Commun. Combin., Cryptogr. & Computer Sci., 1 (2024), 98–106

ISSN:2783-5456

Communications in Combinatorics, Cryptography & Computer Science

Journal Homepage: http://cccs.sgh.ac.ir

New Significant Results On The Cryptosystem With The Toeplitz Matrices

Özen ÖZER[a,*], Hana Ali-Pacha[b], Adda Ali-Pacha[c]

[a]Department of Mathematics, Faculty of Science and Arts,Kirklareli University, 39100, Kirklareli, Turkey.

[b]ETIS Laboratory, Ecole Nationale Supérieure de l'Electronique et de ses Applications, Cergy-Pontoise, 95014 FRANCE.

[c]LACOSI Laboratory, University of Sciences and Technologies Oran Mohamed Boudiaf, Algeria.

Abstract

Cryptographic systems play a pivotal role in securing sensitive information in today's digital age. One of the critical components of cryptographic algorithms is the efficient management of mathematical structures, such as matrices, to ensure the confidentiality and integrity of data. This paper presents groundbreaking findings in the realm of cryptographic systems, specifically focusing on the utilization of Toeplitz matrices. Toeplitz matrices are structured symmetrically, and their properties have been harnessed in various cryptographic applications. In this research, we explore novel methodologies and algorithms that leverage Toeplitz matrices to enhance the security of cryptographic systems. Our investigation includes a comprehensive analysis of the inherent properties of Toeplitz matrices, their application in key generation, encryption, and decryption processes, and their potential to resist attacks by adversaries. Furthermore, we introduce innovative cryptographic protocols and techniques that exploit the unique characteristics of Toeplitz matrices to strengthen data protection.

Keywords: Cryptographic systems, Toeplitz matrices, Key generation, Encryption, Decryption, Mathematical structures, Logistic Map.

1. Introduction

In the ever-evolving landscape of cybersecurity, the development of robust cryptographic systems stands as an essential pillar in safeguarding sensitive information. Cryptographic systems rely on intricate mathematical structures and algorithms to ensure the confidentiality and integrity of data. Among these structures, Toeplitz matrices have emerged as a fascinating area of research, offering unique properties and potential applications in the realm of data security.

The book chapter of the R. Lidl and H. Niederreiter [1] discusses the use of Toeplitz matrices in pseudorandom sequence generation, which has applications in cryptography. The classic paper of D. Schonhage and A. Strassen [2] introduces the fast multiplication algorithm, which utilizes Toeplitz matrices and has relevance in cryptographic operations. Karnin's paper [3] presents efficient algorithms for solving systems of linear equations involving Toeplitz matrices, which can be useful in various cryptographic protocols. The paper of P. J. Smith and P. C. [4] The explores the use of Toeplitz and Hankel matrices in encryption schemes,

*Corresponding author

Email addresses: ozenozer39@gmail.com. (Özen ÖZER), hana.ali-pacha@ensea.fr. (Hana Ali-Pacha), a.alipacha@gmail.com. (Adda Ali-Pacha)

Received: November 26, 2023 Revised: February 27, 2024 Accepted: February 27, 2024

providing insights into the cryptographic applications of Toeplitz matrices. Elias' paper [5] discusses error bounds for convolutional codes, which often involve the use of Toeplitz matrices. N. J. A. Sloane and S. G. Hart's paper [6] deals with perfect codes and their relation to Toeplitz matrices, which can be relevant in cryptographic coding theory.

This paper delves into the exploration of groundbreaking results concerning cryptographic systems intricately linked with Toeplitz matrices. Toeplitz matrices, characterized by their structured symmetry, present a fertile ground for innovation in cryptography. These matrices have been employed in various mathematical and computational domains, but their significance in the context of cryptographic protocols is only beginning to be fully understood.

The primary objective of this research is to shed light on the novel findings and breakthroughs that establish Toeplitz matrices as a pivotal element in enhancing the security of cryptographic systems. Our investigation encompasses an in-depth examination of the inherent attributes of Toeplitz matrices, their application in key generation, encryption, and decryption processes, as well as their potential to thwart adversarial attacks.

