NSS
Neutrosophic Sets and Systems, Vol. 102, 2027
University of New Mexico

On Partially Homomorphic Encryption over Neutrosophic Integers Using the AH-Isometry

Mark Petersen[1,*]
[1] Mathematical and Physical Science Foundation, 4200 Slagelse, Denmark; mpetersendk@protonmail.com
* Correspondence: mpetersendk@protonmail.com

Abstract: Neutrosophic algebraic structures provide a way to work with indeterminacy within algebraic systems. This makes it natural to investigate whether a classical homomorphic cryptosystem such as Paillier can be formulated over the ring of neutrosophic integers Z(I). This paper introduces a neutrosophic version of the Paillier cryptosystem built over the ring of neutrosophic integers Z(I). It uses the foundations of the AH-isometry introduced by Abobala and Hatip to derive the neutrosophic formulas used in the cryptosystem. Since ordinary neutrosophic primes do not provide a suitable modulus corresponding to the classical Paillier modulus, this paper introduces neutrosophic paired-prime integers. The resulting cryptosystem defines encryption, decryption, and homomorphic properties and shows examples of encryption, decryption, and homomorphic addition of neutrosophic plaintexts based on this paired-prime modulus.

Keywords: Public Key Cryptography; Homomorphic Encryption; Neutrosophic Cryptography; Paillier Cryptosystem; Neutrosophic Number Theory; Neutrosophic Paillier Cryptosystem

1. Introduction

In 2006, Kandasamy and Smarandache introduced algebraic structures with neutrosophic properties, where the algebraic symbol "I" refers to indeterminacy and satisfies $I^2 = I$ [1]. For neutrosophic integers, this gives integers of the form a + bI. These neutrosophic structures have been studied in neutrosophic number theory [2–4], and the concept of indeterminacy has also been applied to neutrosophic cryptography, which was first suggested by Merkepci et al. [5, 6].

In 2021, Abobala and Hatip introduced the AH-isometry, showing that a neutrosophic number a + bI can be represented by (a, a + b) [7]. In this paper, the AH-isometry is used as an algebraic structural tool for investigating neutrosophic integers through an isomorphism T. This allows for an easier translation of the formulas from the classical Paillier cryptosystem to a neutrosophic version of this cryptosystem [8].

A problem with this translation is the choice of modulus. In the classical Paillier cryptosystem, the modulus is based on ordinary primes [8]. For neutrosophic integers, ordinary neutrosophic primes do not provide a suitable modulus corresponding to the classical Paillier modulus [3, 4]. Therefore, this paper introduces neutrosophic paired-primes as a formal definition inspired by methods used in previous research on neutrosophic cryptography [5]. This gives the modulus used for the neutrosophic version of the Paillier cryptosystem.

This paper is built on known definitions and theorems from neutrosophic number theory [2–5, 9]. These definitions and theorems are stated in the preliminaries in relation to the isomorphism T, using the foundations of the AH-isometry [7]. Using this foundational theory, the paper establishes the translation from the classical Paillier cryptosystem to a neutrosophic version, where encryption, decryption, and homomorphic addition can be formulated over Z(I) by using a modulus based on neutrosophic paired-primes.

2. Materials and Methods

The arithmetic of neutrosophic rings of the form a + bI can be studied through a representation provided by the foundations of the AH-isometry by Abobala-Hatip [7]. This section presents existing definitions and theorems through the foundations of the AH-isometry.

2.1. Preliminaries

Definition 2.1 (Neutrosophic Ring of Integers [1]). Let R be any ring. The neutrosophic ring over R is R(I) = {a + bI; a, b ∈ R}, where the indeterminacy "I" satisfies $I^2 = I$. For R = Z, the ring Z(I) = {a + bI; a, b ∈ Z} is called the neutrosophic ring of integers.

Definition 2.2 (Positive Neutrosophic Integers [10]). If A = a + bI and B = c + dI are neutrosophic integers, then A ≤ B if and only if a ≤ c and a + b ≤ c + d. A positive neutrosophic integer is a number A = a + bI, where a > 0 and a + b > 0.

