Journal of Computer and Communications, 2024, 12, 131-140
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Modeling and Implementation of a Data Security and Protection Medium Using the Generated Key Based on Electromagnetic Wave Propagation Theories

Vincent Mbonigaba[1], Fulgence Nahayo[2], Octave Moutsinga[3], Dieudonné Okalas-Ossami[3], Romeo Nibitanga[4], Thérence Niyonsaba[2]

[1]Doctoral School and Faculty of Science and Technology, University of Burundi, Bujumbura, Burundi
[2]LUMISTA-ISTA, University of Burundi, Bujumbura, Burundi
[3]URMI, Masuku University of Science and Technology, Franceville, Gabon
[4]CRIET-FSI, University of Burundi, Bujumbura, Burundi
Email: mbonivinci@gmail.com

How to cite this paper: Mbonigaba, V., Nahayo, F., Moutsinga, O., Okalas-Ossami, D., Nibitanga, R. and Niyonsaba, T. (2024) Modeling and Implementation of a Data Security and Protection Medium Using the Generated Key Based on Electromagnetic Wave Propagation Theories. *Journal of Computer and Communications*, **12**, 131-140.
https://doi.org/10.4236/jcc.2024.129008

Received: March 14, 2024
Accepted: September 23, 2024
Published: September 26, 2024

Abstract

Today, the advent of quantum computers and algorithms is calling into question the semantic security of symmetrical and asymmetrical cryptosystems. The security of objects connected to the network, which must provide a security service and protect the privacy of users by providing protection against attacks such as identity theft, denial of service, eavesdropping and unauthorised access to personal and sensitive data. It is therefore necessary to find a robust method of using the key that is effective in protecting and preventing data tampering. In this paper, we design and implement a security and data protection method using a key generated on the basis of electromagnetic wave propagation theories. Modelling and implementation of a data security and protection method using a key generated on the basis of electromagnetic wave propagation theories.

Keywords

Modeling, Security, Cryptography, Algorithm, Coding, Quantum, Post, Bytes, System, Waves

1. Introduction

For years now, human society has been profoundly thinking about digitization and the security of information systems [1]. It has virtually changed the way we do things, the way we think, the way we work, in short, the way we represent the

world and our social environment. Although the secret must lie in the algorithm used for the key, it must provide security services to protect users' privacy and guarantee protection against attacks [2]. We aim to protect the privacy of the customer's location as well as the privacy of ongoing requests [3], such as identity theft, denial of service, eavesdropping and unauthorised access to personal and sensitive data [4]. Worldwide, the degree to which digital technology has penetrated the social strata varies from place to place and from sector to sector, without forgetting that it has evolved and continues to evolve over time [5].

The security of communication between two interlocutors has always been an issue, as the use of erroneous information can lead to disastrous consequences, so lack of integrity is a serious problem. Consequently, the protection of information sent over networks against modification and interception is of the utmost importance [6]. It can be deduced from this that there is a considerable increase in data exchanges, and this implies a major demand for cryptographic protocols to secure the transmission of sensitive data [7]. One of the most effective solutions adopted today is cryptography. Cryptography serves not only to preserve data confidentiality, but also to guarantee data integrity, authenticity and non-repudiation [8], to transmit digital data over a noisy channel, ensure its protection against transmission errors and unauthorized access.

2. Modeling of the Data Protection System

The modelling of a data protection system is becoming a priority and inevitable element in communication between interlocutors. The cryptographic key that we have generated is imposed on malicious systems as well as on attacks from the environment.

Modelling a data protection system will allow us to have an encryption function and a decryption function (**Figure 1**). We have three equations, the first of which is reserved for modelling data encryption, the second for modelling the encryption key and the third for modelling data decryption.

$$M \equiv y^2 = 3x^3 + 2x^2 + 4x + 3 \tag{1}$$

Data encryption aims to improve the confidentiality of the flow of information from source to destination. This work is part of the context of modelling the form of the plaintext message before data encryption by proposing the development of the form of the message with the equation and the graph (**Figure 2**). In general, database encryption models and encryption key protection models facilitate the work of transmitting the message in full security (clear message) [9]

$$K \equiv y^2 = 2x^2 + 3x + 2 \tag{2}$$

Processors are omnipresent in the technologies that surround us. They compose and orchestrate the operation of data transmission systems. The consumer processors that equip our computers are only a very small part of the total number of processors in use. Data protection via the security key generated from the theory of electromagnetic wave propagation. Modelling the encryption key using an equation and a graph