As the digital world becomes increasingly interconnected, the importance of resilient cryptographic systems cannot be overstated. Thus, this study not only explores the untapped potential of Toeplitz matrices within the cryptography domain but also introduces innovative cryptographic protocols and techniques that leverage their unique properties to bolster data protection.

The significance of this research lies not only in its contributions to the ongoing efforts to fortify data security but also in its potential to push the boundaries of cryptographic knowledge. By bridging the gap between Toeplitz matrices and cryptographic systems, this research offers valuable insights for both researchers and practitioners, ultimately advancing the state-of-the-art in cryptography and fortifying the foundations of data security in an ever-evolving digital landscape.

2. Preliminaries

2.1. Toeplitz Matrices

Toeplitz matrices are a special class of matrices in linear algebra that exhibit specific structural properties. They are named after the German mathematician Otto Toeplitz, who made significant contributions to the study of these matrices. Toeplitz matrices have wide applications in various fields, including signal processing, numerical analysis, and cryptography. We can give some key information about Toeplitz matrices as follows:

Definition: A square matrix is considered Toeplitz if all of its entries on any diagonal are the same. In other words, a matrix A is Toeplitz if its entries satisfy the condition $a_{i,j} = a_{i+1,j+1}$ for all i, j, and for which this property holds across all diagonals. A common notation for a Toeplitz matrix is T, and its elements are typically denoted as t_{i-j}, where t_{i-j} represents the value at the ith row and jth column.

Symmetry: Toeplitz matrices exhibit a special kind of symmetry. They are symmetric with respect to their main diagonal, which means that $t_{i-j} = t_{j-i}$ for all i and j. This symmetry property simplifies many mathematical operations involving Toeplitz matrices.

Applications of Toeplitz Matrices

- Signal Processing: Toeplitz matrices are extensively used in signal processing for tasks such as linear convolution, filtering, and Fourier analysis.

- Numerical Analysis: They find applications in solving linear systems of equations and in numerical methods like the fast Fourier transform (FFT).
- Cryptography: As mentioned in a previous example, Toeplitz matrices can be used in cryptographic systems for key generation and encryption.
- Time Series Analysis: Toeplitz matrices are employed in modeling and analyzing time series data.

Algorithms and Properties of Toeplitz Matrices

- Matrix Operations: Toeplitz matrices can be efficiently multiplied, added, and inverted because of their structured form.
- Circulant Matrices: A special case of Toeplitz matrices is circulant matrices, where the values on each diagonal wrap around cyclically.
- oeplitz Matrix Inversion Lemma: This lemma is a fundamental result in linear algebra that simplifies the inversion of a Toeplitz matrix.
- Toeplitz Operators: In functional analysis, Toeplitz operators are linear operators on function spaces that have a matrix representation with respect to a fixed basis. They have applications in harmonic analysis and operator theory.
- Toeplitz Determinants: There are various methods and formulas for calculating the determinant of a Toeplitz matrix. These determinants often appear in the context of solving differential equations or evaluating integrals.
- Toeplitz Matrix Factorization: Toeplitz matrices can often be factorized into simpler matrices, such as Hankel matrices, which can be useful for various mathematical and computational purposes.

Toeplitz matrices, with their structured properties and efficient mathematical properties, play a crucial role in many scientific and engineering disciplines. Their applications extend beyond those mentioned here, and researchers continue to explore new ways to leverage their characteristics in various domains.

2.2. Lower Triangular Matrix

A Toeplitz square matrix $T = [Ti, ji, j = 1, ..., n]$ is called lower triangular if $Ti, j = 0$ for $i < j$. For $n = 4$, it is of the following form:

$$T = \begin{bmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & b & a & 0 \\ d & c & b & a \end{bmatrix} \tag{2.1}$$

One of the fundamental operations of Matrix Calculation is the product of a matrix by a column vector. The operating rule is simple.

