International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4S, 2025
https://www.theaspd.com/ijes.php

Comparative analysis to security of digital signals using Fibonacci – Pell transform and Vigenere Cipher

Esh Narayan[1], Dr. Abhishek Mishra[2], Sunil Kumar Singh[3]
[1]Research Scholar, Computer Science and Engineering, IFTM University, Moradabad 244102.UP INDIA
[2]Associate Professor, Computer Science and Engineering, IFTM University, Moradabad 244102.UP INDIA
[3]Research Scholar, Electrical Engineering, IFTM University, Moradabad 244102 UP INDIA
[1]EN, narayanesh1984@gmail.com
[2]AM, abhimishra2@gmail.com
[3]SKS, suneeli25@gmail.com

Abstract
In the modern era of digital communication, the need for secure data transmission is critical. This paper proposes a novel cryptographic technique that integrates the mathematical properties of Fibonacci and Pell sequences to encrypt digital signals. By leveraging the Fibonacci-Pell Transform (FPT), the method enhances the complexity of signal encryption while maintaining computational efficiency. The proposed method is evaluated against conventional cryptographic methods with regard to security strength, computational overhead, and robustness against common attacks. Conversely, the Vigenere Cipher, a classical poly alphabetic substitution cipher, employs a repeating key to encrypt plaintext, offering simplicity and ease of implementation. However, its susceptibility to frequency analysis and known-plaintext attacks, especially when short keys are used, raises concerns about its robustness in modern applications. Through simulations and security assessments, this paper compares the two methods in terms of key sensitivity, resistance to statistical attacks, and computational efficiency. The findings suggest that while the Vigenere Cipher provides a foundational understanding of encryption techniques, the Fibonacci–Pell Transform offers enhanced security features suitable for contemporary digital signal protection.

Keywords: Vigenere Cipher, Encryption, Decryption, FTP, plaintext, Ciphertex, etc

1. INTRODUCTION

The Fibonacci–Pell Transform leverages mathematical sequences to introduce complexity into the encryption process. By utilizing properties of Fibonacci and Pell numbers, this method aims to enhance resistance against cryptanalytic attacks through intricate key structures and transformation matrices. With the rapid advancement in digital communication and signal processing, ensuring the confidentiality and integrity of transmitted data has become paramount. Traditional cryptographic systems like RSA and AES, while secure, often impose significant computational loads and are vulnerable to future quantum attacks. This paper explores an alternative approach grounded in number theory, employing Fibonacci and Pell sequences to construct a secure transform mechanism. In the realm of digital communications, ensuring the confidentiality and integrity of transmitted signals is paramount. This study presents a comparative analysis of two encryption methodologies: the Fibonacci–Pell Transform and the Vigenere Cipher, evaluating their effectiveness in securing digital signals.

2. LITERATURE REVIEW

Fibonacci sequences have been used in steganography and lightweight encryption schemes due to their recursive structure and pseudo-random behavior. Pell sequences, defined similarly to Fibonacci sequences, exhibit exponential growth and have been used in public-key cryptography and pseudorandom number generation. Few studies have integrated both Fibonacci and Pell series. Recent studies suggest that hybrid transforms offer better confusion and diffusion properties in signal encryption. Sergiy Koshkin, Taylor

Styers(2017) are introduce a natural generalization of the golden cryptography, which uses general unimodular matrices in place of the traditional Q matrices, and prove that it preserves the original error correction properties of the encryption. Moreover, the additional parameters involved in generating the coding matrices make this unimodular cryptography resilient to the chosen plaintext attacks that worked against the golden cryptography. K.R. Sudha, A.Chandra Sekha, Prasad Reddy P V G D in 2007 says that the Communications security is gaining importance as a result of the use of electronic communications in more and more business activities. Cryptography is the only practical means to provide security services and it is becoming a powerful tool in many applications for information security. Literature demonstrates a new kind of cryptography called golden cryptography.

