A Review on the Neutrosophic Number Theory Based Cryptography and Neutrosophic Public Key Crypto-Systems

Ali Allouf

Tishreen University, Faculty of computer engineering and automation, Latakia, Syria

Ali.allouf@gmail.com

Abstract:

The main objective of this chapter is to introduce the concept of neutrosophic number theory, and to demonstrate its potential applications in modern cybernetic systems. The chapter will also explore the possibility of utilizing neutrosophic theory to enhance existing security algorithms, including a detailed explanation of the neutrosophic version of the RSA algorithm. Furthermore, the chapter will present a novel neutrosophic version of the Diffie-Hellman key exchange algorithm.

Keywords: Neutrosophic Cryptography; Neutrosophic RSA Algorithm; Public key Cryptography; Fusion Neutrosophic Number Theory; Diffie-Hellman key exchange algorithm

1. Introduction

The advent of Industry 5.0, the fifth industrial revolution, has ushered in an era of unprecedented technological advancements. This revolution is marked by the convergence of cyber-physical systems, the Internet of Things (IoT), and artificial intelligence (AI), leading to the creation of intelligent, autonomous, and interconnected systems. As these systems become increasingly complex and integrated, the need for robust and secure communication channels has never been more pressing. Enter Neutrosophic cryptography, a novel and emerging field that leverages the principles of neutrosophic logic to enhance the security and resilience of cryptographic systems.

Neutrosophic logic, an extension of fuzzy logic, introduces the concept of indeterminacy, allowing for the representation and analysis of information with inherent uncertainties and inconsistencies. Neutrosophic algebra, introduced by Kandasamy and Smarandache [4], lays the foundation for various neutrosophic algebraic structures like neutrosophic groups and rings [5, 7]. The inclusion of an indeterminate element (denoted by an "I") offers a unique logical property, fostering significant advancements in the study of algebraic structures (see references [1-3, 6, 8-12]).

The year 2020 marked the birth of neutrosophic number theory, where concepts like neutrosophic greatest common divisor (gcd), neutrosophic Diophantine equations, neutrosophic Euler's function, and neutrosophic congruences were established and explored by several researchers (see references [3, 11]). Drawing an analogy, cryptography can be viewed as the practical application of number theory concepts. As various scientific fields, particularly computing, cryptography, and security systems, witness rapid advancements, the need for more robust security measures becomes increasingly crucial. This very need has fueled the development of neutrosophic cryptography theory.

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024

2. Mathematical Definitions and Issues

Definition 2.1: [3]
Let Z be the ring of integers, we say that $(I) = \{a + bI; a\ b \in Z\}$is the neutrosophic ring of integers.
Definition 2.2: [3]
a) let $a + bI, and\ c + dI$ are two neutrosophic integers, then:
$a + bI \leq c + dI$ if and only if $a \leq$, $a + b \leq c + d$.
b) $a + bI$ is called positive neutrosophic integer if $a > 0$ and $a + b > 0$.
Example 1:
$5 + 2I$ is a positive neutrosophic integer, that is because $5 > 0$, $5 + 2 = 7 > 0$.
Definition 2.3: [3] (Addition)
Let $a + bI, c + dI$:

$$(a + bI) + (c + dI) = (a + c) + (b + d)I \tag{1}$$

Definition 2.4: [3] (Multiplication)
Let $a + bI, c + dI$:

$$(a + bI) \cdot (c + dI) = ac + adI + bcI + bdI^2$$
$$ac + I(ad + bc + bd \tag{2}$$

Definition 2.5: [3] (Neutrosophic Exponentiation)
Let $a + bI, c + dI$:

$$(a + bI)^{c+dI} = a^c + I[(a + b)^{c+d} - a^c] \tag{3}$$

Definition 2.6: [3] (Greatest Common Divisor)
Let $a + bI, c + dI$:

$$\gcd(a, c) + (\gcd(a + b, c + d) - \gcd(a, c))I \tag{4}$$

Definition 2.7: [3] (Division)
Let $(I) = \{a + bI; a, b \in Z\}$ the neutrosophic ring of integers. For any $x, y \in (I)$, we say that $x|y$ if there is $r \in (I); r. x = y$.

Definition 2.8: [3] (Congruence)
In the neutrosophic ring denoted by Z(I), let $x = a + bI$, $y = c + dI$, and $z = m + nI$ be three elements. We say that x **is congruent to** y **modulo** z (denoted by $x \equiv (mod z)$) if and only if z divides the difference between x and y.
An element z in Z(I) is called the **greatest common divisor (GCD) of** x **and** y if it satisfies the following conditions:
1. **Divisibility:** z divides both x and y: $z \mid x\ and\ z \mid y$
2. **Maximality:** For any other element c dividing both x and y (i.e., $c \mid x\ and\ c \mid y$), c must also divide z (i.e., $c \mid z$).