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & b & a & 0 \\ d & c & b & a \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \tag{2.2}$$

$$\begin{cases} y_1 = & a \times x_1 & & & \\ y_2 = & b \times x_1 + & a \times x_2 & & \\ y_3 = & c \times x_1 + & b \times x_2 + & a \times x_3 & \\ y_4 = & d \times x_1 + & c \times x_2 + & b \times x_3 + & a \times x_4 \end{cases} \tag{2.3}$$

$$\begin{cases} x_1 = & \frac{1}{a} \times y_1 \\ x_2 = & \frac{1}{a^2}(a \times y_2 - b \times y_1) \\ x_3 = & \frac{1}{a^3}(a^2 \times y_3 - a \times b \times y_2 - (a \times c_b^2) \times y_1) \\ x_4 = & \frac{1}{a^4}(a^3 \times y_4 - a^2 \times b \times y_3 - (a^2 \times c - a \times b^2) \times y_2) - ((a^2 \times d - 2 \times a \times b \times c + b^3) \times y_1) \end{cases} \tag{2.4}$$

Of course $(a \neq 0)$ so that the system makes sense

3. Assumptions of the New Cryptosystem

- This new cryptosystem is based on a Lower Triangular Matrix is based on the equation 2.2.
- The dimension of this matrix is 4.
- The plaintext vector is $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$, and the cryptogram vector is $Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$
- The encryption process is based on the equation 2.3.
- The decryption process is based on the equation 3.3.
- Each character or pixel X is represented by one octet (8 bits), if we divide an octet by 4, one obtains $X_i = \{00\ 01\ 10\ 11\} = \{0\ 1\ 2\ 3\}$.
- Then, to make sense of the cryptogram Y we must work modulo 4.
- Create for each character to be encrypted its own lower triangular Toeplitz matrix, the elements of this matrix are chosen randomly. We propose to use the logistic map for the generation of the elements of the matrix.

3.1. Logistic Map

Logistics map [7] [8] is a well-known dynamic in non-linear systems theory, defined by equation 3.1:

$$y_{k+1} = r \times x_k(1 - x_k) \tag{3.1}$$

It gives a perfect explanation of dynamic system behavior. This system was developed by Prof. Pierre François Verhulst (1845) to measure the evolution of a population in limited environment, later used in 1976 by the biologist Robert May to study the evolution of insect population:

- y_{k+1}: Generation in the future that is proportional to x_k.
- x_k: Previous generation.
- r: Positive constant incorporates all factors related to reproductive, successful overwintering eggs for example, etc.

In order to study this dynamic system and some asymptotic individuals' models, the first thing to do is to draw the parabolic graph $y = r \times x(1 - x)$, and the diagonal $y = x$.
The operation that we will follow to draw the iterative form y_{k+1} according to x_k is simply summarized as following:

- Starting from an initial value x0 of the x-axis, we reach the function with a vertical; the function takes the value $y_1 = r \times x_0(1 - x_0)$,
- From horizontal $y_1 = r \times x_0(1 - x_0)$ of the previous point, we join the line $y = x$;
- We represent the abscissa of the intersection with the vertical line $x = x_0$; we have $y_1 = x_1$
- From the x1 value of the x-axis, we reach the function with a vertical; the function takes the value $y_2 = r \times x_1(1 - x_1)$; and so on.

We take $r = 3.9$ and, $x_0 = 0.01$ for logistics map, the previous operations for 100 iterations are represented in Figure 1.

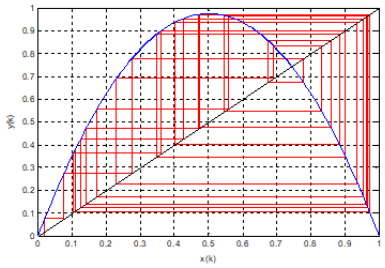

Figure 1: Evolution of y_k in function of x_k.