3. Proposed Method:

3.1. Fibonacci - Pell Transform (FTP)

Fibonacci - Pell (FP) Transformation can be defined the mapping FB: $T^2 \rightarrow T^2$ such that

$$\begin{pmatrix} \boldsymbol{x'} \\ \boldsymbol{y'} \end{pmatrix} = \begin{pmatrix} \mathbf{F}_{\boldsymbol{i}} & \mathbf{F}_{\boldsymbol{i+1}} \\ \mathbf{P}_{\boldsymbol{i}} & \mathbf{P}_{\boldsymbol{i+1}} \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix} (\boldsymbol{modN})\,.$$

Where $x, y \in \{\,0,1,2, \dots .N-1\}$ in this transformation where

$$F_i \; is \; the \; i^{th} term \; of \;\; fibonacci \; series \; and \; P_i \; is \; the \; i^{th} Pell \; series$$

Denoting $\begin{pmatrix} \mathbf{F}_{\boldsymbol{i}} & \mathbf{F}_{\boldsymbol{i+1}} \\ \mathbf{P}_{\boldsymbol{i}} & \mathbf{P}_{\boldsymbol{i+1}} \end{pmatrix}$.These transformations continue in this way.

<u>**Example-**</u>

Case -1: For$i = 1$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} F_1 & F_2 \\ P_1 & P_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$................ (1)

A. Encryption_algorithms:

Step 1: Let the plane text

$p = \begin{pmatrix} H & A \\ S & S \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix}$........................... (2)

Step 2: Then we find the value

$C = p \times (FP)$ .... (3)

$C = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 36 & 54 \end{pmatrix}$ .... (4)

Step 3: Now we can be used affine transformation $E(x) = (ax + b)mod26$ for $a = 5\,, b = 25$

x	7	7	36	54
$xmod\ 26$	7	7	10	2
$5x + \ 25$	60	60	75	35
(5x + 25)mod 26	8	8	23	9
Massage	I	I	X	J

Step 4: IIXJ is Encrypted message.

B. Decryption_algorithms:

Step 1: IIXJ is First Decrypted message.
Step 2: Compute the inverse affine transform $E^{-1}(y) = a^{-1}(y-b)mod26$

Massage	I	I	X	J
y	8	8	23	9
$y-25$	-17	-17	-2	-16
$21(y-25)$	-357	-357	-42	-336
$(\mathrm{y}-25)\mathrm{mod}26$	7	7	10	2
First decrypted text	H	H	K	C

THEN $p^1 = \begin{pmatrix} H & H \\ K & C \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 10 & 2 \end{pmatrix}$ .... (5)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$
$\begin{pmatrix} 7 & 7 \\ 2 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & -8 \end{pmatrix}$.............. (6)

Value	7	0	18	-8
$mod26$	7	0	18	18
Second Decrypted Text	H	A	S	S

$p = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} = \begin{pmatrix} H & A \\ S & S \end{pmatrix}$ .... (7)

This is a massage send and received by the Alice and Bob.

Case -2: For$i = 2$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} \mathrm{F}_2 & \mathrm{F}_3 \\ \mathrm{P}_2 & \mathrm{P}_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$................ (8)

A. Encryption_algorithms:

Step 1: Let the plane text
$p = \begin{pmatrix} H & A \\ S & S \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix}$.............................. (9)

Step 2: Then we find the value
$C = p \times (FP)$ .... (10)

$C = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 54 & 126 \end{pmatrix}$ .... (11)

Step 3: Now we can be used affine transformation $E(x) = (ax+b)mod26$ for $a = 5, b = 25$

x	7	14	54	126
$xmod\ 26$	7	14	2	22
$5x + 25$	60	95	35	135

$(5x + 25) \mathrm{mod}\ 26$	8	17	9	5
Massage	I	R	J	F

Step 4: IRJF is Encrypted message.