Definition 2.9: [3] (primes)
Let $Z(I) = \{a + bI; a, b \in Z\}$ denote the neutrosophic ring of integers**.** An arbitrary element $x \in Z(I)$ is called a **prime element** if, whenever x divides the product of two elements y and z, it divides at least one of the factors y or z.

The concept of utilizing neutrosophic numbers in cryptography was first introduced by Merkepci et al. in [13].

Definition 2.10: [10] (RSA algorithm)

Neutrosophic Euler's Identity:
Let $a + bI$ and $c + dI$ be two **relatively prime** neutrosophic positive integers (meaning their greatest common divisor is the neutrosophic integer 1). Then, the following equation holds:

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024

$$(a + bI)^{\varphi(c+dI)} = 1(mod\ c + dI)$$

(5)

To encrypt a plaintext message m using the RSA algorithm, we follow these steps:

a) We Pick two positive integers $p, and\ q$ and compute $n = pq$.
b) Compute (n).
c) We Pick a positive integer $1 < e < (n)$ such that $g(e,\varphi(n)) = 1$.
d) We Use the formula $C \equiv m^e(mod\ n)$ to get the encryption of (m).
e) To decrypt the original text (m), calc $d \Leftrightarrow e^{-1}$ such that e. d ≡ 1($mod\ \varphi(n)$).
f) Then we compute $m \equiv C^d(mod\ n)$ to get the original text.

We call the pair (e, n) the public key, and we call the pair (d, n) the private key.
The RSA algorithm's security relies on the difficulty of factoring large natural numbers (integers) into their prime components. Choosing a large number n for n makes it computationally challenging to break the code, as this process requires factoring n.

Example 2:
Consider that m = 11 is the plain text, then we pick p = 17, q = 11, then $n = pq$ = 187, $(n) = (p - 1)\ (q - 1)$ = 160.
We choose a small value for e, e = 7 (satisfying gcd(e, φ(n)) = 1).
Then the encrypted message:

$$C \equiv m^e(mod\ n)$$
$$C \equiv 11^7(mod\ 187) = 154$$

To decrypt the previous message, then:
using the Extended Euclidean Algorithm, we can find d such that: $d \cdot e \equiv 1(mod\ \varphi(n))$. In this case, d = 23.

$$m \equiv C^d(mod\ n)$$
$$m \equiv 154^{23}(mod\ 187) = 11$$

3. Enhanced Neutrosophic RSA Algorithm

The primary goal of cryptography is to keep messages confidential. The RSA algorithm relies on the difficulty of factoring large integers into their prime factors. Neutrosophic integers offer a higher level of complexity, making them suitable for cryptographic applications. Analyzing positive neutrosophic integers is significantly more challenging than analyzing regular integers (see [13]).
For example, $n = 20 + 52I$ can be split into many different formulas such as: $(4 + 2I)\ (5 + 7I)$, $(4 - I)\ (5 + 9I)$, $(2 + I)\ (18 + 14I)$ and so on.
This implies that constructing a neutrosophic version of the RSA algorithm will yield a higher level of complexity, making it even more challenging to crack the algorithm.
In our published research paper entitled "The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm", Mehmet Merkepci and Mohammad Abobala introduced a novel formula for the Euler totient function:

$$(x + yI) = (x).(x + y);\ x, x + y > 0.$$

(7)

The Euler phi function counts the number of positive neutrosophic integers, such as $a + bI \leq x + yI$ and that are relatively prime to $\gcd(a + bI, x + yI) = 1$.
Steps for Implementing the Neutrosophic Algorithm: [3]
Assume that Bob and Alice, Bob wants to send an encrypted text to Alice. Suppose that $M = m + nI$ is the text, to encrypt M, Bob should follow these steps:

1) Bob picks two neutrosophic positive integers, $P = a + bI$, $= c + dI$ and compute $N = PQ = ac + (ad + bc + bd)$.
2) Bob computes $\varphi\ (N) = \varphi\ (P).\varphi\ (Q)$, where:

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024

$$\varphi(P) = a - 1 + I[\varphi(a + b) - (a - 1)] = a - 1 + I[a + b - 1 - a + 1] = a - 1 + bI.$$

(8)

$$\varphi s(Q) = a - 1 + I[\varphi(c + d) - (a - 1)] = c - 1 + dI.$$

(9)

3) Bob picks an arbitrary neutrosophic positive integer $E = e_1 + e_2 I$ with $(E, \varphi(N)) = 1$ and $1 < E < \varphi(N)$, the public key is (E, N).