is becoming an important element in data security [10] (Figure 3 & Figure 4)

$$C \equiv y^2 = 3x^3 + 4x^2 + 7x + 5 \tag{3}$$

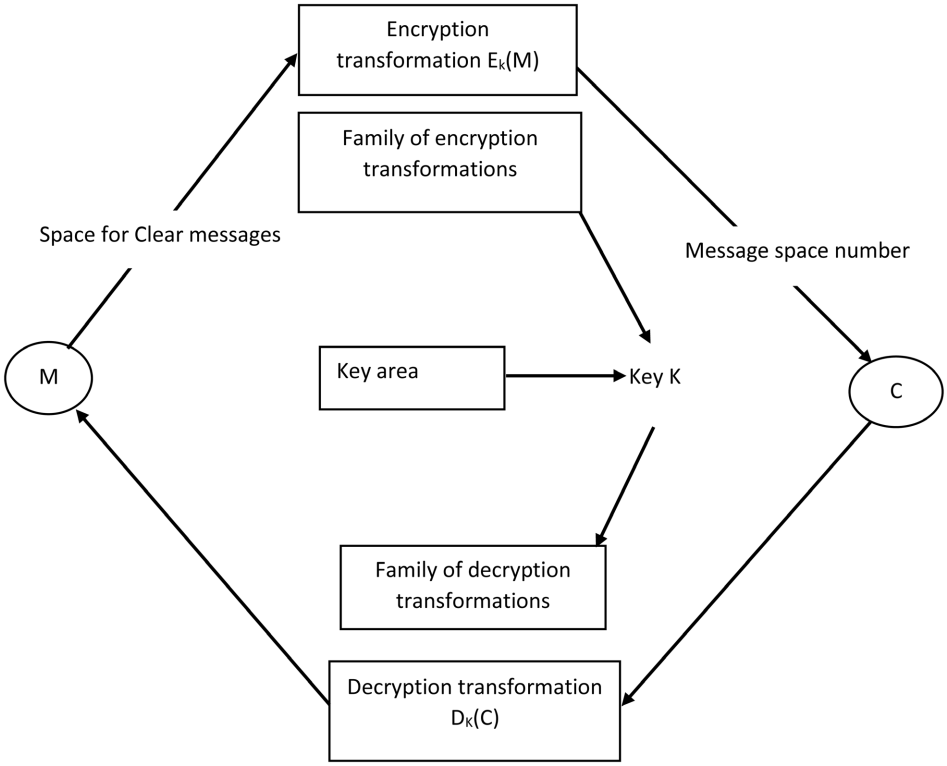


Figure 1. Modelling the data encryption and decryption process.