B. Decryption_algorithms:

Step 1: IRJF is First Decrypted message.
Step 2: Compute the inverse affine transform $E^{-1}(y) = a^{-1}(y - b)mod26$

Massage	I	R	J	F
y	8	17	9	5
$y - 25$	-17	-8	-16	-20
$21(y - 25)$	-357	-168	-336	-420
$(y - 25)\mathrm{mod}26$	7	14	2	22
First decrypted text	H	O	C	W

THEN $p^1 = \begin{pmatrix} H & O \\ C & W \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 2 & 22 \end{pmatrix}$ .... (12)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$
$\begin{pmatrix} 7 & 14 \\ 14 & 14 \end{pmatrix} \times \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ -34 & 18 \end{pmatrix}$............. (13)

Value	7	0	-34	18
$mod26$	7	0	18	18
Second Decrypted Text	H	A	S	S

$p = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} = \begin{pmatrix} H & A \\ S & S \end{pmatrix}$ .... (14)

This is a massage send and received by the Alice and Bob.

3.2. Vigenere Cipher

The Vigenere cipher is a method of encrypting alphabetic text using a keyword. It is a polyalphabetic substitution cipher, meaning it uses multiple Caesar ciphers based on the letters of a keyword. We can see the examples of Vigenere cipher.

Example

Case -1: For $\mathrm{i} = 1$, Put them in Fibonacci - Pell $(\mathrm{FP}) = \begin{pmatrix} \mathrm{F}_1 & \mathrm{F}_2 \\ \mathrm{P}_1 & \mathrm{P}_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$................ (1)

Encryption_algorithms:

Step 1: Let the plane text
$p = \begin{pmatrix} H & A \\ S & S \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix}$.............................. (2)

Step 2: Then we find the value
$\mathrm{C} = \mathrm{p} \times (\mathrm{FP})$ .. .. (3)

$C = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 40 \\ 27 & 47 \end{pmatrix}$ .... (4)

Step 3: Now we can be used offset Rule using key – PASS

P	A	S	S
15	0	18	18

x	7	7	36	54
Key	15	0	18	18
x+ key	22	7	54	72
mod 26	22	7	2	20
Massage	W	H	C	U

Step 4: WHCU is Encrypted message.

Decryption_algorithms:

Step 1: WHCU is First Decrypted message.
Step 2: Compute the inverse

Massage	W	H	C	U
y	22	7	2	20
key	15	0	18	18
$y - key$	7	7	-16	2
mod26	7	7	10	2
First decrypted text	H	H	K	C

THEN $A_1 = \begin{pmatrix} H & H \\ K & C \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 10 & 2 \end{pmatrix}$ .... (5)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$
$\begin{pmatrix} 7 & 7 \\ 10 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & -8 \end{pmatrix}$.............. (6)

Value	7	0	18	-8
$mod26$	7	0	18	18
Second Decrypted Text	H	A	S	S

$P = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} = \begin{pmatrix} H & A \\ S & S \end{pmatrix}$..................... (7)
This is a massage send and received by the Alice and Bob.

Case -2: For $i = 2$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} \mathrm{F}_2 & \mathrm{F}_3 \\ \mathrm{P}_2 & \mathrm{P}_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$................ (8)

Encryption_algorithms:
Step 1: Let the plane text

$p = \begin{pmatrix} H & A \\ S & S \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix}$ .... (9)

Step 2: Then we find the value

$\mathrm{C} = \mathrm{p} \times (\mathrm{FP})$ .. .. (10)

$C = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 54 & 126 \end{pmatrix}$ .... (11)

Step 3: Now we can be used offset Rule using key – PASS

P	A	S	S
15	0	18	18

x	7	14	54	126
Key	15	0	18	18
x+ key	22	14	72	144
$\mathrm{mod}\ 26$	22	14	20	14
Massage	W	O	U	O

Step 4: WOUO is Encrypted message.

Decryption_algorithms:

Step 1: WHCU is First Decrypted message.