4) Bob encrypts the text M by the formula:

$$C \equiv M^e (mod\ n) = (m + nI)^{(e_1 + e_2 I)} (mod\ n)$$
$$= ((m)^{e1} + I[(m + n)^{(e_1 + e_2)} - (m)^{e_1}])(mod\ n)$$

(10)

Bob send C to Alice.

The private key is calculated as follows:

$$d = (e_1^{-1} + I[(e_1 + e_2)^{-1} - e_1^{-1}])(mod \phi_s(n)) =$$
$$s_1 + s_2 I(mod\ \phi_s(n)).$$

(11)

This is how Alice decrypts the message:

$$M \equiv C^d (mod\ n)$$

(12)

Example 3:

Assuming that Bob has the message $M = 3 + 2I$ and $P = 3 + 2I, Q = 5 + 6I > 0$.

$N = PQ = 5 \times 3 + I(5 \times 2 + 6 \times 3 + 6 \times 2) = 15 + I(10 + 18 + 12) = 15 + 40I.$

$\varphi(N) = (4 + 6I)(2 + 2I) = 8 + I(4 \times 2 + 6 \times 2 + 6 \times 2) = 8 + 32I.$

We choose e to satisfy $1 < e < \varphi(N)$, $e = 3 + 6I$.

$$C \equiv M^e (mod\ N) = (3 + 2I)^{3+6I} (mod\ 8 + 32I) \Rightarrow C = 12 + 8I.$$

$d = 3 + 6I \Longrightarrow M \equiv C^d (mod\ N) = (12 + 8I)^{3+6I} (mod\ 8 + 32I) = +3(5 - 3)I = 3 + 2I.$

In our published research, we provided theoretical proofs and demonstrations of the correctness of the algorithm's operation. Additionally, we raised the complexity of the RSA algorithm to the square, making it more resistant and secure against attacks (see [13]).

4. Neutrosophic Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange is a foundational cryptographic method that allows two parties to securely agree on a shared secret key, even if they are communicating over an insecure channel where others might be listening. This shared secret key can then be used to encrypt and decrypt messages, providing confidentiality for their communication. The magic of Diffie-Hellman lies in modular arithmetic and one-way functions:

a) Shared Public Parameters: Two parties, Alice and Bob, begin by agreeing on a large prime number (p) and a generator (g) within a finite field. These are public values and can be known by anyone.

b) Private Keys: Alice and Bob each choose a secret, random number. Alice's is called a, and Bob's is called b. These are kept absolutely private.

c) public Key Calculation:

- Alice calculates: $A = g^a\ mod\ p$, and sends the result (A) to Bob.

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024

- Bob calculates: $B = g^b \ mod \ p$, and sends the result (B) to Alice.

d) Shared Secret Calculation:

- Alice receives B and computes $B^a (mod\ p)$.
- Bob receives A and computes $A^b (mod\ p)$.

Crucially, due to the properties of modular arithmetic, both Alice and Bob will arrive at the same shared secret value

5. Proposed Neutrosophic Algorithm

The Description of neutrosophic Diffie-Hellman Algorithm:

a) Alice and Bob agree on a neutrosophic prime $\boldsymbol{p = p_1 + p_2 I}$, i.e. $\boldsymbol{p_1}$, $\boldsymbol{p_1 + p_2}$ are classical primes and a base $\boldsymbol{g = g_1 + g_2 I > 0}$, i.e. $\boldsymbol{g_1}$, $\boldsymbol{g_1 + g_2}$>0.

b) Alice chose a secret number $\boldsymbol{a = a_1 + a_2 I > 0}$, and sends Bob $\boldsymbol{g^a (mod\ p)}$. [Remark that $\boldsymbol{g^a (mod\ p) = g^a{}_1 (mod\ p_1) + I[(g_1 + g_2)^{a_1 + a_2} (mod\ p_1 + p_2) - g^a{}_1 (mod\ p_1)]}$.

c) Bob choose a secret number $\boldsymbol{b = b_1 + b_2 I > 0}$, and sends Alice $\boldsymbol{g^b (mod\ p)}$.

d) Alice computes $\boldsymbol{(g^b)^a (mod\ p) = g^{a_1 b_1}{}_1 (mod\ p) + I[(g_1 + g_2)^{(a_1 + a_2)(b_1 + b_2)} (mod\ p_1 + p_2) - g^{a_1 b_1}{}_1 (mod p_1)]}$.

e) Bob computes $\boldsymbol{(g^a)^b (mod\ p)}$.

