ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **11** (2022), no.12, 1361–1378
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.11.12.13

SHARING KEYS USING CIRCULANT MATRICES AND LOGISTIC MAPS THROUGH QUANTUM CHANNAL

Adoui Salah, Brahim Benzeghli[1], and Lamnouar Noui

ABSTRACT. To ensure confidentiality and avoid humain attacks against our data, we exchange encryption and decryption keys. In our proposal scheme, we use the commutative properties of the product of circular matrices to create a common encryption key by applying the protocol of *Diffie-Hellman* exchange through a classic channel. To raise the security level of our system we have introduced the sensibility of chaotic logistic maps in another exchange protocol which is the $BB84$ throuth a quantum channal.

INTRODUCTION

In an encryption symmetric system, the sender and receiver of a message share the same key, which is used for encryption and decryption. however, the asymmetric system uses two keys, a public key to encrypt messages and a private key for decryption.

[1] *corresponding author*

2020 *Mathematics Subject Classification.* Cryptology, Algebra, Arithmetic.

Key words and phrases. Circulant matrices, Logistic maps, Encryption, Decryption, Quantum cryptography, Deffie-Hellman protocol, $BB84$ protocol.

Submitted: 28.11.2022; *Accepted:* 13.12.2022; *Published:* 28.12.2022.

Symmetric key systems are simpler and faster, but their main drawback is that both sides must remain secure. Public key encryption avoids this problem, because the public key can be distributed in an insecure way, and the private key will never be transmitted.

Symeric key cryptography is sometimes called secret key cryptography. Here, we are working to share two desired encryption keys [6].

The first one will be a square matrix of ordre n generated by the terms of a chaotic logistic map [10] after having shared two parameters which we obtained through a quantum channal that uses a protocol known as quantum exchange $BB84$.

The one-dimensional logistic maps used has interest properties, such as: periodicity and sensitive dependence on the initial values, but its securty is weak. To overcome the inconvenience of its small key space, we can use several logisic maps to generate the key in the first step.

Then, with the encryption scheme based on the ideas of Diffie and Hellman [1], the famous protocol for changing keys, that we used to create the second key from the first based on the commutativity of the circular matrix multiplication. This last key will be used to encrypt and decrypt a text or image using a proposed formula.

1. Key exchange protocols in Cryptography

Cryptology is the science of secrecy, it's the study of mathematics techninques that are used to accoplish several goals to ensure the security of our communications, these goals are:

- The confidentiality of the data;
- The integrity of the data;
- The self-identification of data and communications;
- The none-repudiation of data.

The science of cryptoplogy is embodied in two distinct branchs, but interrlated:

- **Cryptography:** That proposes solutions to ensure the secret. it has two types:
  - **Asymmetric cryptography:** two different keys to encrypt and decrypt a text or an image.

  - **Symmetic cryptography:** The same key for encryption and decryption.
- **Cryptanalyses:** Which seeks to revial the weaknesses of these systems.

Cryptography uses modern cryptographic algorithms and concepts from many fields as " *Computer science, electronics, and specially in applied mathematics using for example: algebraic structures, elliptic curves, matrices, polynomials, . . .* ", used for determine a great possible value for a security variable, and this value is called the key secret. To determine this key, it is necessary to use techniques more secure and compliant against attaks, these techniques are called the key exchange protocols.

A cryptographic protocol is a communication protocol that uses cryptography tools to achieve a security goal to develop a common secret key. Each protocol is based on special mechanismes, there are protocols that are based on polynomials for example: *Protocol Bloom KPS, Protocol of Shamir, Protocol of Lagrange,* there are protocols based on the problem of discret-logarithm called *Diffie-Hillman protocol*. In this last one, the calculs are very simple, faster and very secure in the same time.

In our system, we detail how we can obtain a secret key by this protocol using the properties of circular matrices for encrypting and decrypting images.

The question is: Can we ensured the security of this protocol? For this, to raise the security levels of our system, we have intoduced *chaotic logistic maps* with *quantum cryptography* which is based on the use of two channals.

Quantum channal: through were objects governed by the laws of quantum mechanincs transit quantum and classical channals. There are several protocols of quatium cryptography, the famous one is $BB84$ which uses the polarisation of photons (this is the first protocol of quantum key distribution). The goal of the $BB84$ protocol proposed by *Charles Bennett* and *Gilles Brassard* in 1984, is to allow two users to exchange a random and secret key.