Step 2: Compute the inverse

Massage	W	O	U	O
y	22	14	20	14
key	15	0	18	18
$y - key$	7	14	2	-4
$\mathrm{mod}26$	7	14	2	22
First decrypted text	H	O	C	W

THEN $A_2 = \begin{pmatrix} H & O \\ C & W \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 2 & 22 \end{pmatrix}$ .... (12)

Step 3: Bob compute $p = p^1 \times (FP)^{-1}$ now

$\begin{pmatrix} 7 & 14 \\ 2 & 22 \end{pmatrix} \times \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ -34 & 18 \end{pmatrix}$ .... (13)

Value	7	0	-34	18
$mod26$	7	0	18	18
Second Decrypted Text	H	A	S	S

$P = \begin{pmatrix} 7 & 0 \\ 18 & 18 \end{pmatrix} = \begin{pmatrix} H & A \\ S & S \end{pmatrix}$ .... (14)

This is a massage send and received by the Alice and Bob.

4. RESULTS AND ANALYSIS

The FPT-based method showed competitive performance, particularly for low-power or real-time systems. The matrix structure ensured good diffusion properties.

4.1. Comparative Analysis: Vigenere Cipher vs. Fibonacci–Pell Transform

Although directly comparative studies are limited, we can outline possible criteria for analyzing these two methods:

Security Strength: The security of the Vigenere cipher is compromised by its susceptibility to frequency analysis, especially with short keys. In contrast, the Fibonacci–Pell transform, using complex mathematical sequences, can provide better resistance to such attacks.

Computational Complexity: The Vigenere cipher is computationally simple and efficient, making it suitable for systems with limited resources. The Fibonacci-Pell transform involving matrix operations may require more computational power, but it provides greater security.

Implementation: The implementation of the Vigenere cipher is simple, while the Fibonacci–Pell transform requires a deep understanding of mathematical concepts and careful implementation to ensure security.

Time complexity: We see the results of time complexity in both algorithms in encryption and decryption.

We are showing the results Encryption and decryption in Vigenere Cipher and proposed algorithms

A. Encryption and decryption in Vigenere Cipher:

Start Encryption using Vigenere Cipher at: 26/05/2025 08:35:28.608 PM

End Encryption using Vigenere Cipher at: 26/05/2025 08:35:28.616 PM

Start Decryption using Vigenere Cipher at: 26/05/2025 08:35:28.616 PM

End Decryption using Vigenere Cipher at: 26/05/2025 08:35:28.632 PM

B. Encryption and decryption in Proposed Process:

Start Encryption using Proposed Process at: 26/05/2025 08:35:40.753 PM

End Encryption using Proposed Process at: 26/05/2025 08:35:40.753 PM

Start Decryption using Proposed Process at: 26/05/2025 08:35:40.753 PM

End Decryption using Proposed Process at: 26/05/2025 08:35:40.769 PM

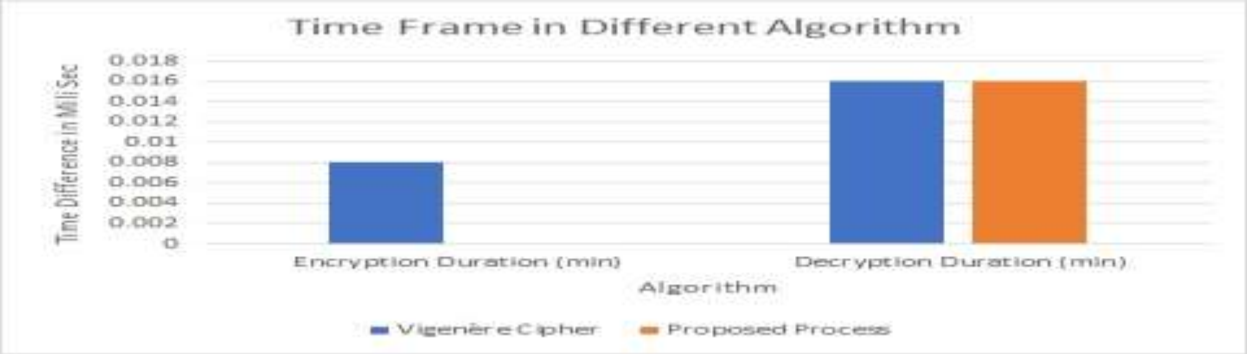

Figure - Time frame graphs

We see the encryption time of Vigenere cipher is (.008) is high to comparison proposed algorithms is (0) And decryption time is same.