Theorem 2.3 (The AH-isometry [7]). Let R(I) = {a + bI; a, b ∈ R} be the neutrosophic ring with $I^2 = I$. The one-dimensional AH-isometry is the map T : R(I) → R × R given by T(a + bI) = (a, a + b). In particular, for R = Z, this gives the map T : Z(I) → Z × Z defined by the same formula. Moreover, its inverse is $T^{-1}(x, y) = x + (y-x)I$.

Proof. Let $(x, y) \in R \times R$. Then $T(T^{-1}(x, y)) = T(x + (y-x)I) = (x, x + y-x) = (x, y)$. Similarly, for $a + bI \in R(I)$, $T^{-1}(T(a + bI)) = T^{-1}(a, a+b) = a + ((a+b)-a)I = a + bI$. Hence T^{-1} is the inverse of T, so T is bijective.

Lemma 2.4 (The AH-isometry is a ring isomorphism [7]). The AH-isometry $T : Z(I) \to Z \times Z$, $T(a + bI) = (a, a+b)$, is a ring isomorphism, where Z×Z is equipped with componentwise addition and multiplication.

Proof. Let $A = a+bI$ and $B = c+dI$ be elements of Z(I). For addition, $A + B = (a+c) + (b+d)I$, so $T(A+B) = (a+c, a+c+b+d) = (a,a+b) + (c,c+d) = T(A) + T(B)$. For multiplication, using $I^2 = I$, $AB = (a+bI)(c+dI) = ac + (ad+bc+bd)I$, so $T(AB) = (ac, ac+ad+bc+bd) = (ac, (a+b)(c+d)) = (a,a+b)(c,c+d) = T(A)T(B)$. Thus T preserves addition and multiplication. Since T is bijective by Theorem 2.3, T is a ring isomorphism.

We recall the standard definitions from neutrosophic number theory and translate them under the ring isomorphism T.

Definition 2.5 (Addition [1, 7]). For $A = a+bI$ and $B = c+dI$, $T(A+B) = T(A)+T(B) = (a+c, a+b+c+d)$, and using T^{-1}, $A+B = (a+c) + (b+d)I$.

Definition 2.6 (Multiplication [1, 7]). For $A = a+bI$ and $B = c+dI$, $T(A \cdot B) = T(A) \cdot T(B) = (ac, ac+ad+bc+bd)$, and using T^{-1}, $A \cdot B = ac + (ad+bc+bd)I$.

Definition 2.7 (Neutrosophic Exponentiation [2, 5, 7]). For $A = a+bI$ and $B = c+dI$, $T(A\hat{}B) = T(A)\hat{}T(B) = (a^c, (a+b)\hat{}(c+d))$, and using T^{-1}, $A\hat{}B = a^c + ((a+b)\hat{}(c+d) - a^c)I$.

Definition 2.8 (Divisibility [2, 3, 7]). Let $A = a+bI$ and $B = c+dI$ be neutrosophic integers. We say $A \mid B$ if there exists $Q \in Z(I)$ such that $B = Q \cdot A$. Using T, this is equivalent to $(a,a+b) \mid (c,c+d)$; hence $A \mid B$ iff $a \mid c$ and $(a+b) \mid (c+d)$.

Definition 2.9 (Division [2, 4, 7, 9]). Let $A = a+bI$ and $B = c+dI$ be neutrosophic integers with $c > 0$ and $c+d > 0$, and assume $B \mid A$. Then $A/B = T^{-1}(a/c, (a+b)/(c+d)) = a/c + [(a+b)/(c+d) - a/c]I$.

Definition 2.10 (Neutrosophic Primes [2, 3, 7]). Let $A = a+bI$, $B = c+dI$, and $P = p+qI$ be neutrosophic integers. P is a neutrosophic prime if, whenever P divides $A \cdot B$ for some A, B $\in Z(I)$, then P divides A or P divides B. The primes in Z(I) are of the following forms:

$$\pm(p+(1-p)I), \pm(p-(1+p)I), \pm(1+(p-1)I), \pm(1-(p+1)I)$$

where p is a positive prime in Z.