Figure 1 shows two signals y_k generated from the logistic map in chaotic mode ($r = 3.9$), one with an initial condition $x_0 = 0.1$ and the other with $x_0 = 0.100000000000001$ very close to 0.1.

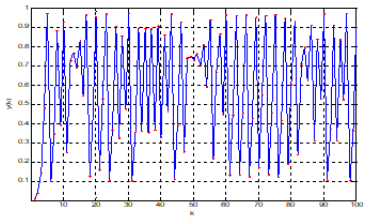

Figure 2: Chaotic regime in function of K.

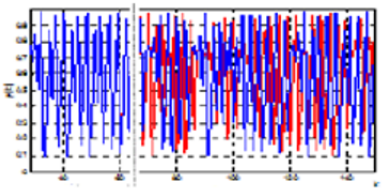

Figure 3: Sensitivity to initial conditions.

We note that a very small error in the knowledge of the initial state x0 in the phase space will be rapidly amplified and gives us two widely different signals. Quantitatively, the growth of error is locally exponential for highly chaotic systems (sensitivity to initial conditions). It should be noted that the initial condition error in this case is 10^{-15} and this is the smallest value because Matlab works with only 52 bits but the system can be sensitive to smaller values than 10^{-15} depending on the work environment.

3.2. Encryption Process

First of all, we choose randomly four data (a, b, c and d) from the logistic map to constate the lower triangular matrix of Toeplitz. The choice of the values of this data will be in agreement on the one hand with the encryption alphabet which is $\{0, 1, 2,$ and $3\}$, and on the other hand with the validity of the encryption 2.3. and decryption equations 3.3.

Equation 3.3 cannot be valid only if we work in an algebraic field, unfortunately, $Z/4Z$ is not an algebraic field. The solution of this problem is to use the $Z/5Z$ switching body (5 is a prime number), (all its non-zero elements are invertible, we take into account the following condition if we have 0 as the pixel value or the value of the elements of the Toeplitz matrix, we put 4), 4 is the inverse of 4 in $Z/5Z$ [9] [10]. Also knowing that 4 is equal to 0 modulo 4.

- Generation the elements of the Toeplitz matrix
- The plaintext vector is $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$,
- Take into account the following condition if we have 0 as the pixel value or the value of the elements of the Toeplitz matrix, we put 4 [9] [10].
- Calculate the cryptogram vector is $Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$ following the next equation

$$\begin{cases} y_1 = & ((a \times x_1 \times \mathrm{mod}(5))\mathrm{mod}(4)) \\ y_2 = & ((b \times x_1 + a \times x_2 \times \mathrm{mod}(5))\mathrm{mod}(4)) \\ y_3 = & ((c \times x_1 + b \times x_2 + a \times x_3 \times \mathrm{mod}(5))\mathrm{mod}(4)) \\ y_4 = & ((d \times x_1 + c \times x_2 + b \times x_3 + a \times x_4 \times \mathrm{mod}(5))\mathrm{mod}(4)) \end{cases} \tag{3.2}$$

3.3. Decryption Process

First of all, we choose randomly four data (a, b, c and d) from logistic map to constate the lower triangular matrix of Toeplitz, with the same conditions used during encryption process.

- Generation the elements of the Toeplitz matrix.
- The cryptogram vector is $Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$
- Take into account the following condition if we have 0 as the pixel value or the value of the elements of the Toeplitz matrix, we put 4 [9] [10].
- Calculate the inverse of a modulo 5.

a	1	2	3	4
a^{-1}	1	3	2	4

- Calculate the plaintext vector is $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$ following the next equation

$$\begin{cases} x_1 = & ((\frac{1}{a} \times y_1 \times \mathrm{mod}(5))\mathrm{Mod}(4)) \\ x_2 = & ((\frac{1}{a^2}(a \times y_2 - b \times y_1) \times \mathrm{mod}(5))\mathrm{Mod}(4)) \\ x_3 = & ((\frac{1}{a^3}(a^2 \times y_3 - a \times b \times y_2 - (a \times c_b^2) \times y_1) \times \mathrm{mod}(5))\mathrm{Mod}(4)) \\ x_4 = & ((\frac{1}{a^4}(a^3 \times y_4 - a^2 \times b \times y_3 - (a^2 \times c - a \times b^2) \times y_2) - ((a^2 \times d - 2 \times a \times b \times c + b^3) \times y_1) \times \mathrm{mod}(5))\mathrm{Mod}(\end{cases} \tag{3.3}$$