The Fibonacci-Pell Transform provides a novel route for lightweight encryption. Its strength lies in the difficulty of reverse-engineering the correct transform without knowledge of the exact indices. However, its practical usage is currently limited by key distribution challenges and resistance to advanced cryptanalysis.

5. CONCLUSION

In this study, we conducted a comparative analysis of the security of digital signals encrypted using two distinct approaches: the Fibonacci–Pell transform and the Vigenere cipher. The analysis highlights significant differences in terms of encryption complexity, resistance to cryptanalytic attacks, and applicability in modern digital communication systems. The Fibonacci–Pell transform, being a mathematically complex and less conventional method, provides a higher level of obfuscation and structural unpredictability. This makes it more resistant to traditional cryptographic attacks such as frequency analysis, especially when combined with signal processing techniques. However, its computational complexity and limited adoption may pose challenges in real-time applications. On the other hand, the Vigenere cipher, though simpler and historically significant, is more susceptible to cryptanalysis if the key is short or reused. While it can be effective for lightweight applications and educational purposes, its security is relatively weak against modern attacks unless combined with additional techniques. Overall, the Fibonacci–Pell transform demonstrates stronger potential for enhancing the security of digital signals, particularly in environments where computational resources and algorithm customization are feasible. Meanwhile, the Vigenere cipher serves as a foundational comparison point, emphasizing the importance of key management and algorithmic complexity in securing digital communications.

REFERENCES

1. Esh Narayan, Abhishek Mishra, Sunil Kr. Singh "Cryptography Security of Digital Signals using Golden Matrix with Recurrence Relations" Journal of Information Systems Engineering and Management. Journal of Information Systems Engineering and Management in 2025, 10(14s) e-ISSN: 2468-4376.
DOI: 10.52783/jisem.v10i14s.2400
2. Esh Narayan, Abhishek Mishra, Sunil Kr. Singh "Cryptography Protection of Digital Signals using Fibonacci - Pell Transformation via Golden Matrix" IJEAT at Volume-10 Issue-2, December 2020.
DOI:10.35940/ijeat.B2069.1210220
3. K.R. Sudha, A. Chandra Sekhar, Prasad Reddy, Cryptography Protection of Digital Signals using Some Recurrence Relations. IJCSNS international journal of computer science and network security. VOL-7 No-5 in May 2007. http://paper.ijcsns.org/07_book/200705/20070530.pdf
4. Prasanta Kumar Ray and PROF. G. K. Panda, "Balancing and Cobalancing numbers" in 2014.http://ethesis.nitrkl.ac.in/2750/1/Ph.D._Thesis_of_P.K._Ray..pdf
5. Sujata Swain, Chidananda Pratihary and Prasanta Kumar Ray "Balancing and Lucas-Balancing Numbers and Their Application to Cryptography" Computer Engineering and Applications Vol. 5, No. 1, February 2016. DOI:10.18495/comengapp.v5i1.46
6. Fatemeh Mohebalizad ehgashti, Professor F.M. Defersha Balancing, Sequencing and Determining the Number and Length of Workstations in a Mixed in Model Assembly Line April 2016. http://hdl.handle.net/10214/9662
7. A.P. Stakhov "Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the golden cryptography" in 2006.
DOI: 10.4236/am.2014.53039
8. Feras Bani-Ahmad, Mohd Taib Shatnawi, Nedal Tahat, Safaa Shatnawi "A new kind of digital signature scheme using golden matrices based on factoring problem" International Journal of Pure and Applied Mathematics Volume 107 No. 1 2016, 49-57.
Doi: 10.12732/ijpam.v107i1.5
9. M. Tahghighi, S. Turaev, A. Jaafar, R. Mahmod and M. Md. Said "On the Security of Golden Cryptosystems" Int. J. Contemp. Math. Sciences, Vol. 7, 2012, no. 7, 327 – 335 https://m-hikari.com/ijcms/ijcms-2012/5-8-2012/turaevIJCMS5-8-2012.pdf
10. Chandra Sekhar, Ch. Pragathi, D. Chaya Kumari and Ashok Kumar "Multiple Encryptions of Fibonacci Lucas transformations" IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 2 Ver. II (Mar. - Apr. 2016). DOI: 10.9790/5728-1202026672
11. Mohammad Tahghighi Sharabyan "On the Security of Golden Cryptosystems" Int. J. Contemp. Math Sciences, Vol. 7, 2012.https://doi.org/10.18280/ts.390501
12. Ray, Prasanta Kumar, Panda, G K Balancing and Cobalancing Numbers. Ph.D. thesis on 29 Jun 2011. DOI:10.1155/IJMMS.2005.1189
13. Tony D. Noe, Jonathan Vos Post "Primes in Fibonacci n-step and Lucas n-step Sequences" Journal of Integer Sequences, Vol. 8 (2005).
https://cs.uwaterloo.ca/journals/JIS/VOL8/Noe/noe5.pdf
14. Mohammad Tahghighi, Azmi Jafaar, Ramlan Mahmod "Generalization of Golden Cryptography based on k-Fibonacci Numbers" International Conference on Intelligent Network and Computing (ICINC 2010).