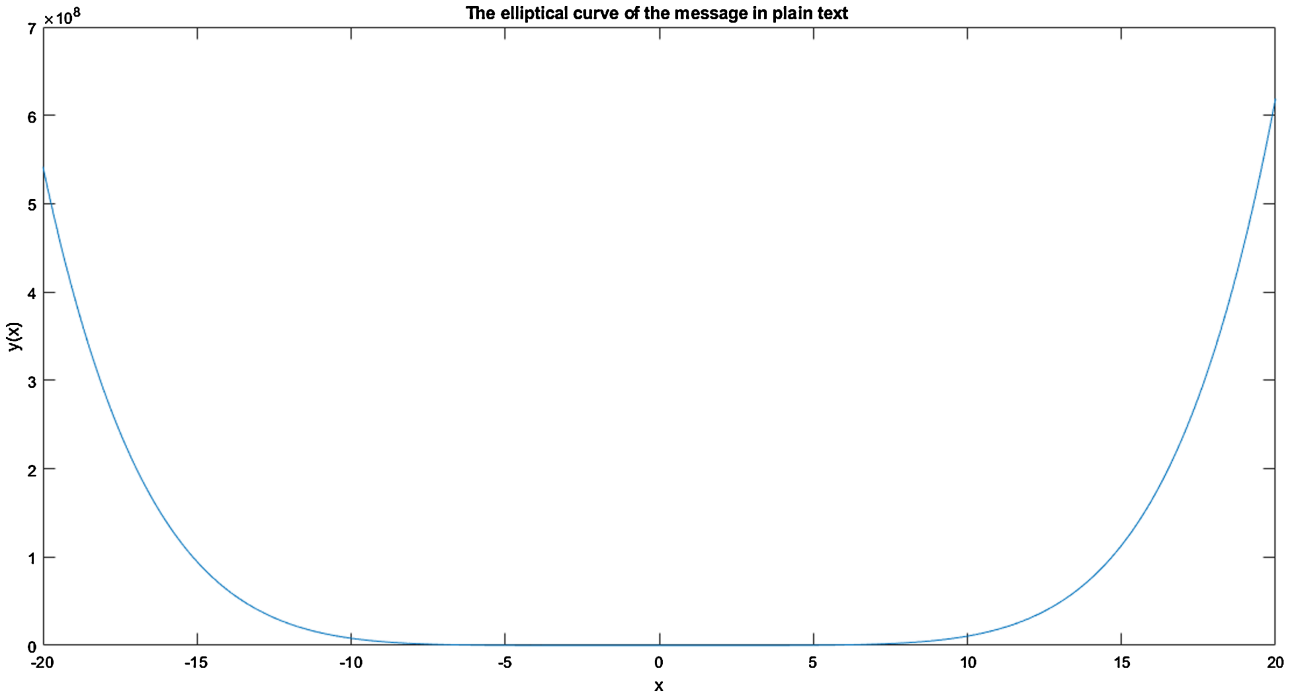


Figure 2. Modelling the plain text message.

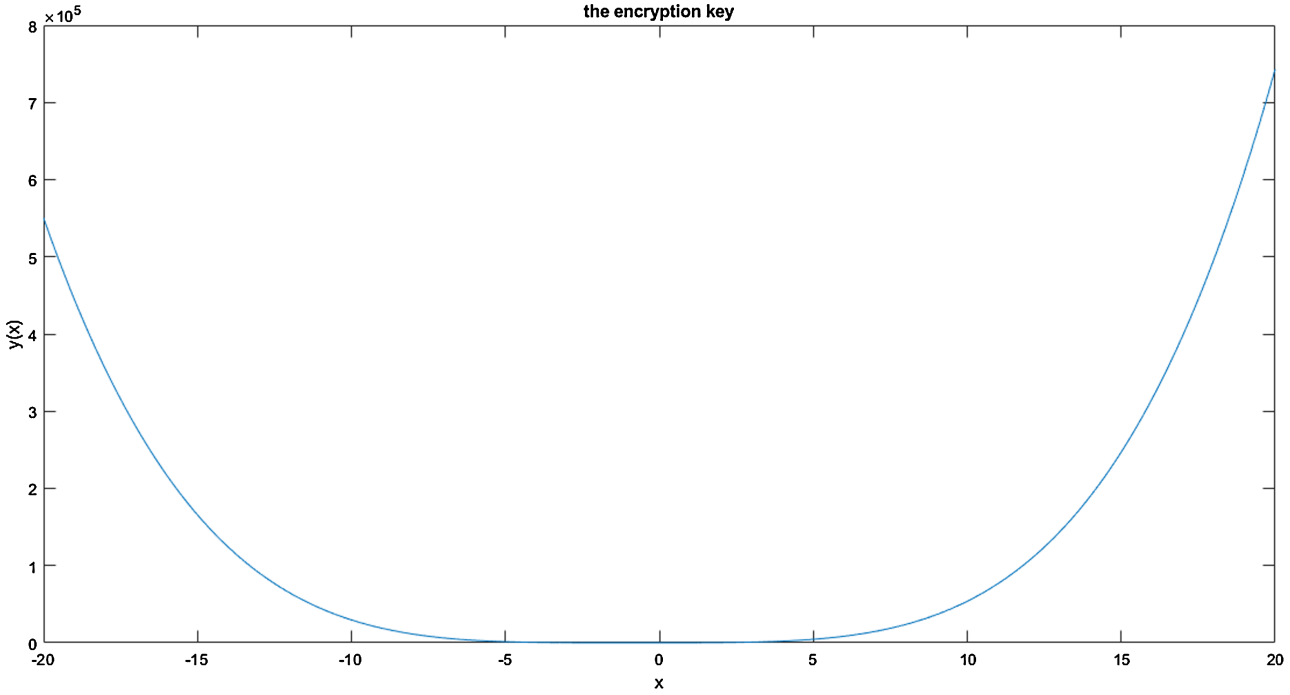


Figure 3. Modelling the encryption key.