3.4. Example of Encryption of our cryptosystem

This numerical example demonstrates a simplified encryption and decryption process using Toeplitz matrices in a cryptographic system. In practice, more complex algorithms and security measures are employed, but this example serves to illustrate the concept of utilizing Toeplitz matrices in cryptographic key generation.

Exemple 1:

- Generation the elements of the Toeplitz matrix give us $a = 0$; $b = 3$; $c = 2$, and $d = 3$.
- The binary plaintext vector is$X = \begin{bmatrix} 10 \\ 11 \\ 01 \\ 10 \end{bmatrix}$, we convert X into decimal, then $X = \begin{bmatrix} 2 \\ 3 \\ 1 \\ 2 \end{bmatrix}$,
- • Take into account the following condition if we have 0 as the pixel value or the value of the elements of the Toeplitz matrix, we put 4: we change $a = 0$ to $a = 4$.
- Calculate the cryptogram vector is $Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$ following the next equation

$$\begin{cases} y_1 = & ((4.2 \times \mathrm{mod}(5))\mathrm{mod}(4)) = 3 \\ y_2 = & ((3.2 + 4.3 \times \mathrm{mod}(5))\mathrm{mod}(4)) = 3 \\ y_3 = & ((2.2 + 3.3 + 4.1 \times \mathrm{mod}(5))\mathrm{mod}(4)) = 2 \\ y_4 = & ((3.2 + 2.3 + 3.1 + 4.2 \times \mathrm{mod}(5))\mathrm{mod}(4)) = 3 \end{cases} \tag{3.4}$$

Then the cryptogram vector is $Y = \begin{bmatrix} 3 \\ 3 \\ 2 \\ 1 \end{bmatrix}$, we convert Y into binary, then $Y = \begin{bmatrix} 11 \\ 11 \\ 10 \\ 11 \end{bmatrix}$

Exemple 2:

- Generation the elements of the Toeplitz matrix give us $a = 3$; $b = 1$;$c = 0$, and $d = 0$
- The binary plaintext vector is$X = \begin{bmatrix} 00 \\ 01 \\ 01 \\ 11 \end{bmatrix}$, we convert X into decimal, then $X = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 3 \end{bmatrix}$,

- • Take into account the following condition if we have 0 as the pixel value or the value of the elements of the Toeplitz matrix, we put 4: we change $\mathsf{c} = 0$ to $\mathsf{c} = 4$; we change $\mathsf{d} = 0$ to $\mathsf{d} = 4$; we change $\mathfrak{x}_1 = 0$ to $\mathfrak{x}_1 = 4$;
- Calculate the cryptogram vector is $\mathsf{Y} = \begin{bmatrix} \mathfrak{y}_1 \\ \mathfrak{y}_2 \\ \mathfrak{y}_3 \\ \mathfrak{y}_4 \end{bmatrix}$ following the next equation

$$\begin{cases} \mathfrak{y}_1 = & ((3.4 \times \mathfrak{mod}(5))\mathfrak{mod}(4)) = 2 \\ \mathfrak{y}_2 = & ((1.4 + 3.1 \times \mathfrak{mod}(5))\mathfrak{mod}(4)) = 2 \\ \mathfrak{y}_3 = & ((4.4 + 1.1 + 3.1 \times \mathfrak{mod}(5))\mathfrak{mod}(4)) = 0 \\ \mathfrak{y}_4 = & ((4.4 + 4.1 + 1.1 + 3.3 \times \mathfrak{mod}(5))\mathfrak{mod}(4)) = 0 \end{cases} \tag{3.5}$$