Remark 2.11 (Norm and Neutrosophic Primes [3]). Let A = a+bI. Using T, the norm of A is N(A) = a(a+b). Therefore, if N(A) = p, where p is a prime in Z, then A is a neutrosophic prime.

Definition 2.12 (Congruence Modulo a Neutrosophic Integer [2, 7]). Let A = a+bI, B = c+dI, M = m+nI. A ≡ B (mod M) if M divides A−B. Using T, this is equivalent to (m,m+n) ∣ (a−c, a+b−c−d); hence A ≡ B (mod M) iff a ≡ c (mod m) and a+b ≡ c+d (mod m+n). For m>0, m+n>0: A mod M = (a mod m) + (((a+b) mod (m+n)) − (a mod m))I.

Definition 2.13 (Greatest Common Divisor [2, 4, 7]). For A = a+bI, B = c+dI: gcd(A,B) = T^{-1}(gcd(a,c), gcd(a+b,c+d)) = gcd(a,c) + (gcd(a+b,c+d) − gcd(a,c))I.

Definition 2.14 (Least Common Multiple [4, 7]). For A = a+bI, B = c+dI: lcm(A,B) = T^{-1}(lcm(a,c), lcm(a+b,c+d)) = lcm(a,c) + (lcm(a+b,c+d) − lcm(a,c))I.

2.2. The Classical Paillier Cryptosystem

Before defining the neutrosophic version, we recall the classical Paillier cryptosystem and provide an example to show how encryption and decryption work.

Definition 2.15 (Paillier Cryptosystem [8]). Let n = pq, where p and q are two distinct large primes, and let λ = lcm(p−1, q−1). Let L(u) = (u−1)/n and choose a base g ∈ B ⊆ Z*_{n^2}, where B denotes the set of elements in Z*_{n^2} whose order is a non-zero multiple of n, such that gcd(L(g^λ mod n^2), n) = 1. The Paillier cryptosystem is then defined by the following steps [8]:

Step 1 (Plaintext and Randomness): let the plaintext be m ∈ Zn where m < n, and choose a random value r < n, r ∈ Z*_n.

Step 2 (Encryption): compute the ciphertext c = g^m r^n mod n^2, where c < n^2 and c ∈ Z*_{n^2}.

Step 3 (Decryption): given c ∈ Z*_{n^2}, the original plaintext is m = [L(c^λ mod n^2) / L(g^λ mod n^2)] mod n = L(c^λ mod n^2) · L(g^λ mod n^2)$^{-1}$ mod n, where the denominator denotes the multiplicative inverse modulo n.

Example 2.16 (Classical Paillier). Choose p = 5 and q = 7. Then n = pq = 35, and n^2 = 1225. Compute λ = lcm(4,6) = 12. We choose g = 36; since gcd(36,1225) = 1, g ∈ Z*_{1225}. Verify: g^λ mod n^2 = 36^{12} mod 1225 = 421, so L(421) = (421−1)/35 = 12; since gcd(12,35) = 1, g is valid.

Step 1: choose plaintext m = 10 (m ∈ Z35), and r = 4 (gcd(4,35) = 1, r ∈ Z*35).

Step 2: c = g^{10} 4^{35} mod 1225 = 1024. Since 1024 < 1225 and gcd(1024,1225) = 1, c ∈ Z*_{1225}.

Step 3: c^λ mod n^2 = 1024^{12} mod 1225 = 526, so L(526) = (526−1)/35 = 15. From above, L(g^λ) = 12, and 12^{-1} mod 35 = 3. Therefore m = 15·3 mod 35 = 45 mod 35 = 10. The decrypted plaintext is m = 10, the original plaintext.

3. Results

We now use the previous definitions to extend the classical Paillier cryptosystem to neutrosophic integers.