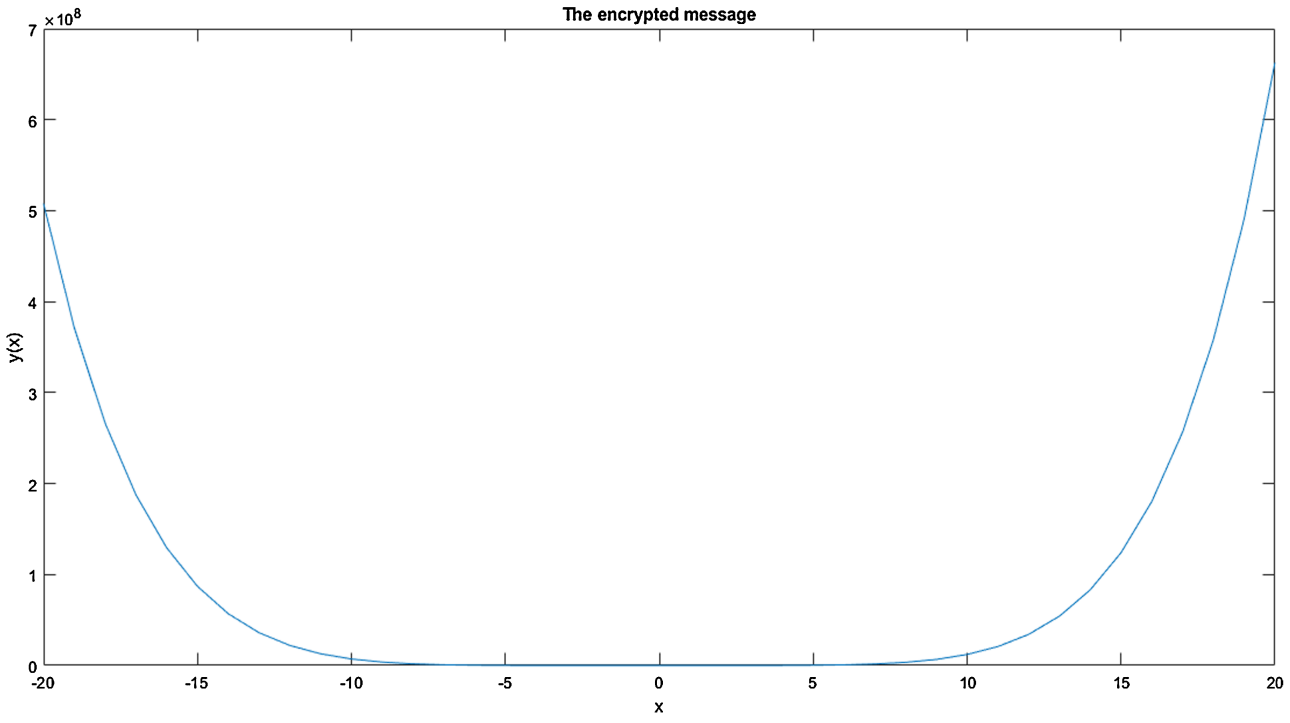


Figure 4. Secure message modelling.

The principle of encryption is becoming very important, but it is also a technique that enables mathematical operations to be carried out on previously encrypted data, without access to the data in clear text. In this context, only the owner of the data has the ability to decrypt the data, while guaranteeing the

confidentiality of the rest of the raw data, an authorised third party has the ability to extract selected information themselves. Recent advances in the encryption of information flows seem to offer new application prospects. We are particularly interested here in the proposed scheme based on an equation for modelling the encrypted message [11].

This article is based on the design and implementation of algorithms for protecting computer data, most of which is stored on terminals hosted by various companies and institutions, or exchanged via network transmission media. This algorithm is motivated by its unique use of the encryption key already generated through the theory of electromagnetic wave propagation. The java libraries will be used to implement the solution, as will Boole's mathematical logic, which was proposed by Shannon to verify the compatibility of the information lattice with quantities such as entropy, which measures a quantity of information.