Then the cryptogram vector is $\mathsf{Y} = \begin{bmatrix} 2 \\ 2 \\ 0 \\ 0 \end{bmatrix}$, we convert Y into binary, then $\mathsf{Y} = \begin{bmatrix} 10 \\ 10 \\ 00 \\ 00 \end{bmatrix}$

3.5. Encryption Key

Secret key field: In the proposed algorithm, the secret key field is set as follows:
$\mathsf{ST} = \{\mathsf{X}_0, \mu, \mathsf{F}, \mathsf{K}\}$.
The initial state of the logistics map $\mathfrak{x}_0 = 0.1$, $\mu = 3.9999$, $\mathsf{F} = 10^7$, the encryption key can be represented by the following fields:

- X_0
- μ
- F: scalar
- K: starting point or the starting moment k, where we begin to do the encryption/decryption.

Where X_0, μ are double-precision numbers. K are integer constants. If the precision of calculating X_0, μ, is 10^{15}, and $\mathsf{K} \in [1, 1000]$. Therefore, the key space is larger than $10^{15} \times 10^{15} \times 10^7 \times 10^3 = 10^{40}$ (with $10^3 \approx 2^{10}$) in this case we will have a key field of the order of 2^{133}. We have 133 bits larger of key.

4. Conclusion

In this paper, we have embarked on a journey to explore the untapped potential of Toeplitz matrices within the realm of cryptographic systems. Our research has yielded new and significant results that underscore the significance of Toeplitz matrices in enhancing the security of cryptographic protocols. As we draw our study to a close, several key takeaways and contributions emerge: Our cryptosystem has 133 bits larger of key, this number is huge. Therefore, the encryption algorithm has a very large key space to withstand all kinds of brute force attacks.

Declaration

This study does not require ethics committee approval.

Conflict of Interest

There is no conflict of authors in this work.

References

[1] R. Lidl and H. Niederreiter, "Finite Fields," Chapter 11: "Toeplitz Matrices and Pseudorandom Sequences." 1
[2] D. Schonhage and A. Strassen, "Schnelle Multiplikation großer Zahlen," Computing, vol. 7, no. 3-4, pp. 281-292, 1971. 1
[3] E. D. Karnin, "Efficient Randomized Algorithms for Toeplitz Systems," Journal of Computer and System Sciences, vol. 12, no. 2, pp. 252-261, 1976. 1
[4] P. J. Smith and P. C. Teh, "Encryption using Toeplitz and Hankel matrices," Journal of Cryptology, vol. 5, no. 3, pp. 189-200, 1992. 1
[5] P. Elias, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 4-12, 1967. 1
[6] N. J. A. Sloane and S. G. Hart, "On the existence of extended perfect codes," IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 383-386, 1978. 1
[7] Devaney, L. (1992) A First Course in Chaotic Dynamical Systems, Westview Press (Oct. 21st, 1992), Edition, 321 pages, Studies in Nonlinearity, ISBN: 9780813345475. 3.1
[8] Gleick, J. (1987) "Chaos: Making a New Science", Albin Michel edition, 420 pages. 3.1
[9] Hana Ali- Pacha, Naima Hadj-Said, Adda Ali-Pacha, "Data Security based on Homographic Function" Pattern Recognition Letters, Volume 129, January 2020, Pages 240-246. https://doi.org/10.1016/j.patrec.2019.10.032. 3.2, 3.3
[10] Hana Ali-Pacha, Naima Hadj-Said , Adda Ali-Pacha and Özen Özer," Significant role of the specific prime number p = 257 in the improvement of cryptosystems", Notes on Number Theory and Discrete Mathematics, DOI: 10.7546/nntdm.2020.26.4.213-222, Vol. 26, No. 4, pp. 213–222, December 2020. http://nntdm.net/volume-26-2020/number-4/213-222/. 3.2, 3.3