2. Logistic maps

Sine 1930 iterated maps are considered very important in many fields such as in population biology, encryption,. . . . One of most famous maps is the *logistic map*.

A logistic map is a simple example of the sequence which recurrence is not linear. Often cited as an example of complexity which can appear as a simple non-linear relation, this reccurence was popularized by the biologist *Robert* in 1976. His relationship reccurence is:

$$x_{n+1} = \mu x_n(1 - x_n)\ ;\ 3 < \mu < 4. \tag{2.1}$$

It leads, according to the values of μ to a convergent sequence, a continuation subject to oscillation or a chaotic sequel.

Towards $\mu = 3.57$, the chaos settles. No oscillation is still visible and slight variations in the initial population lead to a radically different differences.

Sensitivity to initial conditions: [8]. We can see that a very small changes in the initial state can lead to behaviors radically different in their final state, as in the following example (see Figure 1).

The two graphs correspond to the variation of the same sequence (x_n) defined in (2.1). If we fixe the parameter $\mu = 3.90$ and take two initial values x_0 and x'_0 withe a little changing in its values (in the ordre of 10^{-2}). In our example we have chosen $x_0 = 0.100$ and $x'_0 = 0.99$.

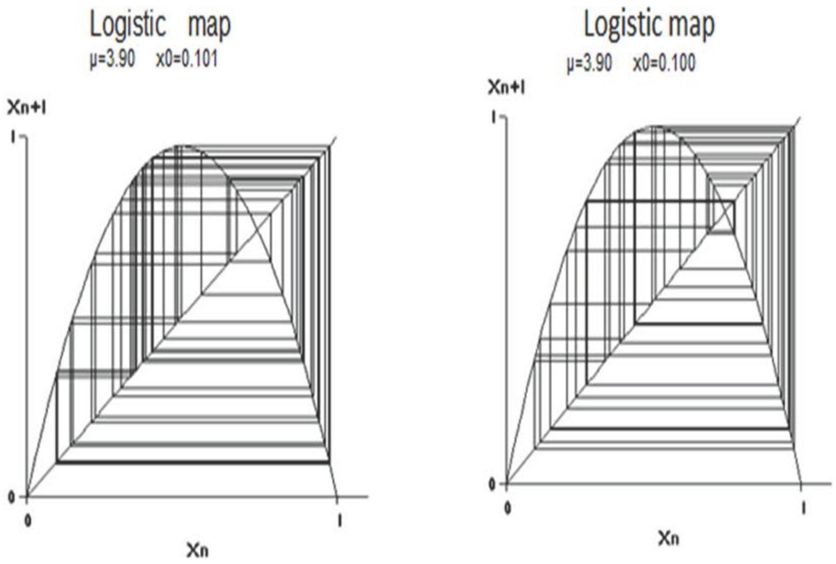


FIGURE 1. State of a logistic map with very small changes in the initial state

In Figure 1, we observe that the two sequences trajectories move away from the begining until some orders n_c for the first case and n'_c for the other, the acceleration become massive and we get a chaotic phenomenon.

In a concrete problem the initial conditions are never known exactly: after a certain time, a chaotic phenomenon became unpredictable even though the law that defines it is perfectly deterministic.

3. Quantum Cryptography

Quantum cryptography is the use of the properties of quantum physics to establish cryptographic protocols that achieve levels of security that are proven or conjectured not attainable using only conventional phenomena [12].

An important example of quantum cryptography is the quantum distribution of keys, which allows to distribute a secret encryption key between two remote interlocutors, while ensuring the security of transmission through the laws of quantum physics and information theory. This secret key can then be used in a symmetric encryption algorithm to encrypt and decrypt confidential data.

The different quantum cryptography protocols:

There are several quantum cryptography protocols. We often present the one developed by Bennet and Brassard in 1984, which uses photon polarization. We refer to it as the $BB84$ protocol. The $E91$ protocol was conceived by *Artur Ekert* in 1991. It uses a pair of entangled photons and therefore relies on the EPR effect well highlighted by the experiments of *Alain Aspect* and his colleagues. Applications of quantum cryptography Quantum cryptography has been out of the realm of theory for years, it is not a laboratory curiosity because it has already been put into practice, for example, and for the first time in 2004 for a major financial transaction requiring absolute security and in 2007 when the Swiss company *id Quantique* transmitted the results of the national elections in Geneva.

Obviously, quantum cryptography is of great interest to the military. *Darpa* (the American agency for advanced military research) has been using a quantum key distribution network since 2004. The European Union is not left out because in response to the Echelon spying program, it was at the origin of the Secoqc network.

