Journal of Information Security, 2024, 15, 53-62
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Development of a Post Quantum Encryption Key Generation Algorithm Using Electromagnetic Wave Propagation Theory

Vincent Mbonigaba[1,2,3], Fulgence Nahayo[1,2,3], Octave Moutsinga[1,2,3], Okalas-Ossami Dieudonné[1,2,3]

[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
Email: mbonivinci@gmail.com, fulgence.nahayo@auf.org, dokalas@e-tumba.com, octave.moutsinga@univ-masuku.org

How to cite this paper: Mbonigaba, V., Nahayo, F., Moutsinga, O. and Dieudonné, O.-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

Received: November 3, 2023
Accepted: January 28, 2024
Published: January 31, 2024

Abstract

In today's rapid widespread of digital technologies into all live aspects to enhance efficiency and productivity on the one hand and on the other hand ensure customer engagement, personal data counterfeiting has become a major concern for businesses and end-users. One solution to ensure data security is encryption, where keys are central. There is therefore a need to find robusts key generation implementation that is effective, inexpensive and non-invasive for protecting and preventing data counterfeiting. In this paper, we use the theory of electromagnetic wave propagation to generate encryption keys.

Keywords

Key, Wave, Electromagnetic, Cryptography, Post, Quantum, Network, Protocol, Propagation, Algorithm

1. Introduction

Miniaturization of computer components allows for increased computing power in the modern era. Gordon E. Moore believes in his article that the size of these circuits will shrink and that we will be able to double the number of components integrated in a single circuit every two years, allowing us to increase ipsof facto these performances and, in particular, its speed. It had considered doubling them once every 18 months [1]. Postquantum encryption and signature systems are among the more difficult mathematical problems to solve, such as those found in Euclidean networks and error-correcting codes, and their implementa-

tion in practice imposes numerous constraints, particularly in restricted environments such as microcontrollers [2]. The exponential factor that describes and predicts the rate of electronic component miniaturization and cost reduction. The development of a quantum computer will have a significant impact on the cryptography we use every day to secure our communications, particularly asymmetric cryptography. Furthermore, the proliferation of connected objects in our daily lives, as well as their limitations in terms of computing capacity and available memory, make them targets [3]. Post-quantum cryptography is based on mathematical problems that, even with quantum computers, are difficult to solve [4]. A Drinfeld module is an algebraic construction resulting from function body arithmetic. These objects have algebraic properties that are very similar to elliptical curves [5]. To address this, businesses/organizations are collaborating with research institutions to develop tools, techniques, technologies, and methods for securing and protecting data and information exchanged via various or redundant communication networks. In this context, the goal of this article is to provide a portion of the solutions by designing and implementing a tool for generating postquantum encryption keys based on the theory of electromagnetic wave propagation [6], in order to improve security, data protection, and business information through unbreakable cryptographic algorithms based on quantum mechanics [7].

2. Tools and Materials

The tool for generating postquantum encryption keys based on electromagnetic wave propagation theory, which will be very useful in protecting computer data exchanges via optical fibers from attacks by quantum machines, which are typically backed up on terminals hosted on servers or exchanged via transmission networks [8]. This is the famous Moore's Law. He contended that these circuits would pave the way for new machines (from portable computers to electronic watches) and improve the performance of systems like radar [9]. The use of this algorithm is motivated by its unique use of the encryption key in comparison to the crypto systems of RSA, which allows for the discovery of an algorithm that allows for the factoring of any number in polynomial time when the size of the number is a problem of very large length.

The community has long struggled to find a polynomial algorithm to determine whether a number is first or not. The RSA problem, which involves calculating the root the modulo a compound number, corresponds to inverting the encryption function without the trap. Java libraries will be required for the solution's implementation as well as the mathematical logic of Boole.

3. Approach to Key Generation Using Electromagnetic Wave Propagation

An approach that seems more appropriate to us is to use chiffrement mechanisms using the theory of electromagnetic wave propagation, which also allows the various stakeholders to access their data since both communicators are able

to dechiffres them. We talk about modelling the generation algorithm using the cyclic redundancy technique and elliptic curves, and implementing the modelled algorithm.