Entropy is therefore compatible with the definition of information as an equivalence class, since two variables in bijection can have essentially the same law and therefore the same entropy. We then have obvious links as proposed in conditional entropy [12]. The entropy $E(a)$ of a discrete random variable a is presented as the amount of information contained in a, and the notion of mutual information $W(a; b)$ between two variables a and b.

$$a \le b \Leftrightarrow E(a \mid b) = 0. \tag{4}$$

In particular, H is "increasing" which gives the value of the greater information to a greater entropy:

$$a \le b \Leftrightarrow E(a) \le E(b) \text{ and } E(a) \ge E(0) = 0 \tag{5}$$

for

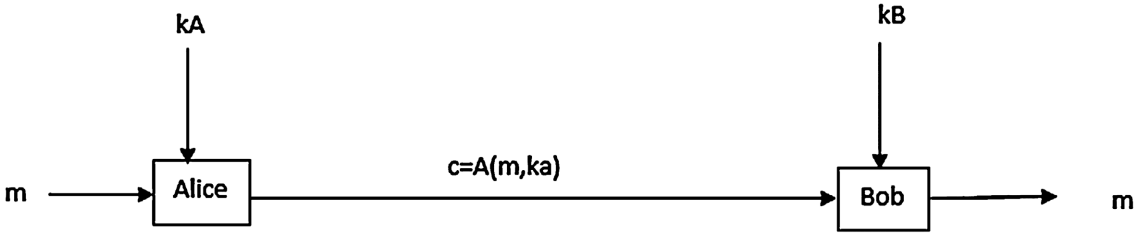


Figure 5. Modelling the secure communication process between Bob and Alice.

With

A: Alice

B: Bob

M: message space

C: cryptogram space

K: key space

This will enable us to have an encryption function and a decryption function

That is,

$$A = M * K \to C \tag{6}$$

which is an encryption function when the message is sent between the two parties, and

$$B = C * K \to M \tag{7}$$

which gives Bob a decryption function to find out the contents of the secret message. If two parties want to exchange information confidentially, they must first exchange a secret key securely. Once $kA = kB$, the encryption will be symmetrical with m being the clear message as defined in Figure 5, so the secret depends on k being the key, otherwise the messages at Alice's (A) and Bob's (B) are public.

3. Methods

As with information processing, *i.e.* retrieving data to extract information, several methods are used to encode and decode information. These methods are developing in parallel with the perpetual evolution of computer software and tools enabling information to be intercepted for third-party use, so we're talking about asymmetrical encryption, which is almost classic, and so-called modern symmetrical encryption. Among these commonly used methods, we'll mention symmetrical encryption, known as the secret n-key algorithm. This is a unique decoding method that must be provided to the recipient before the message can be decrypted. Security properties indicate that the data before and after encryption must be structured in the same way. We also observe that a limit increase in data size can be tolerated, so we rely on a symmetrical encryption method, so for a large amount of data to be used the asymmetrical decryption method is less widely used [13]. Asymmetric encryption, on the other hand, uses two different keys—public and private which are mathematically linked and therefore to some extent interdependent. In practical terms, the keys consist solely of large numbers that have been paired together but are not identical. In view of the above, we're going to set up a protection mechanism.

4. Implementation of the Result

We've managed to use the key we've generated from the theory of electromagnetic wave propagation, which is a secret key cryptosystem and therefore symmetrical. Since it will be used to secure the exchange of information between the various departments of a company or organization, data which is rarely transmitted via a public network, this algorithm has the advantage of being theoretically unbreakable, but also thanks to its unique use of the encryption key.

The crypto system will enable us to better secure our information, which will be very useful in crypto systems that use the attack-resistant algorithm in possession of quantum machines in order to remedy factorization and exponential problems. Here's the java code we used for this encryption.

5. Data Encryption Algorithm

Step 1. Initialise the string KT

Step 2. For i from 1 to a specified length
Step 3. Initialise the empty character string T
Step 4. For j from 1 to n
Step 5. Initialise the empty character string EM
Step 6. For i from 1 to n
Step 7. Initialise the empty character string DM
Step 8. For j from 1 to n
Step 9. Call the randbit function to add a random bit to the string
Step 10. Add string T to string KT
Step 11. Return the KT string containing the key
Step 12. Add KT to EM to find DM
Step 13. Return the DM string containing the encrypted message

6. Presentation and Discussion of the Results

6.1. Experienced Results

In this work, we have tried to use Vernam's algorithm, which belongs to the family of symmetrical algorithms based on secret-key encryption. The key is generated by the logical function XOR between magnetic induction and magnetic induction. Since it will be used to secure information exchanged between interlocutors with quantum computers, *i.e.* data rarely transmitted via a public network, this algorithm has the advantage of being theoretically unbreakable, but also thanks to its unique use of the encryption key. The key we've already generated from electromagnetic wave propagation theories is as follows [14]:

10100100011111011011011110101110110111010001001100101011011
00010100111011010000011010000100101010011000100100110001001
10011101000010010111001010100111011110110101110001000100010
10110000111110111000110010010100100011101110011111000000111
00110111000001101111010100111010111010011011111011111001101
01001010001101000010001100010111011101000001100001011011010
10000010111000010011011010010010001000111001001101010100110
11011111010101000010011011100100011010100101101001101110110
00100110111110111111000000010110100000000

The example of the message in clear is as follows: Hi Prof, I'm working on post-quantum cryptography.