The quantum properties of a polarized photon:

The quantum cryptography protocol is based entirely on the quantum properties of polarized photons. Knowing and understanding these properties is essential to understanding quantum cryptography [9].

(1) A photon can be polarized on any axis.

(2) A photon polarized on an angle axis a passing through a b axis polarizing filter has a chance equal to $\cos^2(b-a)$ to pass the polarizing filter [7]. So:

- if the filter is oriented precisely in the photon polarization axis $(b=a)$, the photon will certainly pass through the filter

$$(proba = \cos^2(b-a) = \cos^2(0) = 1).$$

- if the filter is oriented 90^0 from the photon polarization axis $(b = a + 90)$, the photon will certainly be stopped by the filter

$$(proba = \cos^2(b-a) = \cos^2(90) = 0).$$

- if the filter is oriented 45° from the photon polarization axis $(b = a + 45)$, the photon will have a 50% chance of passing the filter

$$(proba = \cos^2(b-a) = \cos^2(45) = \frac{1}{2}).$$

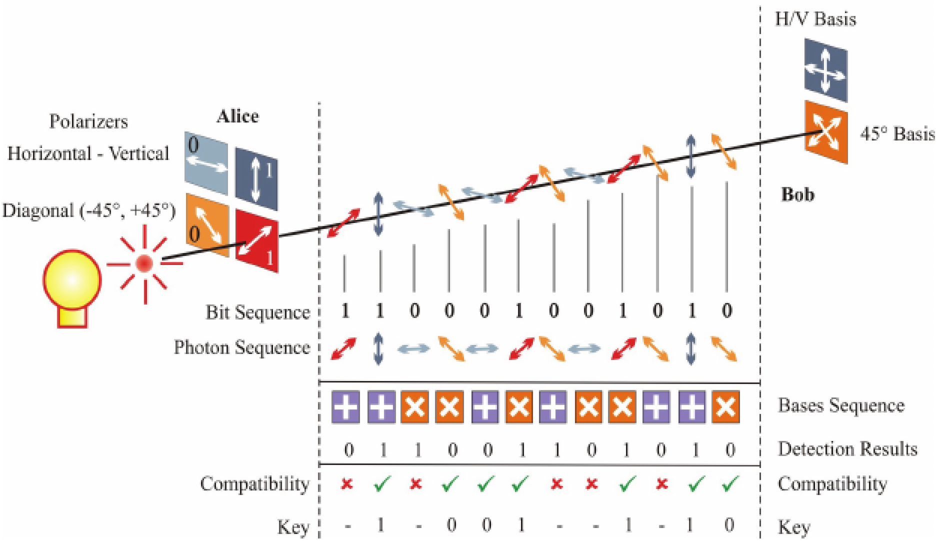


FIGURE 2. The Quantum Key Distribution System using $BB84$ Protocol

(3) The above properties are still in the "classic" domain [11]. The purely quantum properties used by quantum cryptography are:
- When the probability of passing the filter is neither 0 nor 1, the passage of an individual photon through the filter is fundamentally unpredictable and indeterminist.
- The polarization axis can only be known by using a polarizing filter (or more generally, by making a measurement whose result is YES or NO). There is no direct measurement, giving an angle for example, of the polarization axis of the photon.
- The initial polarization axis of the photon can only be known if the filter axis is precisely oriented at 0^0 or 90^0 relative to that of the photon. In the case where the filter is transverse (45^0 for example), there is basically no way of knowing what the initial polarization axis of the photon was.

Key Transmission Protocol. The key to transmit is a series of random bits, thus taking as value 0 or 1.

The emitter of the key codes each bit of the key in one of two polarization modes, randomly, at the choice of the emitter:

- **Mode 1:** 0 is encoded by a 0^0 polarization axis photon and 1 by a 90^0 polarization photon.
- **Mode 2:** 0 is encoded by a 45^0 polarization axis photon and 1 by a 135^0 polarization photon.

The transmitter emits the bit-by-bit, photon-by-photon key, randomly choosing the polarization mode (Mode 1 or Mode 2) for each emitted photon. The transmitter notes for each bit the selected polarization mode. Each photon is emitted at regular intervals.

The receiver has a polarizing filter, which can be oriented at will at 0^0 or 45^0. Before the expected arrival of a photon, it positions the filter, also randomly, at 0^0 or 45^0. When the photon arrives, it notes the result (the photon has passed the filter, or the photon has not passed the filter), as well as the chosen orientation of the filter.