Example 4:
Assume that Alice and Bob have agreed on $p = 3 + 4I$, and $g = 5 + I$.
Alice choose the secret neutrosophic number $a = 2 + 3I$. Alice sends Bob$(5 + I)^{2+3I} (mod\ p) = 5^2 (mod\ 3) + I[6^5 (mod\ 7) - 5^2 (mod\ 3)] = 1 + 5I$.
Bob choose the secret neutrosophic number $b = 4 - 2I$, and sendsAlice$(5 + I)^{4-2I} (mod\ p) = 5^4 (mod\ 3) + I[6^2 (mod\ 7) - 5^4 (mod\ 3)] = 1$.
Alice computes $1^{2+3I} (mod\ p) = 1$.
Bob computes $(1 + 5I)^{4-2I} (mod\ p) = 1$.
Thus, we observe that both parties generated the same secret key value, and therefore the neutrosophic algorithm worked correctly.

6. Conclusion

In this chapter, we presented some of the mathematical foundations of neutrosophic number theory and explained the potential for using it to develop and enhance existing information security algorithms, making them more secure and resistant to attacks. At the end of the chapter, we presented an approach for using neutrosophic numbers in the Diffie-Hellman key exchange algorithm. Neutrosophic number theory may have a great impact on cryptography, so we suggest researchers define a version of Diffie-Hellman depending on the refined neutrosophic number theoretical approach [12].We believe that the convergence of Neutrosophic cryptography and Industry 5.0 represents a paradigm shift in the way we approach data security and communication in the realm of cyber-physical systems. By embracing the principles of neutrosophic logic and leveraging its ability to handle uncertainties and inconsistencies, Neutrosophic cryptography offers a robust and resilient framework for securing data exchange in the interconnected and autonomous systems that characterize the fifth industrial revolution.

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024

References

[1] Celik, M., & Olgun, N. (2022). An introduction to neutrosophic real Banach and Hillbert spaces. *Galoitica Journal of Mathematical Structures and Applications*, 2(1), 8-13.

[2] Celik, M., & Olgun, N. (2022). On the classification of neutrosophic complex inner product spaces. *Galoitica Journal of Mathematical Structures and Applications*, 2022(1), 14-23.

[3] Abobala, M. (2021). Partial foundation of neutrosophic number theory. *Neutrosophic Sets and Systems*, 39, 120-132.

[4] Smarandache, F., & Kandasamy, W. B. V. (2011). Finite neutrosophic complex numbers. arXiv.org.

[5] Agboola, A. A. A., Akinola, A. D., & Oyebola, O. Y. (2011). Neutrosophic rings I. *International Journal of Math Combinatorics*, 4, 1-14.

[6] Adeleke, E. O., Agboola, A. A. A., & Smarandache, F. (2020). Refined neutrosophic rings I. *International Journal of Neutrosophic Science*, 2(2), 77-81.

[7] Abobala, M. (2021). On some algebraic properties of n-refined neutrosophic elements and n-refined neutrosophic linear equations. *Mathematical Problems in Engineering*, 2021, 1-7.

[8] Abobala, M. (2021). On refined neutrosophic matrices and their applications in refined neutrosophic algebraic equations. *Journal of Mathematics*, 2021, 5531093.

[9] Cozzens, M. Miller, S.J. (2013). The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society.

[10] Wahab Sait, A. R., Pustokhina, I., & Ilayaraja, M. (2019). Modeling of multiple share creation with optimal signcryption technique for digital image security. *Journal of Intelligent Systems and Internet of Things*, 0(1), 26-36.

[11] Sankari, H., and Abobala, M., "Neutrosophic Linear Diophantine Equations With two Variables", Neutrosophic Sets and Systems, Vol. 38, pp. 22-30, 2020.

[12] Ibrahim, M., & Abobala, M. (2021). An introduction to refined neutrosophic number theory. *Neutrosophic Sets and Systems*, 45, 1-10.

[13] Merkepci, M., Abobala, M., & Allouf, A. (2023). The applications of fusion neutrosophic number theory in public key cryptography and the improvement of RSA algorithm. *Fusion: Practice and Applications (FPA)*, 10(2), 69-74.

DOI: https://doi.org/10.54216/IJAACI.060103
Received: November 2, 2023 Revised: January 24, 2023 Accepted: June 12, 2024