Plithogenic Logic and Computation

Journal Homepage: sciencesforce.com/plc

Plithogenic Log. Comp. Vol. 2 (2024) 49–54

Paper Type: Original Article

Neutrosophic One-Round Zero-Knowledge Proof

Ranulfo Paiva Barbosa [1,*] and Florentin Smarandache [2]

[1] Web3 Blockchain Entrepreneur; 37 Dent Flats, Monte de Oca, 11501, San José, Costa Rica; ranulfo17@gmail.com .

[2] Department of Mathematics & Sciences, University of New Mexico, Gallup, NM 87301, USA; smarand@unm.edu.

Received: 25 Apr 2024 **Revised:** 19 Jul 2024 **Accepted:** 20 Aug 2024 **Published:** 23 Aug 2024

Abstract

Zero-Knowledge Proofs (ZKPs) are cryptographic tools that enables one party, known as the prover, to prove to another party, the verifier, that a certain statement is true without revealing any information beyond the validity of the statement itself. We introduce the Neutrosophic One-Round Zero-Knowledge Proof protocol (N-1-R) ZKP, which is an extension of the One-Round (1-R) ZKP in the realm of Neutrosophic numbers. The N-1-R ZKP is the first Neutrosophic ZK protocol.

Keywords: Zero-Knowledge Proofs; Neutrosophic One-Round Zero-Knowledge Proof Protocol; Neutrosophic Zero-Knowledge Protocol.

1 | Introduction

Since Smarandache introduced Neutrosophy to study the basis, nature, and range of neutralities as well as their contact with ideational spectra in the 1990s [1], we have seen the emergence of neutrosophic algebraic structures such as neutrosophic groups and rings [2], neutrosophic numbers [3], single-valued neutrosophic sets (SVNSs) [4], Neutrosophic number theory [5], and several applications[6]. Kandasamy and Smarandache [2] defined Neutrosophic algebraic structures and inserted the algebraic symbol indeterminacy (I) with the logical property I2 = I.

The inception of neutrosophic number theory occurred in 2020 [5]. This nascent field witnessed the exploration of fundamental concepts including neutrosophic greatest common divisor (GCD) [7], neutrosophic Diophantine equations [8], neutrosophic Euler's function, and neutrosophic congruence [9]. Merkepci et al. suggested for the first time the idea of using neutrosophic numbers in cryptography [10]. In recent years, researchers have been actively developing neutrosophic versions of well-known cryptographic systems with the potential to enhance security, such as RSA [11], El Gamal [12], and Diffie-Hellman key exchange [13]. The Neutrosophic community has made significant progress, yet there remains substantial potential for advancing neutrosophic cryptography, especially considering the growing threats to traditional cryptographic systems and protocols.

Traditional cryptographic systems, such as those based on prime factorization (RSA) [14], discrete logarithm problem (DLP) [15], and elliptic curve cryptography (ECC) [16, 17], including TLS protocols [18], are susceptible to quantum attacks [19]. In this context, organizations like NIST (National Institute of Standards and Technology) proposed new algorithms that are potentially quantum resistant [20]. Unfortunately, the threats posed to cryptographic protocols by the emerging computing paradigm, MemComputing [21, 22], are

Corresponding Author: ranulfo17@gmail.com

https://doi.org/10.61356/j.plc.2024.2363

Licensee **Plithogenic Logic and Computation**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

not widely recognized yet. Unlike quantum computers, digital MemComputing machines (DMMs) can be constructed using standard electronic components [23].

None of the mentioned cryptographic systems were developed with Neutrosophic numbers. Since neutrosophic number theory emerged in 2020, it should be devised to start exploring ZKP protocols in the realm of Neutrosophic number theory.

In this paper, we explore a simple and efficient Zero-Knowledge Proof protocol (ZKP), the One-Round ZKP developed by Almuhammadi and Neuman [24], which basis resides in the Discrete Logarithm Problem (DLP) [24]. Historically, the DLP was used by Diffie-Hellman key exchange [15] marking the beginning of asymmetric cryptography in the 1970s. And considering this historic algorithm we chose it to start exploring the use of Neutrosophic numbers in the realm of ZKP. We intend to explore more modern approaches as lattices among others in the future.

The next section presents an overview of Neutrosophic number theory and section 3 presents a brief introduction to ZKP and the One-Round ZKP. In section 4, we introduce the Neutrosophic One-Round ZKP.

2 | Some Elements of Neutrosophic Number Theory

Definition 2.1. [25] Let Z be the ring of integers, we say that (I) = {a + bI; a b ∈Z} is the neutrosophic ring of integers.

Definition 2.2. [25]

a) let a +bI, and c + dI be two neutrosophic integers, then:

   a + bI ≤ c + dI if and only if a ≤ a + b ≤ c + d.

b) a + bI is called positive neutrosophic integer if a > 0 and a + b >0.

Example 2.3. 5 + 2I is a positive neutrosophic integer, that is because 5 >0, 5 + 2 = 7 >0.