For each bit, two scenarios are possible:

(1) The transmitter and receiver have randomly chosen the same polarization orientation. This happens every other time. In this case, the received photon is representative of the emitted bit and can be translated directly into bit.

(2) The transmitter and the receiver have chosen a separate orientation of 45^0, and in this case the received photon is perfectly random and contains no information.

Once all the bits have been transmitted (at least $2.N$ bits must be emitted for a useful $N-$bit key), the transmitter communicates to the receiver, by conventional means and not necessarily reliable, the polarization mode used for each bit.

The receiver can then know which bits have the same polarization orientation. It knows that these bits are not random. It thus knows in a certain way N bits on average for $2.N$ bits transmitted.

So far, this protocol is only a (very complicated) way of communicating random N bits from point A to point B. What is the advantage of doing this? The advantage is that the receiver can have absolute certainty that the key, or part of the key, has not been intercepted by a spy.

This is possible because, in case a receptor chooses a wrong orientation for the filter, the received photon is perfectly random and gives no information on its initial orientation. A possible spy is also obliged to use a polarizing filter to know the orientation state of the photon that encodes the bit value. To go unnoticed, it must re-emit a photon, with the same state of polarization as the received photon. But if the spy has chosen a wrong orientation of the filter to receive the photon (this happens on average every other time), he will reissue a photon in a random state. In the case where there is a spy on the line, it can happen the case where the receiver receives a different bit of the emitted bit when the transmitter and receiver have chosen the same polarization axis. This never happens (technical problems aside) when the quantum state of the photon is preserved from one end of the line to the other.

Therefore, to test the security of the key, the transmitter will, after communicating the polarization modes used for each photon, also communicate the value of a number of bits [11,12] for which the transmitter/receiver orientations are the same. These bits are therefore "sacrificed" since they are communicated by an unsafe channel. If only one of these bits differs between the transmitter and the receiver, the key is discarded and the process is restarted.

4. CIRCULANT MATRICES

Assum that k is a field ($k = \mathbb{R}$ or $\mathbb{C}$).

In linear algebra, a circulant matrix A is an element of $\mathcal{M}_n(k)$ generated by one vector $V(a_1 a_2 \cdots a_n)$ where $a_1 a_2 \cdots a_n$ in this ordre are the elements of its first line, and the i^{th} line ($2 \leq i \leq n$) is the target of V by the translation which translate elements of V by $i - 1$ times as following:

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \tag{4.1}$$

We can note it:

$$A = \langle V \rangle = \langle a_1 a_2 \cdots a_n \rangle = C(a_1 a_2 \cdots a_n).$$

The most important properties of circulant matrices are cited the two following lemmas:

Lemma 4.1. *Let $A = C(a_1 a_2 \cdots a_n)$ and $B = C(b_1 b_2 \cdots b_n)$ be two circulant matrices of $\mathcal{M}_n(\mathbb{C})$, then*

$$A \times B = B \times A.$$

The proof of this lemma is given in [2,3,5].

Lemma 4.2. *Let A be an invertible circulant matrix, then A^{-1} is a circulant matrix too.*

The proof of this lemma is given in [2–5].

5. APPLICATION WITH A NEW SCHEME

5.1. **The idea.** Using the logistic maps, we choose an arbitrer couple (μ, x_0) where x_0 is the initial term of the sequence 2.1. Through the quantum channal and by applying the $BB84$ protocol, we share the encryption key (μ, x_0). And the two prospecters create the same circulant matrix generated by $\langle x_1, x_2, \cdots, x_n \rangle$, where $(x_1, x_2, \cdots, x_n)$ are the terms of the sequence (2.1).

Then, we will create and exchange an other key using the set of circulant matrices by applying the *Diffie-Hellman* protocol to get a second common key that will be used in the encryption and decryption.

The same idea can be realised using several logistic maps for getting a best level security.

In this work, it is assumed that the constructed matrix is invertible and if not, the initial parameters are selected again until an invertible matrix is obtained. It is noted that the probability of having an inverted matrix is greater than $\frac{1}{2}$.

Two people want to communicate each with other:

FIRST STEP:

Through the quantum channal.