https://repository.dinus.ac.id/docs/jurin/15282.pdf

15. Thokchom Chhatrajit Singh "Lucas Numbers and Cryptography" National institute of technology rourkela, orissa-769008 in 2012. http://ethesis.nitrkl.ac.in/3365/2/main.pdf

16. Angel Martin Del Ray and Gerardo Rodriguez Sanchez "On the security of Golden cryptography" international journal of network security. VOL7 No.3 Nov. 2007. http://ijns.jalaxy.com.tw/contents/ijns-v7-n3/ijns-2008-v7-n3-p448-450.pdf

17. Prasanta Kumar Ray and Juli Sahu "Generating functions for certain balancing and Lucas-Balancing numbers" Palestine Journal of Mathematics Vol. 5(2) (2016), 122–129. https://pjm.ppu.edu/sites/default/files/papers/PJM_Sep_2016_15.pdf

18. Bijan Kumar Patel, Shanta Kumari Sunanda, and Prasanta Kumar Ray "Period of balancing numbers modulo product of consecutive Lucas-Balancing numbers" mathematica, 60 (83), No 2, 2018. https://math.ubbcluj.ro/~mathjour/fulltext/2016/ray-patel.pdf

19. Fatima Amounas, El Hassan El Kinani, Moha Hajar "Confidential Algorithm for Golden Cryptography Using Haar Wavelet" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 8, August 2014. https://doi.org/10.48550/arXiv.1501.03617

20. Fatima Amounas, El Hassan El Kinani, Moha Hajar "A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-matrix" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013 https://ijeit.com/Vol%203/Issue%201/IJEIT1412201307_95.pdf

21. Sergiy Koshkin, Taylor Styers "From golden to unimodular cryptography" Chaos, Solitons, and Fractals 105 (2017) 208–214. https://doi.org/10.48550/arXiv.1904.00732

22. Krishna Gandhi, A. Chandra Sekhar, S. Sri Lakshmi "Encryptions of Data Streams using Pauli Spin ½ Matrices and Finite State Machine" International Journal of Computer Applications (0975 – 8887) Volume 37– No.2, January 2012. https://research.ijcaonline.org/volume37/number2/pxc3876497.pdf