3.1. Modeling the Generation Algorithm Using Cyclical Redundancy Technique and Elliptic Cuves

With

E_k : which is an elliptic curve on m

D_k : which is an elliptic curve applied to E_k to find the clear message m

In the case of so-called symmetrical safety, we use a peculiarity of the expression

$$y^2 = ax^2 + bx + C \tag{1}$$

for a given value of *x*, there are generally two possible values of *y*, symmetrical with respect to the x-axis. In principle, therefore, it is possible to calculate an elliptic curve solely on the basis of the *x* coordinate if we are not concerned about the sign of *y*. This idea is made concrete by the use of Montgomery curves, which are defined as the quotient of the curve by the involution $y \mapsto -y$. The advantage of working with just one coordinate is a reduction in the amount of data manipulated or transmitted, and for well-chosen curves, a reduction in the number of operations performed.

These methods are being developed in parallel with the constant evolution of software and IT tools enabling data to be intercepted for use by third parties.

Cyclic redundancy techniques can be used. Controlling cyclic redundancy involves protecting blocks of data, known as frames. Each frame is associated with a block of data. We therefore have $P(x)$ which is the characteristic polynomial of the message to be sent, $G(x)$ which is the generator polynomial and $T(x)$ which is the concatenated message that will pass through the transmission channel.

When our N-bit key is transmitted, it is considered to be a polynomial of degree N-1 which is $P(x)$ and another generator polynomial $G(x)$. The generator polynomial may depend on the type of protocol on a given network. The encoding process is carried out both at the transmitter and at the receiver, the decoding process is carried out using the same generator polynomial $G(x)$. With IEEE 802 protocol, we have

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1. \tag{2}$$

or with HDLC protocol, we have

$$G(x) = x^{16} + x^{12} + x^5 \tag{3}$$

as generator polynomial $G(x)$

$$P(x) = \sum_{u=(0,1)} \sum_{k=0}^{n} ux^k \tag{4}$$

$$T(x) = P(x) * x^k. \tag{5}$$

$$Q(x)=\frac{T(x)}{G(x)} \tag{6}$$

$$T(x)=Q(x)*G(x)+R(x) \tag{7}$$

One of the most common methods is symmetric encryption, also known as a secret n-key algorithm. Before the message can be decrypted, the recipient must be provided with a one-of-a-kind decoding method.

Asymmetric encryption, on the other hand, employs two distinct keys - public and private that are mathematically related and thus, to some extent, interdependent. In particular, the keys are made up of large numbers that have been linked together but are not identical. In light of the foregoing, we will implement a mechanism for protecting and securing data based on a crypto system that resists attacks with machines designed according to physical laws, the advantage of which is the use of the same key upstream and downstream, that is, when encryption and decryption. We propose a new non-interactive key exchange protocol based on a simple transitive group action that is easy to calculate and difficult to reverse. Referring to Maxwell's laws, which discuss the propagation of a digital signal (information) through an optical fiber.

3.2. Implimentation of the Modelled Algorithm

1) Implementation principle of the algorithm

The values of the various variables used in the clear propagation of information will be converted to binary format. The unique XOR or OR logic operation is applied to the different bits of the clear variable and key flow between magnetic induction and magnetic excitation to generate a key. The XOR operation has the advantage of being reversible by simply performing the same operation again. In other words, encryption is the process of applying on variables in clear text. Using Boolean algebra between variables with XOR (Exclusive OR).

While it is true that a qubit is a generic description of a quantum system in which an observable has two accessible levels known as $\lceil 0\rangle$ and $\lceil 1\rangle$ that are part of an orthonormed base. The phase quantifies the state. In the case of the density matrix, a pure state is defined as a linear superposition of the generic base states $\lceil 0\rangle$, $\lceil 1\rangle$. Basic quantum information ideas are next outlined, including qubits and data compression, quantum gates, the "no cloning" property and teleportation The propagation equation in optical fibers is given by the following figure: Using the Pythagorean theorem Magnetic Induction's worth B will be considered as the value of the opposite side at the angle ω that varies with time or the variation of magnetic permeability, and H will be considered as the value of the adjacent side at the angle ω that varies with time or the variation of magnetic permeability as shown in Figure 1.