3.1. Extending the Cryptosystem to Neutrosophic Integers

The classical Paillier cryptosystem is based on a modulus n = pq, where p and q are distinct large classical primes [8]. Since the construction depends on modular arithmetic over Zn and Z*_{n^2}, a neutrosophic version requires a corresponding modulus in the ring of neutrosophic integers Z(I). The natural first attempt is to choose two neutrosophic primes P and Q, where N = PQ. However, this direct approach does not provide the desired structure, since the product of two neutrosophic primes does not necessarily produce a valid modulus, as the indeterminate part can be the trivial case. This is seen using Definition 2.10, where neutrosophic primes belong to one of four forms [3]. This gives the eight cases shown in Table 1 [3]:

Table 1. All cases for neutrosophic prime integers

Case	Form	Choice	P	T(P)
1	P=±(p+(1−p)I)	+	P = p+(1−p)I	(p, 1)
2	P=±(p+(1−p)I)	−	P = −p+(p−1)I	(−p, −1)
3	P=±(p−(1+p)I)	+	P = p+(−1−p)I	(p, −1)
4	P=±(p−(1+p)I)	−	P = −p+(1+p)I	(−p, 1)
5	P=±(1+(p−1)I)	+	P = 1+(p−1)I	(1, p)
6	P=±(1+(p−1)I)	−	P = −1+(1−p)I	(−1, −p)
7	P=±(1−(p+1)I)	+	P = 1+(−p−1)I	(1, −p)
8	P=±(1−(p+1)I)	−	P = −1+(p+1)I	(−1, p)

For $p > 0$, Table 1 shows that the positive neutrosophic prime cases are Case 1 and Case 5, shown in Table 2:

Table 2. Positive neutrosophic prime integers

Case	P	T(P)
1	$p+(1-p)I$	$(p, 1)$
5	$1+(p-1)I$	$(1, p)$

For a product $N = PQ$, there are three possible choices. If both factors are chosen from Case 1, $T(N) = (pq, 1)$. If both are from Case 5, $T(N) = (1, pq)$. In both cases, one component is trivial. If one factor is chosen from each case, $T(N) = (p, q)$; this avoids a trivial component, but it reveals the prime components directly.

Since n in classical Paillier is part of the public key pair (n, g), while the primes (p, q) are private [8], the modulus N should likewise be public in a neutrosophic version of Paillier, while its factors should remain private. Therefore, using neutrosophic primes alone does not provide a suitable modulus for the construction.

This motivates a construction closer to the classical form, where each neutrosophic factor has two prime components under T. This idea is similar to the approach used in the neutrosophic RSA algorithm introduced by Merkepci et al. in 2023 [5].

Definition 3.1 (Neutrosophic Paired-Prime Integer). A positive neutrosophic integer $A = a+bI$ is called a neutrosophic paired-prime integer if a and $a+b$ are distinct positive primes in Z. Since a and $a+b$ are distinct primes, $\gcd(a, a+b) = 1$.

Remark 3.2. Every positive neutrosophic paired-prime integer can be written as a product of two neutrosophic primes. If $A = a+bI$ is a neutrosophic paired-prime integer, then a and $a+b$ are positive primes in Z, and $T(A) = (a, a+b) = (a,1)\cdot(1,a+b)$. Thus A corresponds under T to the product of a Case 1 neutrosophic prime and a Case 5 neutrosophic prime.

To construct a modulus close to the classical modulus, we choose two neutrosophic paired-prime integers as private factors.

Definition 3.3 (Neutrosophic Paillier Modulus). Let $A = a+bI$ and $B = c+dI$ be distinct neutrosophic paired-prime integers with $\gcd(a,c) = 1$ and $\gcd(a+b, c+d) = 1$. The neutrosophic Paillier modulus is $N = A\cdot B$.

3.2. The Paillier Cryptosystem over Neutrosophic Integers

Step 1 (Parameter Setup): let A = a+bI and B = c+dI be distinct neutrosophic paired-prime integers, N = A·B = n1+n2I the modulus. Let Λ = lcm(A−1, B−1) = λ1+λ2I. The neutrosophic L-function is Lneutro(U) = (U−1)/N for U = u1+u2I, whenever U−1 is divisible by N in Z(I). The base G = g1+g2I is chosen such that G ∈ B ⊆ Z(I)*_{N²} with gcd(Lneutro(G^Λ mod N²), N) = 1. Here (N,G) is the public key pair; (A,B) are private.