(1) **Using one logistic map:**

- Let (μ, x_0) two parameters, where, $3 < \mu < 4$ and x_0 is the initial term of the sequence (2.1), this couple will be exchanged between the two interlocutors through the quantum channal using the $BB84$ protocol.
- After having exchanged (μ, x_0), we introduce the logistic map defined in (2.1) for getting the n terms $x_1, x_2, \cdots, x_n$.
- We create the matrix

$$Q = \langle x_1, x_2, \cdots, x_n \rangle = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_n & x_1 & \cdots & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & \cdots & x_1 \end{pmatrix}.$$

(2) **Using three logistic maps:**

- Let (μ_1, x_0^1), (μ_2, x_0^2) and (μ_3, x_0^3) three couples of parameters, where, $\{\mu_i : 3 < \mu_i < 4 \text{ pour } i \in \{1,2,3\}\}$ and $\{x_0^i : i \in \{1,2,3\}\}$ is the initial terms of sequences defiend as in (2.1), these couples will be exchanged between the two interlocutors through the quantum channal using the $BB84$ protocol.
- After having exchanged these three couples of parameters, we introduce the logistic map defined in (2.1) for getting the n terms of each

sequence:

$$\{x_1^1, x_2^1, \cdots, x_n^1\}\ ,\ \{x_1^2, x_2^2, \cdots, x_n^2, \cdots, x_{\frac{n^2-n}{2}}^2\}$$

and

$$\{x_1^3, x_2^3, \cdots, x_n^3, \cdots, x_{\frac{n^2-n}{2}}^3.\}$$

- We create the matrix

$$Q = \begin{pmatrix} x_1^1 & x_1^2 & x_2^2 & \cdots & \cdots & x_{n-2}^2 & x_{n-1}^2 \\ x_1^3 & x_2^1 & x_n^2 & \cdots & \cdots & x_{2n-4}^2 & x_{2n-3}^2 \\ x_2^3 & x_3^3 & x_3^1 & \cdots & \cdots & x_{3n-7}^2 & x_{3n-6}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ {x^3}_{\frac{n^2-5n+4}{2}} & {x^3}_{\frac{n^2-5n+6}{2}} & {x^3}_{\frac{n^2-5n+8}{2}} & \cdots & \cdots & x_{n-1}^1 & {x^2}_{\frac{n^2-n}{2}} \\ {x^3}_{\frac{n^2-3n+2}{2}} & {x^3}_{\frac{n^2-3n+4}{2}} & {x^3}_{\frac{n^2-3n+6}{2}} & \cdots & \cdots & {x^3}_{\frac{n^2-n}{2}} & x_n^1 \end{pmatrix}.$$

In the two case, we managed to build a matrix Q which will be the first secret commun key between the interlocutors; this key will also be used ti generate an other key through the classical channal by applying the protocol of *Diffie-Hellman*.

In the following table (see Table 1), we show the time required to run the key Q using one logistic map by *Matlab2009* on *PC-intel(R) Core(TM) i5-3470CPU@ 3.20GHz 3.20GHz*.

TABLE 1. Execution time of proposed method of generating the key Q

Size of the first key Q	225×225	256×256	400×400	500×500	512×512	960×960
Time required of our method	0.010919 second	0.013829 second	0.076993 second	0.152158 second	0.164088 second	1.277364 second

SECOND STEP:

Through the classical channal.

- Let Q be the previous matrix obtained during the first exchange.

- Each one of the two interlocutors choose a circular matrix of order n, let C_1 the matrix choosed by the sender and C_2 by the receiver.
- Each one send to the other a new matrix S_1 and S_2 through a classical channal such that:

$$\begin{cases} S_1 &= C_1 Q, \\ S_2 &= C_2 Q. \end{cases} \tag{5.1}$$

- The first person received S_2 and calculates:

$$K_1 = C_1 S_2.$$

Likewise the second person received S_1 and calculates:

$$K_2 = C_2 S_1.$$

Proposition 5.1. *The two interlocutors get the same key K, such that*

$$K = K_1 = K_2.$$

Proof. The commutativity of the product of circular matrices seen in Lemma 4.1 gives:

$$K_1 = C_1 S_2 = C_1 C_2 Q = C_2 C_1 Q = C_2 S_1 = K_2.$$

□

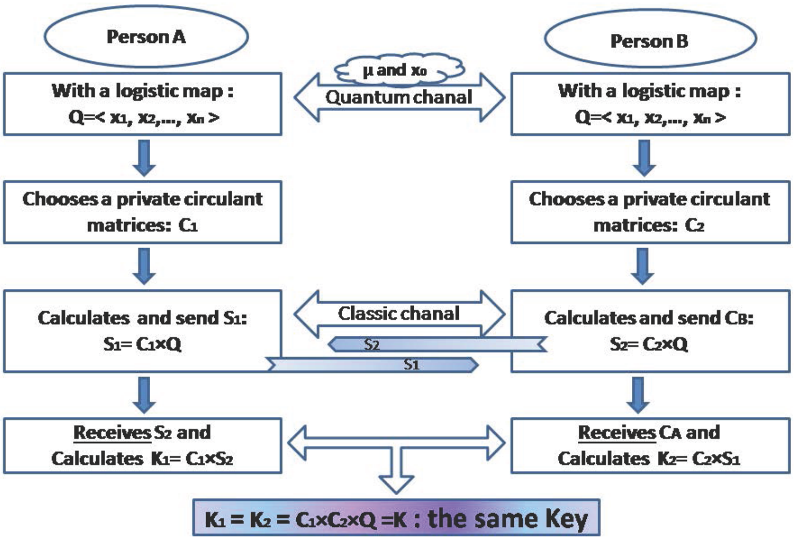

Person A
Person B
µ and x0
Quantum chanal
With a logistic map : Q=< x1, x2,..., xn >
With a logistic map : Q=< x1, x2,..., xn >
Chooses a private circulant matrices: C1
Chooses a private circulant matrices: C2
Calculates and send S1: S1= C1×Q
Classic chanal
S2
S1
Calculates and send CB: S2= C2×Q
Receives S2 and Calculates K1= C1×S2
Receives CA and Calculates K2= C2×S1
K1 = K2 = C1×C2×Q =K : the same Key

FIGURE 3. Block diagram of the procedure for creating a commun key

The previous diagram resum the operation how to create the commun keys through the quantic and classical chanal.

We have managed to build a matrix K which will be the secret commun key between the interlocutors; It will also be used to encrypt and decrypt.

In the following table (see Table 3), we show the time required to run the key K using *Matlab2009* on *PC-intel(R) Core(TM) i5-3470CPU@3.20GHz 3.20GHz*.

TABLE 2. Execution time of proposed method of generating the key K

Size of the second key K	225×225	256×256	400×400	500×500	512×512	960×960
Time required of our method	0.026830 second	0.029325 second	0.164801 second	0.337485 second	0.365084 second	2.803810 second

APPLICATION:

Encryption and Decryption of an image. Let I be an image of size $n \times n$ pixel, If some one want to send the image to an other person, he must convert it to a matrix of order n. Let G be the converted matrix, Q and K are the exchanged keys obtained previousely.

Encryption operation: The sender calculates and sends the encrypted matrix

$$H = KGQ.$$

Decryption operation: The receiver get H and calculates

$$H' = K^{-1}HQ^{-1},$$

to decrypt H and obtaines the intial matrix G correspending to the initial image I.

5.2. **Performance and security analysis.** To study the efficacy of our image incryption, we test its security. The proposed method should resist against several types of attacks, because its symmetric keys used during the encryption and the decryption must be transmitted through a secure channal and an other unsecured one.

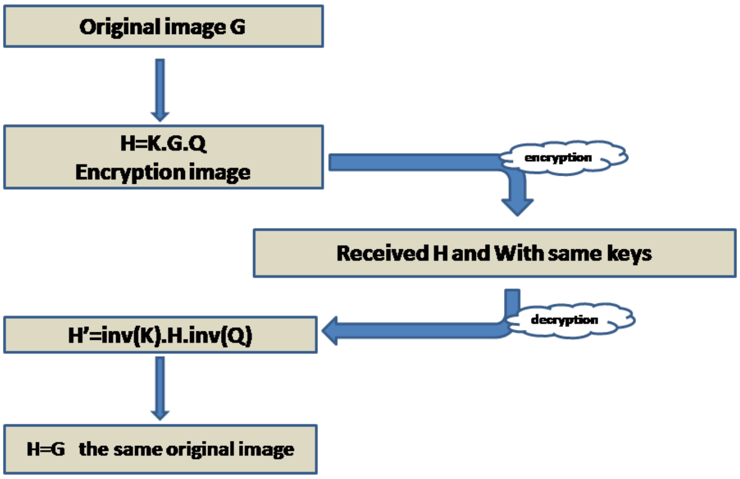


FIGURE 4. Block diagram of the encryption and decryption procedure

For the implementation of the proposed scheme, we choose the size of image $n = 256$ or $n = 512$. The proposed schem key K is none-deterministic, because the interlocutors use arbitrary circulant matrices $(C_1$ and $C_2)$ for getting a commun key K.