$$B=\mu 0\cdot\cos\omega \tag{8}$$

whith

$$\omega=2\times pif \tag{9}$$

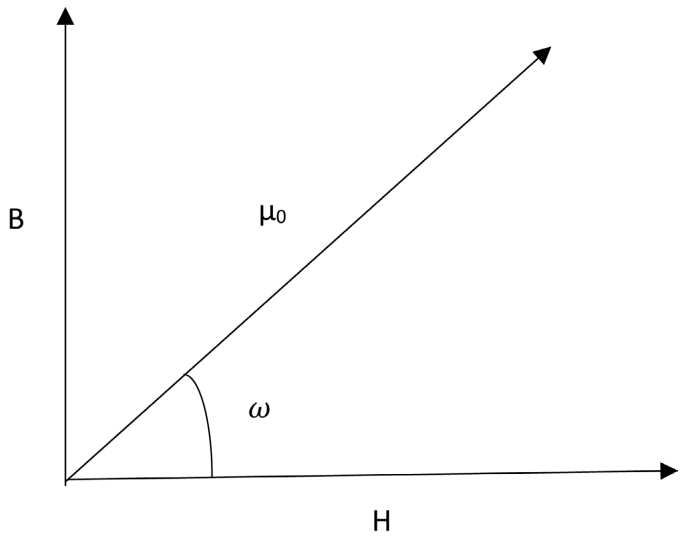

Figure 1. The propagation diagram of electromagnetic waves.

becomes the magnetic induction value

$$H = B/\tan\omega \tag{10}$$

By substituting B for its value, we get

$$B = \mu \times H \tag{11}$$

$$H = B/\mu \tag{12}$$

In a vacuum or in the air gap, $\omega 0$ is used. The example below is a practical illustration of the algorithm for generating a number that will be used as an encryption key against attacks.

2) Implementation of the algorithm

In general, the dimension of this base can be greater than or less than two, the observable is associated with the state, and we concentrate on the state itself. These are the Maxwell's laws that govern electromagnetic wave propagation [10].

$$\nabla \wedge \boldsymbol{E} = \frac{\varepsilon \boldsymbol{B}}{\varepsilon t} \quad \text{Faraday Law} \tag{13}$$

$$\nabla \wedge \boldsymbol{H} = \frac{\varepsilon \boldsymbol{D}}{\varepsilon t} + \boldsymbol{J} \quad \text{Ampere's Law} \tag{14}$$

$$\nabla \cdot \boldsymbol{D} = \rho \quad \text{Gauss Law} \tag{15}$$

$$\nabla \cdot \boldsymbol{B} = 0 \quad \text{Gauss Law} \tag{16}$$

Entrances

μ: *Permeability*

$\mu 0$: *Magnetic permeability in vacuum with value* 4×10^{-7} Herry/m

μr: *Relative permeability*

E: *Electric fields expressed in* volt/m

S: *Driver Section* m^2

Φ: *phi in a magnetic medium*

D: *the electric displacement*

ω: *Angular velocity in radian per second*

T: *time*

Exit

B: *Magnetic induction expresses in weber*

H: *Magnetic excitation expresses in Tesla*

Step 1: Calculation of the magnetic induction *B* using the permeability in the iron gap μ: $B = \mu 0 \cdot \cos \omega$

Step 2: Converting B induction to binary

Step 3: Calculation of the magnetic excitansion H using the magnetic induction B and the value of the tangent of the angle tangt ω between magnetic excitation and permeability in a vacuum $\mu 0$

Step 4: Converting the result of H magnetic excitation into binary

Step 5: Using Boolean Algebra (or exclusive) between Magnetic Induction and Magnetic Excitation B XOR H

Step 6: Generating the key and completing the algorithm

3.3. Application of the Algorithm

Beginning

$B \to 0$

$H \to 0$

Number generates $\to 0$

While $(\mu 0 > 0)$

$B = \mu \times 0 \cos \pi t$

Converting the value from B to Binary

$H = B/\tan \omega t$

Converting the value of H to Binary

The generated number = B XOR H

End while

end.

3.4. Presentation of the Results

The algorithm of key generation with the laws of physics referring to the propagation of information in optical fibers developed in this work is part of the family of symmetric algorithms based on key encryption secret. Given that it will be used to secure information exchange between different users in an information system based on evaluations of various companies and institutions in Burundi, data that is rarely transmitted via a public network, this algorithm has the advantage of being theoretically unbreakable, but also because of its unique use of the encryption key.

Development of a post quantum encryption key generation algorithm using electromagnetic wave propagation theory.

