

Choose $m = 4$

Thus $G_1 = \begin{pmatrix} 4 & 16 \\ 17 & 23 \end{pmatrix}, G_2 = \begin{pmatrix} 18 & 24 \\ 3 & 21 \end{pmatrix}, G_3 = \begin{pmatrix} 8 & 6 \\ 25 & 8 \end{pmatrix}, G_4 = \begin{pmatrix} 8 & 12 \\ 7 & 3 \end{pmatrix}$
Hence $D_1 = -180,\ D_2 = 306,\ D_3 = -86,\ D_4 = -60$

$$P = \begin{pmatrix} -180 & 4 & 216 & 23 \\ 306 & 18 & 24 & 21 \\ -86 & 8 & 6 & 8 \\ -60 & 8 & 12 & 3 \end{pmatrix}$$

Decryption:

$$\left(Q^{8^*}\right)^4 = \begin{pmatrix} x_4 & 8y_4 \\ y_4 & x_4 \end{pmatrix} = \begin{pmatrix} 577 & 1632 \\ 204 & 577 \end{pmatrix}$$

$\Rightarrow q_{11} = 577, q_{12} = 1632, q_{21} = 204, q_{22} = 577.$

$\therefore$ One can find,

p_{11}	p_{12}	p_{21}	p_{22}	p_{31}	p_{32}	p_{41}	p_{42}
5572	15760	15282	43224	5840	16518	7064	19980

On solving the equation

$$D_j = p_{j1}(q_{12}s_j + q_{22}g_{j4}) - p_{j2}(q_{11}s_j + q_{21}g_{j4}),$$

one can get $s_1 = 17, s_2 = 3, s_3 = 25, s_4 = 7.$

Thus $g_{13} = s_1 = 17, g_{23} = s_2 = 3, g_{33} = s_3 = 25, g_{43} = s_4 = 7.$

Thus,

$$G_1 = \begin{pmatrix} 4 & 16 \\ 17 & 23 \end{pmatrix}, G_2 = \begin{pmatrix} 18 & 24 \\ 3 & 21 \end{pmatrix}, G_3 = \begin{pmatrix} 8 & 6 \\ 25 & 8 \end{pmatrix}, G_4 = \begin{pmatrix} 8 & 12 \\ 7 & 3 \end{pmatrix} \text{ from } P.$$

Hence

$$G = \begin{pmatrix} A & M & O & U \\ N & T & * & R \\ E & C & E & I \\ V & E & D & * \end{pmatrix}$$

3 Conclusions

The paper identifies a few particular cryptographic applications that can be utilised to demonstrate and comprehend the fundamental idea of the Fibonacci Q matrix. Fibonacci, often spelled Bonacci, Leonard of Pisa, or Leonardo Bigollo Pisano, was an Italian mathematician who was born in the Republic of Pisa. He is regarded as "the most talented Western mathematician of the Middle Ages" and had a significant impact on number theory. Moreover, Pell's equation refers to any Diophantine equation of the type $x^2 - 8y^2 = 1$, where n is a given positive non-square integer and integer solutions are sought for x and y.

In this work, using the solutions of the Pell equation$x^2 - 8y^2 = 1$ and Q^{D^*} is defined. This contributes to the decryption algorithm. In encryption, the message must first be transformed into an even single matrix, then into slabs of size 2. The fact that the entries Q^{D^*} get bigger and bigger depends on the strict secrecy. One may search the decryption algorithm for the solutions of other well-known equations with the new matrix Q^{D^*}. On the basis of this scheme various more algorithms can be developed.

References

C. Berges. A history of the fibonacci q-matrix and a higher- dimensional problem. *Fibonacci Quart*, 19(3):250–257, 1981.

R. Carmichael. *The Theory of Numbers and Diophantine Analysis*. Dover Publications Co., New York, 1950.

L. Disckson. *History of The Theory of Numbers, Volume II*. Chelsia Publishing Co., New York, 1952.

H. Gould. A history of the fibonacci q-matrix and a higher- dimensional problem. *Fibonacci Quart*, 19(3):250–257, 1981.

G. Janaki and C. Saranya. Observations on the binary quadratic diophantine equation $x^2 - 2xy - y^2 + 2x + 14y = 72$. *International Journal of Scientific Research in Mathematical and Statistical sciences*, 7(2):152–155, 2020.

C. Saranya and G. Janaki. Solutions of pell's equation involving jarasandha numbers. *International Journal of Scientific Research in Mathematical and Statistical sciences*, 6(1):234–236, 2019.

U. Sumeyra, T. Nihal, and N. Ozgur. new application to coding theory via fibonacci and lucas numbers. *Mathematical Sciences and Applications E-Notes*, 7(1):62–70, 2019.

N. Tas, S. Ucar, N. Ozgur, and O. Kaymak. A new coding/ decoding algoirithm using fibonacci numbers. *Discrete Mathematics, Algorithms and Applications*, 10(2), 2018.

W. Trappe and L. Washington. *Introduction to Cryptography*. Prentice Hall, 2006.