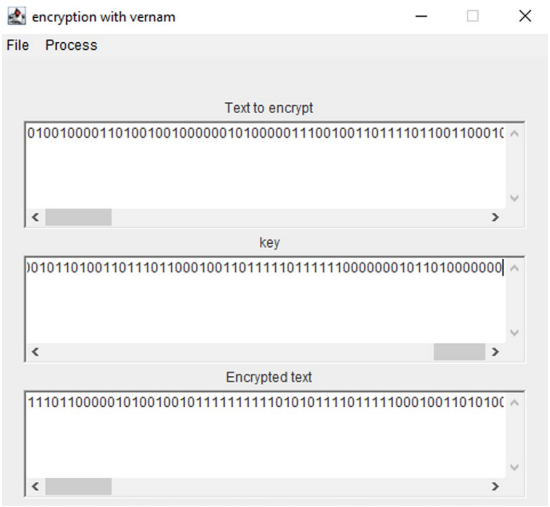
The message is encrypted using the key above:

11100110000100101101100111000100101100100110011001011001010
00010110011011101001010111111111110011000111010000011001101
10000010001000001011011111011101111100011000000011101110000
00011000100010001101010100010111101100111000000001001010100
00000010101000000000011001100101000111011111000100111011111
00011111001000001110000101001010010011001101001010001110000
11011001000110100010010100010000100111110001000101110100 11
00100001011011010110100000100001001000010001111001010011 10

00111110101011110001110100101010

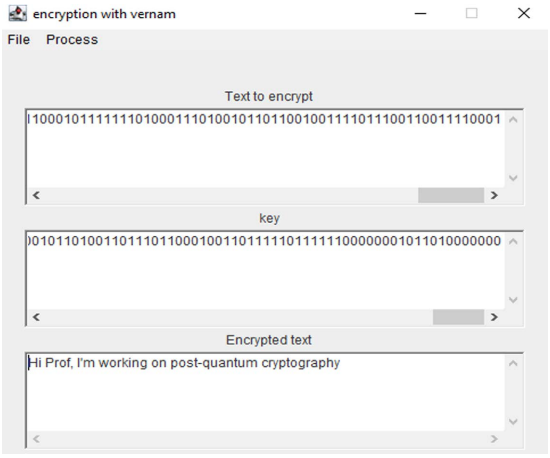
6.2. Clear Text

The plain text is the message at source Governments and companies spend a lot of money to ensure the security of their data. In spite of this, the data is still damaged. In the present work, Vernam's cryptographic system will be applied to data exchanged via optical fibers as a medium for transmitting information in communication systems, in order to render them incomprehensible, thus becoming unusable to interceptors. Python languages and web development will enable us to develop the algorithms that will be put forward, but also to put them into practice.



6.3. Plain Text Found Again

Governments and companies spend a lot of money to ensure the security of their data. Despite this, data can still be compromised. In this work, cryptography will be applied to data exchanged over optical fibers, making it incomprehensible to computer attacks and unusable by interceptors. Java and web development will enable us to develop the algorithms that will be put forward, as well as to put them into practice [15].



7. Discussion

We have managed to secure the information that will be exchanged between the various parties with the unbreakable key that will enable us to better secure our information, which will be very useful in the cryptosystems that use the security algorithm compared with the malicious systems in the possession of quantum computing machines in order to remedy the problems of factoring and exponentials. As the key is used once and only once, a disposable mask key, this last specificity will facilitate the transmission of data while respecting the security mechanisms, and therefore substantial reliability, which reinforces the security of the data to be protected and or defended against the threats of alteration or interception for malicious use.

8. Conclusions and Future Works

8.1. Conclusions

Information security is the lifeblood of the enterprise, but traditional IT security is neither flexible nor scalable enough to protect this new digital ecosystem. It is necessary to protect them with multiple protection systems, including Hadoop-assisted, cross-platform security, including data and information security infrastructure based on post-quantum cryptography systems. The present work focuses on enhancing the security of data rarely transferred via communication channels.