If we use the proposed key generation methode with

$$x_i \in \{0, \cdots, 255\};\ (x_i \textit{ are the composants of the key } K).$$

This provides uper then 256^{256} possible case to obtain the key K. We have also 10^{60} possible case for getting the key Q (with ten digits decimal after the comma) if we use three logistic maps.

The used 1-dimentional logistic map has intersting properties like periodicity and sensitivity of intial values, but it has a low security to overcome the inconvenience of its small key space, for these raison we choose in this phase to use several logestic maps to generate the key Q.

The key space size of our proposed scheme is greater then $256^{256} \times 256^{256} \times 10^{60}$ (for the formula $K = C_1C_2Q$) and the key space is wide enough for a brute force attack or exhaustive attack is not possible.

Tests to encrypt and decrypt some images. To confirm the level of security of the proposed system and its efficiency, in the operation of encryption and decryption of a digital image, we must test the three properties:

- Histogram;
- Entropy;
- Correlation.

Histogram. We know that the histogram of an image of an encryption system must be uniform if we have a good level of securty.

The proposed image encryption scheme is examined using the histogram. We used two test images, Camera-men of size 256×256 and Barbara of size 512×512. The histogram of our encrypted images is almost uniform and considerably different to the histogram of simple images that makes difficult statistical attacks (see Figure 5).

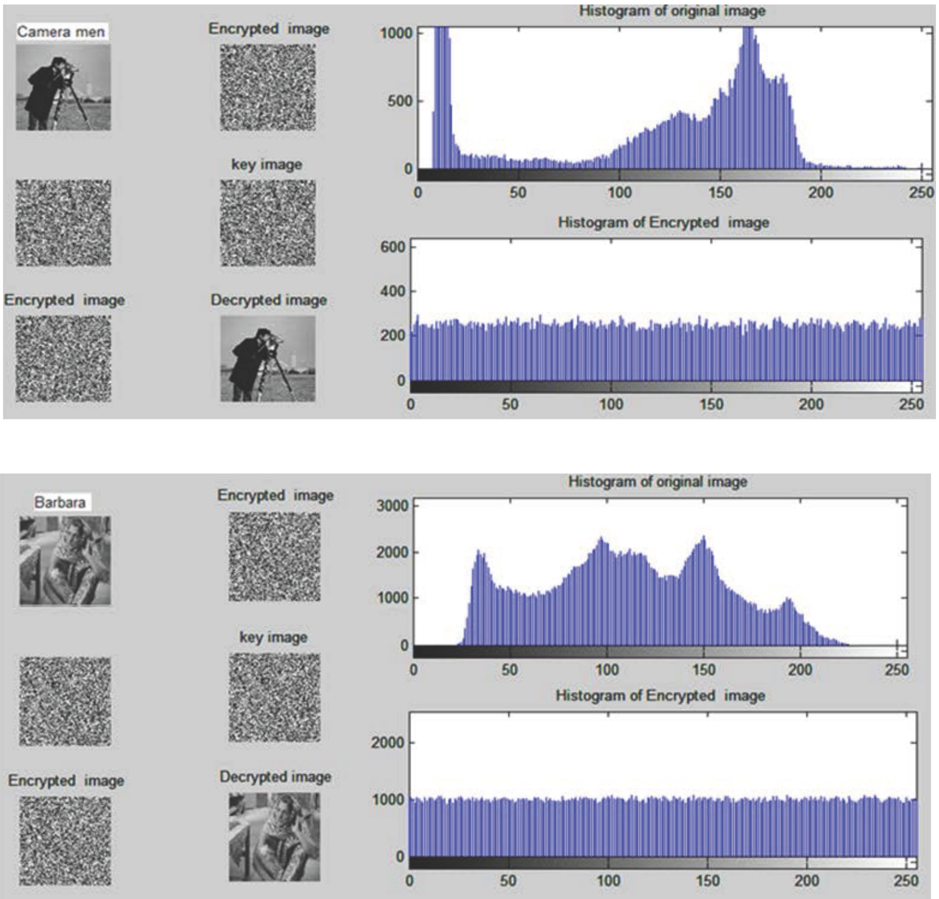


FIGURE 5. Encrypted and decrypted Barbara and Camera-men images and their correspended histogram of original and encrypted images

Entropy analysis of information. Entropy is one of the best functions for calculating and measuring character random of the encrypted image.