Step 2 (Plaintext and Randomness): let M ∈ Z(I)N, M = m1+m2I with M < N, meaning m1<n1 and m1+m2<n1+n2. Choose a random neutrosophic value R ∈ Z(I)*N, R = r1+r2I, with R<N and gcd(R,N)=1, equivalently gcd(r1,n1)=gcd(r1+r2,n1+n2)=1.

Step 3 (Encryption): the ciphertext C = c1+c2I ∈ Z(I)*_{N²}, C<N², is C = G^M R^N mod N².

Step 4 (Decryption): M = [Lneutro(C^Λ mod N²) / Lneutro(G^Λ mod N²)] mod N = Lneutro(C^Λ mod N²)·Lneutro(G^Λ mod N²)$^{-1}$ mod N.

3.2.1. Verifying the Homomorphic Properties

The homomorphic properties of the neutrosophic Paillier construction follow from the structure of the isomorphism T. If M1 = m1+m2I and M2 = μ1+μ2I are in Z(I)N with M1<N, M2<N, their encryptions are C1 = G^M1 R1^N mod N² and C2 = G^M2 R2^N mod N², where R1,R2 ∈ Z(I)*N.

Using multiplication in Z(I)*_{N²}: C1C2 = (G^M1 R1^N)(G^M2 R2^N) mod N². Since exponentiation is componentwise under T (Definition 2.7), C1C2 = G^(M1+M2) (R1R2)^N mod N². Since R1,R2 ∈ Z(I)*N implies R1R2 ∈ Z(I)*N, this is an encryption of M1+M2 mod N. Hence D(C1C2) = M1+M2 mod N, i.e. the system is additively homomorphic.

The system also supports multiplication of a plaintext by a neutrosophic scalar. Let K = k1+k2I ∈ Z(I)N with k1≥0 and k1+k2≥0. If C = G^M R^N mod N², then C^K = (G^M R^N)^K mod N² = G^(KM) (R^K)^N mod N². Since R ∈ Z(I)*N, also R^K ∈ Z(I)*N, so C^K is an encryption of KM mod N, giving D(C^K) = KM mod N. Thus the neutrosophic Paillier construction preserves the usual Paillier homomorphic properties through T: D(E(M1)E(M2)) = M1+M2 mod N and D(E(M)^K) = KM mod N.

3.3. Examples of the Neutrosophic Paillier Cryptosystem

Example 3.4 (Neutrosophic Paillier Encryption and Decryption). If Alice wants to send Bob a message, Bob first chooses two distinct neutrosophic paired-prime integers A = 3+4I and

B = 11+2I, where A≠B, and 3, 7, 11, 13 are primes in Z, with gcd(3,11)=1 and gcd(3+4,11+2)=gcd(7,13)=1: valid neutrosophic paired-prime integers.

Bob computes the modulus: $N = A \cdot B = 3 \cdot 11 + (3 \cdot 2 + 4 \cdot 11 + 4 \cdot 2)I = 33 + 58I$. Then $\Lambda = \text{lcm}(A-1, B-1) = \text{lcm}(2+4I, 10+2I) = \text{lcm}(2,10) + (\text{lcm}(6,12) - \text{lcm}(2,10))I = 10 + 2I$.

The base $G = g1+g2I \in B \subseteq Z(I)^*\_\{N^2\}$, where $N^2 = (33+58I)^2 = 33^2 + ((33+58)^2 - 33^2)I = 1089 + 7192I$. This means G must lie in $Z(I)^*\_\{1089+7192I\}$; if G = N+1 = 34+58I, this holds, since $\gcd(G, N^2)=1$, equivalently gcd(34,1089)=gcd(92,8281)=1.

Bob keeps A, B and Λ private and publishes the public key (N,G). Alice uses Bob's public key and chooses a message M = m1+m2I where M<N and $M \in Z(I)\_\{33+58I\}$. Alice wants to encrypt the message 4+5I, which fits since 4<33 and 9<91.

Alice randomly chooses $R = 2+3I \in Z(I)^*N$ with R<N, verifying gcd(R,N)=1: gcd(r1,n1)=gcd(2,33)=1 and gcd(r1+r2,n1+n2)=gcd(5,91)=1; also R<N since 2<33 and 5<91.