H = 00111110100110101000000011111011101100010110100010011010110100 00

B = *10111111011110011111101111011111010111101111010110101110110000 11*

key generated = *10100100011111011011011110101110111011101000100110010 10110110001010011101101000001101000010010101001100010010011000100110 01110100001001011100101010011101111011010111000100010001010110000111 11011100011001001010010001110111001111100000011100110111000001101111 01010011101011101001101111101111100110101001010001101000010001100010 11101110100000110000101101101010000010111000010011011010010010001000 11100100110101010011011011111010101000010011011100100011010100101101 00110111011000100110111110111111000000010110100000*

The curve was obtained for a variation in μ in the range −4 and +4 as shown in Figure 2. It is clear that the magnetic induction curve varies as a function of the magnetic permeability in the air gap. The shape of the curve is similar to that of the sinusoidal shape and also depends on the variation in frequency during propagation of the electromagnetic wave. On the other hand, they can be used to generate the security key against the spy who wants to acquire a large amount of information during the quantum communication phase. Permeability The curve was obtained for a variation in magnetic induction in the range −2 and 5×10^{-5} as shown in Figure 3 and the value of the frequency varying from 0 to 3000 Hz. It is clear that the Magnetic Excitation curve varies as a function of the magnetic permeability in the air gap and the frequency. The shape of the curve is periodic with the presence of noise during the propagation of the electromagnetic wave. On the other hand, they can be used to generate the security key against a spy who wants to acquire a large amount of information during the quantum communication phase.

4. Discussion of Results

We have managed to generate an unbreakable key that will enable us to better

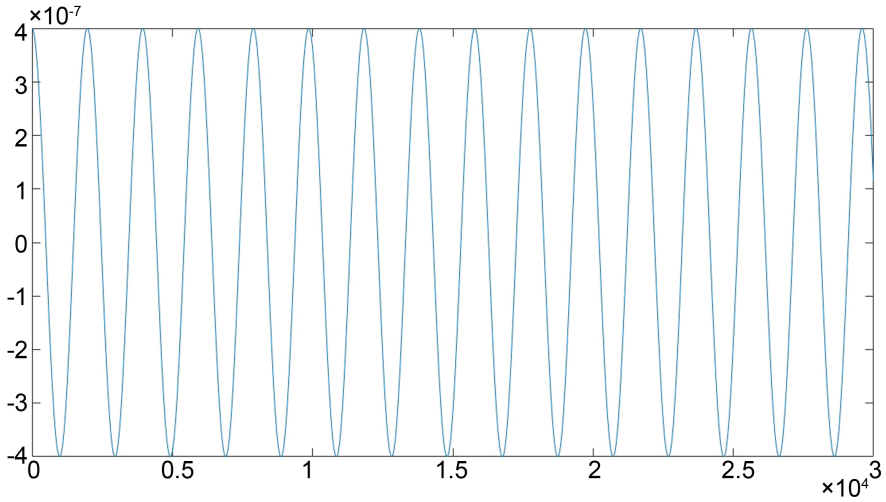

Figure 2. Analysis curve of the magnetic induction obtained by the permeability in the iron in relation to the frequency.

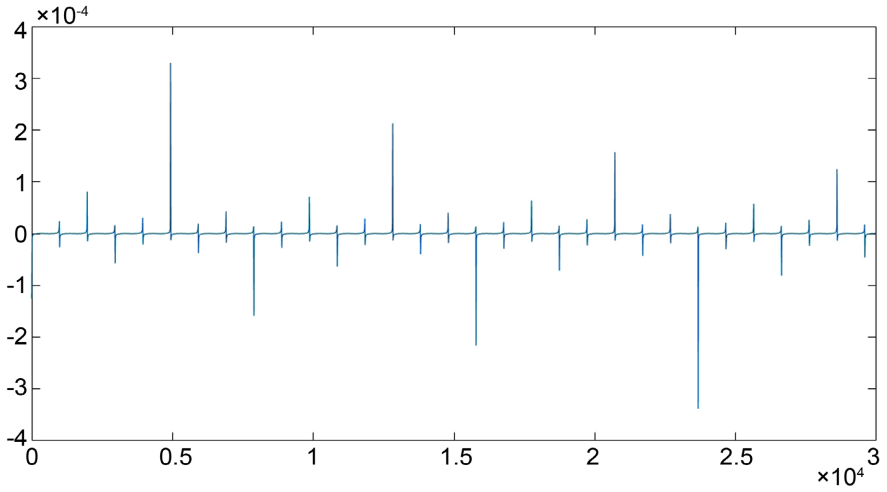

Figure 3. Analysis curve of magnetic excitation obtained by permeability in the iron gap in relation to frequency.

secure our information, which will be very useful in cryptosystems that use the attack-resistant algorithm in the possession of quantum machines in order to remedy the problems of factoring and exponentials.

A crypto system with a secret key and therefore symmetrical. As the key is used once and only once, disposable mask key, this last specificity confers to this cryptographic system a high, substantial degree of reliability, which reinforces the safety of the data to be protected and or to defend against the threats of deterioration or interception for malicious use.