Ideally, the entropy of information should be $8-bit$ for grayscale images. If a scheme of encryption generates an output digit image with lower entropy at $8-bits$, then there would be a possibility of predictability, which can threaten his security. The entropy of information is calculated using the equation former. The simulation results for the entropy analysis concerning some images are presented in the table:

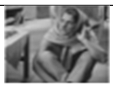
Encrypted images	images	size	μ	x_0	Entropy
Pepper		225×225	3.67	0.87	7.9966
Camera men		256×256	3.21	0.67	7.9977
Lena		256×256	3.57	0.47	7.9973
Im 400		400×400	3.57	0.47	7.9988
Im 500		500×500	3.47	0.33	7.9994
Barbara		512×512	3.59	0.41	7.9994
Im 960		960×960	3.30	0.28	7.9998

TABLE 3. Entropy results of some encrypted images

Correlation analysis of two adjacent pixels. Correlation determines the connection between two variables. In other terms, correlation is a measure that determines level of similarity between two variables. Correlation coefficient is a useful evaluation to judge encryption quality of any cryptosystem. Any image cryptosystem is said to be good, if encryption method hides all attributes and features of a plain text image, and encrypted image is totally random and extremely uncorrelated. For a regular image, each pixel is highly associated with its nearby pixels. An ideal encryption technique should generate the cipher images with no such correlation in the adjacent pixels. We have examined the correlation of two adjacent pixels in original image and encrypted image in several images like Pepper immage; Camera-man image; Lena image; Barbara, Im 400; $\cdots$ and we find theirs correlation very close to 1, we mean there is a perfect match between the original and decrypted images.

References

[1] E. Bresson, O. Chevassut, D. Pointcheval, J.J. Quisquater: *Provably authenticated group diffie-hellman key exchange.*, In Proceedings of the 8th ACM Conference on Computer and Communications Security, **CCS '01**, , New York, NY, USA, 2001, 255–264. Association for Computing Machinery.

[2] D. Canright, J.H. Chung, P. Stanica: *Circulant matrices and affine equivalence of monomial rotation symmetric boolean functions.*,Discrete Mathematics, **338**(12) (2015), 2197–2211.

[3] A. Carmona, A.M. Encinas, S. Gago, M.J. Jiménez, M. Mitjana: *The inverses of some circulant matrices.*,Appl. Math. Comput., **270**(C) (2015), 785–793.

[4] A. Carmona, A.M. Encinas, M.J. Jiménez, M. Mitjana: *The group inverse of some circulant matrices*, Linear Algebra and its Applications, **614** (2021), 415–436.

[5] L. Fuyong: *The inverse of circulant matrix*, Applied Mathematics and Computation, **217**(21) (2011), 8495–8503.

[6] S. Goldwasser, S. Micali: *Probabilistic encryption*, J. Comput. Syst. Sci., **28**(2) (1984), 270–299.

[7] A. Iqbal, M. Aslam, A. Hafiza, S. Nayab: *Quantum cryptography: A brief review of the recent developments and future perspectives*, **03**, 2016.

[8] A. Kanso, N. Smaoui: *Logistic chaotic maps for binary numbers generations*, Chaos, Solutions and Fractals, **40**(5) (2009), 2557–2568.

[9] A. Kawachi, H. Nishimura: *Communication complexity of private simultaneous quantum messages protocols*, 2021.

[10] M. Kumar, S. Kumar, R. Budhiraja, M.K. Das, S. Singh: *A cryptographic model based on logistic map and a $3-d$ matrix*, Journal of Information Security and Applications, **32** (2017), 47–58.

[11] A. Navarrete, M. Pereira, M. Curty, K. Tamaki: *Practical quantum key distribution that is secure against side channels.* arXiv: Quantum Physics, 2020.

[12] G. Zeng: *Quantum private communication*, Springer and Higher Education Press, 2010.

Department of Mathematics
University of Mustapha Ben Boulaid - BATNA 2
53, Constantine Street. Fésdis, Batna 05078,
Algeria.
Email address: s.adoui@univ-batna2.dz

Department of Mathematics
University of Mustapha Ben Boulaid - BATNA 2
53, Constantine Street. Fésdis, Batna 05078,
Algeria.
Email address: b.benzeghli@univ-batna2.dz

Department of Mathematics
University of Mustapha Ben Boulaid - BATNA 2
53, Constantine Street. Fésdis, Batna 05078,
Algeria.
Email address: nouilem@yahoo.fr