Alice computes the ciphertext C = G^M R^N mod N^2 through the isomorphism T. Since T(G)=(34,92), T(M)=(4,9), T(R)=(2,5), T(N)=(33,91): $T(G^M) = (34,92)^(4,9) = (34^4, 92^9)$, and $T(R^N) = (2,5)^(33,91) = (2^{33}, 5^{91})$. Thus $T(G^M R^N) = (34^4 \cdot 2^{33}, 92^9 \cdot 5^{91})$. Since $T(N^2)=(1089,8281)$, Alice computes $C = T^{-1}(34^4 \cdot 2^{33} \bmod 1089, 92^9 \cdot 5^{91} \bmod 8281) = T^{-1}(569, 2595) = 569 + 2026I$.

The ciphertext sent to Bob is C = 569 + 2026I. Bob decrypts using $M = \text{Lneutro}(C^\Lambda \bmod N^2) \cdot \text{Lneutro}(G^\Lambda \bmod N^2)^{-1} \bmod N$. With T(C)=(569,2595), T(Λ)=(10,12), $T(N^2)=(1089,8281)$: $T(C^\Lambda \bmod N^2) = (569^{10} \bmod 1089, 2595^{12} \bmod 8281) = (232,1548)$, so $C^\Lambda \bmod N^2 = T^{-1}(232,1548) = 232+1316I$.

Then $\text{Lneutro}(C^\Lambda \bmod N^2) = (232+1316I-1)/(33+58I) = (231+1316I)/(33+58I) = T^{-1}(231/33, 1547/91) = T^{-1}(7,17) = 7+10I$.

Bob also computes $T(G^\Lambda \bmod N^2) = (34,92)^(10,12) \bmod (1089,8281) = (34^{10} \bmod 1089, 92^{12} \bmod 8281) = (331,1093)$, so $G^\Lambda \bmod N^2 = 331+762I$, and $\text{Lneutro}(G^\Lambda \bmod N^2) = (330+762I)/(33+58I) = T^{-1}(330/33, 1092/91) = T^{-1}(10,12) = 10+2I$.

The inverse of 10+2I modulo N is found through T: T(10+2I)=(10,12), T(N)=(33,91), so $(10,12)^{-1} \bmod (33,91) = (10^{-1} \bmod 33, 12^{-1} \bmod 91) = (10,38)$, giving $(10+2I)^{-1} \bmod N = T^{-1}(10,38) = 10+28I$.

Finally, M = (7+10I)(10+28I) mod (33+58I) = $T^{-1}((7,17)\cdot(10,38) \bmod (33,91)) = T^{-1}((70,646) \bmod (33,91)) = T^{-1}(4,9) = 4+5I$. Bob recovers the original plaintext M = 4+5I.

Example 3.5 (Homomorphic Properties). In the previous example, Alice sent an encrypted message M1 = 4+5I using the neutrosophic Paillier algorithm. Charlie does not know the original message, but has the ciphertext C1 = C = 569+2026I, and knows only the public modulus N, the public base G, and the ciphertext. Charlie wants to add his own message to the ciphertext so that Bob can receive the combined plaintext after decryption.

Charlie encrypts M2 = 6+I, valid since M2<N and M2 ∈ Z(I)_{33+58I}, choosing R2 = 4+I, valid since R2<N and gcd(R2,N)=1 (gcd(4,33)=1, gcd(5,91)=1). Then T(M2)=(6,7), T(R2)=(4,5), and Charlie computes $T(C2) = (34^{6}\cdot 4^{33} \bmod 1089,\ 92^{7}\cdot 5^{91} \bmod 8281) = (460,2322)$, so $C2 = T^{-1}(460,2322) = 460+1862I$.

Charlie multiplies the two ciphertexts: $T(C1C2) = (569,2595)\cdot(460,2322) \bmod (1089,8281) = (380,5303)$, so $C1C2 = T^{-1}(380,5303) = 380+4923I$, with $C1C2<N^2$ and $C1C2 \in Z(I)^*\_\{N^2\}$.