We made the algorithms on base of the laws of Maxuel in which we resorted to the magnetic induction and the magnetic Excitation with the logical door XOR. The XOR gate was chosen because it is the only symmetrical cryptosystem that guarantees data confidentiality, availability and integrity. The java code we used to generate its number.

```
double d = −0.00634372;
String s = Long * toBinaryString(Double*doubleToLongBits(d));
s = ZEROS*substring(s*length()) + s;
```

Based on the permeability between iron and frequency, we were able to draw curves to analyze magnetic induction and magnetic excitation. We used Matlab to generate the analysis curve between the coordinates.

$$f = 1:5:3000$$

$$B = 4*10^{-7}*\cos(6.28*f);$$

$$f = 1:5:3000$$

$$H = \left(4*10^{-7}*\cos(6.28*f)\right)/\left(\tan(6.28*f)\right);$$

5. Conclusions and Future Works

5.1. Conclusions

The engine of post-quantum cryptography is a tool for generating post-quantum

encryption keys based on electromagnetic wave propagation theory, but traditional IT security is neither flexible nor scalable enough to protect this new reality of the digital ecosystem.

It is necessary to protect them using multiple protection systems, including Smart Grid security, cross-platform assistance, and data security infrastructure based on quantum mechanics [11]. The current work has focused on improving the security of data exchange between sensitive post quantum institutions and companies adapting to this new technology, whether in Burundi or elsewhere, as data is rarely transferred via communication channels.

The use of the quantum cryptographic algorithm is suitable for securing this type of data in information rarely transmitted and exchanged and the processing usually undergone in read-only mode. In the following work, we'll see how to use this generated key to protect the message being sent when exchanging information.

5.2. Future Works

Threats and attacks weaken IT systems, leading some companies to incur significant and often unforeseen costs. The aim of this article is to generate a data security key using the theory of electromagnetic wave propagation. In future work, we will proceed to use this key to secure data between different communicators, as well as its modelling, and then we will see how secure the transmission of this key is against malicious systems.

Conflicts of Interest

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

References

[1] Theis, T.N. and Philip Wong, H.-S. (2015) The End of Moore's Law: A New Beginning for Information Technology. *Computing in Science & Engineering*, 19, 41-50. https://doi.org/10.1109/MCSE.2017.29

[2] Huang, W., Nizam, M. H., Andonovic, I. and Tur, M. (2000) Coherentoptical CDMA (OCDMA) Systemsused for High-Capacityopticalfiber Networks-System Description, OTDMA Comparison, and OCDMA/WDMA Networking. *Journal of Lightwave Technology*, **18**, 765-778. https://doi.org/10.1109/50.848384

[3] Chithralekha, T., Singh, K., Ganeshvani, G. and Rajarajan, M. (2021) Code-Based Post-Quantum Cryptography. *Journal Not Specified*, 24 p.

[4] Reina, J.H. (2009) Fundamentals of Information and Computation in the Realm of the Quanta. *Revista de la Academia Colombiana de Ciencias Exactas*, *Fisicas y Naturales*, **33**, 201.

[5] Joux, A. and Narayanan, A.K. (2019) Drinfeld Modules May not Be for Isogenybasedcryptography. *Cryptology ePrint Archive*, 16 p.

[6] Malina, L., *et al*. (2021) Post-Quantum Era Privacy Protection for Intelligent Infrastructures. *IEEE Access*, **9**, 36038-36077. https://doi.org/10.1109/ACCESS.2021.3062201

[7] Messiah, A. (2014) Quantum Mechanics. Courier Corporation, Chelmsford.

[8] Gagnidze, A., Iavich, M. and Iashvili, G. (2017) Analysis of Post Quantum Cryptography Use in Practice. *Bulletin of the Georgian National Academy of Sciences*, **11**, 29-36.

[9] Papon, P. (2017) Moore's Law Anticipates the Future of Electronics. *Futuribles*, **417**, 79-84. https://doi.org/10.3917/futur.417.0079

[10] Rabia, A. (2021) Électromagnétisme: Propagation des ondes électromagnétiques-Lois et équations. Propagations libre et guidée-Cours, exemples et exercices corrigés. Editions Ellipses, Paris, 348 p.

[11] Zijlstra, T. (2020) Secure Hardware Acceleration for Post-Quantum Cryptography. Ph.D. Thesis, Université de Bretagne Sud, Lorient.