The use of verman's post-quantum cryptography key generation algorithm is suitable for securing this type of rarely transmitted and exchanged data and information, which is generally processed in read-only mode. Post-quantum cryptography is a very important element in securing information systems in different companies, but traditional IT security is neither flexible nor scalable enough to protect this new data in the digital ecosystem. Three parameters need to be ensured: data integrity, availability against attacks using a quantum computer, cross-platform support including data and information security infrastructure based on cryptographic systems.

8.2. Future Works

The implementation of security mechanisms against attacks from the environment between different interlocutors weakens computer systems in different companies. The aim of this article is to model and implement data security between different communicators using a key generated from the theory of electromagnetic wave propagation. In future work, we will proceed to use this key to secure transactions in mobile payments, and then we will see to what extent the transmission of this key is secure against malicious systems.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Besençon, S. (2022) Encoding Information Security between Maintenance and Innovation: The Case of OpenPGP. RESET. Social Science Research on the Internet.

[2] Sammoudi, A., Hamdi, O., Chalouf, M.-A. and Montavont, N. (2022) The Contributions of Biometrics and Artificial Intelligence in Securing the IoT. In: Chalouf, M.-A., Ed., *Intelligent Security Management and Control in the IoT*, Wiley, 197-221. https://doi.org/10.1002/9781394156030.ch8

[3] Aloui, A. (2020) A Security Approach for M-Business. Doctoral Dissertation, Universite Mohamed Khider de Biskra.

[4] Dumont, R. (2010) Cryptography and Computer Security. PhD Thesis, University of Liège.

[5] Korba, K.A. (2022) Security of Wireless Multimedia Networks Using Choatic Systems. PhD Thesis, Université 08 mai 45 Guelma.

[6] Rioul, O., Béguinot, J., Rabiet, V. and Souloumiac, A. (2022) Shannon's True (and Little-Known) Theory of Information. 28*e Colloque GRETSI*'22, Nancy, September 2022, 1-5.

[7] (2022) Protection of Economic Information in French-Canadian Law, the Right to Confidentiality and the Right of Access to Information for the Public Case of Whistleblowers.

[8] Labayle, H., Poelemans, M., Dupin, B., Durand, T., Andreu, T., Batcho, O., *et al.* (2024) Annuaire de droit de l'Union européenne. In: Blumann, C. and Picod, F., Eds., *Annuaire de droit de l'Union européenne*, Éditions Panthéon-Assas, 509-566. https://doi.org/10.3917/epas.bluma.2023.01.0509

[9] El Bouchti, K. (2020) Database Security: Data Encryption and Key Protection Models. Thèses et Mémoires, Université Mohammed 5 de Rabat.

[10] Laborde, T., Gensse, A., Chartier, P., Lemou, M., Méhats, F., Chaillan, F. and Gicquel, C. (2023) Application of Functional Encryption on Confidential Data for the Design of Machine Learning Models. *Conference on Artificial Intelligence for Defense*, Rennes, November 2023, 1-8.

[11] Elalouf, J. (2022) Choc et entropie: Walter Benjamin et la théorie de l'information. Design, Arts, Médias, Systèmes: Logiques, Graphies, Matérialités. https://journal.dampress.org/issues/systemeslogiques-graphies-materialites/choc-et-entropie-walter-benjamin-et-la-theorie-de-linformation. ffhal04370925

[12] Traore, M. (2022) RNG Bias Analysis for Cryptographic and Industrial Mechanisms. PhD Thesis, Université Grenoble Alpes.

[13] Puech, W. (2022) Multimedia Security 2: Biometrics, Video Surveillance and Multimedia Encryption. Wiley.

[14] Mbonigaba, V., Nahayo, F., Moutsinga, O. and Dieudonné, O. (2024) Development of a Post Quantum Encryption Key Generation Algorithm Using Electromagnetic Wave Propagation Theory. *Journal of Information Security*, **15**, 53-62. https://doi.org/10.4236/jis.2024.151005

[15] Liu, B.X. and Wu, H.P. (2015) Efficient Architecture and Implementation for NTRUEncrypt System. 2015 *IEEE* 58*th International Midwest Symposium on Circuits and Systems* (*MWSCAS*), Fort Collins, 2-5 August 2015, 1-4. https://doi.org/10.1109/mwscas.2015.7282143