Charlie sends the combined ciphertext to Bob, who decrypts it using the same decryption factors as before (Lneutro(G^Λ mod N^2)=10+2I and $(10+2I)^{-1} \bmod N = 10+28I$). Since T(C1C2)=(380,5303): $T((C1C2)^{\wedge}\Lambda \bmod N^2) = (380,5303)^{\wedge}(10,12) \bmod (1089,8281) = (380^{10} \bmod 1089,\ 5303^{12} \bmod 8281) = (34,911)$. Then $Lneutro((C1C2)^{\wedge}\Lambda \bmod N^2) = T^{-1}((34-1)/33, (911-1)/91) = T^{-1}(1,10) = 1+9I$.

Bob decrypts: $D(C1C2) = (1+9I)(10+28I) \bmod (33+58I) = T^{-1}((1,10)(10,38) \bmod (33,91)) = T^{-1}(10,16) = 10+6I$. Since Bob has Alice's original plaintext M1 = 4+5I, he finds Charlie's message: M2 = D(C1C2) − M1 = (10+6I) − (4+5I) = 6+I.

This shows how Charlie can add his message to Alice's ciphertext without knowing Alice's plaintext. Bob decrypts the combined ciphertext and recovers Charlie's original plaintext from the decrypted sum.

4. Conclusion

In this paper, a neutrosophic version of the Paillier cryptosystem using neutrosophic integers has been presented, which is a system with homomorphic properties. The construction is based on the isomorphism T, which makes it possible to translate the classical Paillier formulas to a neutrosophic version using the neutrosophic integers. It has been shown that neutrosophic primes do not provide a suitable modulus for this construction

since they degenerate or directly expose the private parameters in the cryptosystem. Therefore, neutrosophic paired-prime integers were introduced so that the modulus can be constructed with a product structure in both components under T. Finally, the construction is illustrated by explicit examples of encryption, decryption, and homomorphic addition, where the original neutrosophic plaintext is recovered.

The purpose of this paper is to show how existing algorithms in cryptography can be translated into neutrosophic versions. This neutrosophic version of Paillier does not argue for a stronger cryptosystem, but rather corresponds structurally to two componentwise Paillier systems under T. This means that, in theory, an attack has to take both componentwise systems into account, although this does not by itself prove stronger security than classical Paillier. This question has to be investigated further. This also suggests further work on neutrosophic secure multi-party computation, where existing multi-party cryptographic methods can be investigated in a neutrosophic setting.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kandasamy, W.B.V.; Smarandache, F. Some Neutrosophic Algebraic Structures and Neutrosophic N-Algebraic Structures; Hexis: Phoenix, AZ, USA, 2006.

2. Abobala, M. Foundations of neutrosophic number theory. Neutrosophic Sets and Systems 2021, 39, 120–132.

3. Çeven, Y.; Tekin, Ş. Some Properties of Neutrosophic Integers. Kirklareli University Journal of Engineering and Science 2020, 6(1), 50–59.

4. Çeven, Y.; Çetin, Ö. The Greatest Common Divisors and The Least Common Multiples in Neutrosophic Integers. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2023, 27(3), 411–416.

5. Merkepci, M.; Abobala, M.; Allouf, A. The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm. Infinite Study 2023, 10(2), 69–74.

6. Merkepci, M.; Sarkis, M. An Application of Pythagorean Circles in Cryptography and Some Ideas for Future Non Classical Systems. Galoitica Journal of Mathematical Structures and Applications 2022, 2(2), 28–30.

7. Abobala, M.; Hatip, A. An Algebraic Approach to Neutrosophic Euclidean Geometry. Neutrosophic Sets and Systems 2021, 43(1), 10.

8. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology – EUROCRYPT '99; Stern, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 223–238.

9. Barbosa, R.P.; Smarandache, F. Neutrosophic One-Round Zero-Knowledge Proof. Plithogenic Logic and Computation 2024, 2, 49–54.

10. Abobala, M. Neutrosophic Real Inner Product Spaces. Neutrosophic Sets and Systems 2021, 43, 225–246.

Received: Dec. 21, 2025. Accepted: Sept. 8, 2026.