Definition 2.4. [25] (Addition) Let a + bI, c + dI: (a + bI) + (c + dI) = (a + c) + (b + d)I (1)

Definition 2.5. [25] (Multiplication) Let a + bI, c + dI: (a + bI) * (c + dI) = ac + I(ad + bc + bd) (2)

Scalar Multiplication; Let x be a scalar (real number). Then:

α*(a + bI) = αa + αbI (3)

The AH-Isometry (Abobala-Hatip): [38] Let a + bI, the AH-Isometry relation is given by: f(a + bI) = f(a) + I [f(a + b) - f(a)]

Definition 2.6. [25] (Neutrosophic Exponentiation); Let a + bI, c + dI: $(a+bI)^{(c+dI)} = a^c + I[\,(a+b)^{c+d} - a^c\,]$ (4)

Definition 2.7. [25] (Division)

Let a + bI, c + dI: $\frac{a+bI}{c+dI} = \frac{a}{c} + I[\,\frac{a+b}{c+d} - \frac{a}{c}\,]$ (5)

Definition 2.8. [25] (Root Index n) Let a + bI, its Root index n is given by:

$\sqrt[n]{a+bI} = \sqrt[n]{a} + I\,[\,\sqrt[n]{a+bI} - \sqrt[n]{a}\,]$ (6)

3 | Zero-Knowledge Proofs Protocols

Zero-knowledge proofs (ZKPs) are cryptographic tools that enable one party, known as the prover, to prove to another party, the verifier, that a certain statement is true without revealing any information beyond the validity of the statement itself [26].

Since Goldwasser, Micali, and Rackoff laid the groundwork for ZKPs in the 1980s [26, 27, 28], other important properties as succinctness [29], non-interactive [30] were incorporated in the realm of ZKP paving the way to the emergence of several cryptographic primitives as ZK-SNARKS [31], Bulletproofs [32], ZK-STARKS [33] among others described on ZKP surveys [34-36].

The cornerstone upon which ZKPs applications are built is the verifiable computation, i.e., the ability to prove that an external computation was performed correctly without revealing the inputs or the computation process. This foundational attribute of ZKPs serves as a gateway to their two practical value propositions: succinctness and privacy [36].

Succinctness in ZKPs allows for the quick verification of the correctness of a computation without the extensive resources typically required for direct computation execution. Privacy, the second major value proposition, emerges from the intrinsic nature of ZKPs to prove the correctness of information without revealing the information itself. This characteristic is particularly transformative in scenarios where sensitive or confidential data is involved [36].

The ZKPs became important cryptographic methods in multiple areas, specifically, blockchain [35, 37] and non-blockchain applications [36].

3.1 | One-Round Zero-Knowledge Proof

Almuhammadi and Neuman [24] developed the One-Round ZKP (1-Round ZKP) for the Discrete Logarithm (DL) problem. That is, given a prime p, a generator g for the multiplicative group Zp, and b ∈ Zp, Peggy wants to prove in zero-knowledge that she knows x such that, $g^x \equiv b \ (mod\ p)$. She proves to Victor that her claim is true without revealing the 'x' value through the steps described in Table 1.

Table 1. One-round ZKP of DL problem.

Step		Peggy(P)	Victor(V)
0	Setup	g, p, b, x	g, p, b
1	V generates a random y		y
2	V sends $c \equiv g^y (mod\ p)$ to P	c	$c \equiv g^y (mod\ p)$
3	P sends $r \equiv c^x (mod\ p)$ to V	$r \equiv c^x (mod\ p)$	r
4	V verifies that $r \equiv b^y (mod\ p)$		

This is a one-round proof based on the framework. All parameters are set up at Step 0. There are no more auxiliary messages needed for this protocol [24]. The authors provide the proof of correctness:

Assuming Peggy knows the secret x, she just computes $r \equiv c^x (mod\ p)$ and sends r to Victor. Since Victor knows y, he can verify that:

$r \equiv b^y (mod\ p)$ ≡ gxy ≡ (gx)y ≡ $b^y (mod\ p)$.

If Peggy does not know x, Victor can verify easily that her claim is false [24].

The one-round protocol definitively establishes Peggy's knowledge of 'x' without divulging any information about 'x' to Victor. Almuhammadi and Neuman have demonstrated that non-interactive ZKPs offer superior efficiency in terms of computational resources and communication overhead. By eliminating the need for multiple rounds of interaction, these protocols accelerate execution and minimize latency [24].

4 | Neutrosophic One-Round ZKP

The Neutrosophic 1-Round ZKP to the Discrete Logarithm problem is an extension of the previous protocol in the realm of Neutrosophic numbers. Given the following neutrosophic numbers (in bold), **p**, **g**, **b**, **x**, where:

- **p** is a neutrosophic prime number, **p** = $p_1 + p_2I > 0$, i.e., p_1, $p_1 + p_2I > 0$

- **g** is a generator, **g** = $g_1 + g_2I$, i.e., g_1, $g_1 + g_2I > 0$
- **b** is given by, **b** = $b_1 + b_2I$
- **x** is given by, **x** = $x_1 + x_2I$

Peggy claims knowing **x** = $x_1 + x_2I$, such that: $\boldsymbol{g^x \equiv b\ (mod\ p)}$. From the Neutrosophic exponentiation [25], it follows that $\boldsymbol{g^x \equiv b\ (mod\ p)}$, is given by:

$$(g_1 + g_2I)^{(x_1+x_2I)} = {g_1}^{x_1}(mod\ p_1) + I[\ (g_1 + g_2)^{x_1+x_2}(mod\ p_1 + p_2) - {g_1}^{x_1}(mod\ p_1)\ ]$$

She proves to Victor that her claim is true without revealing the '**x**' value through the steps described in Table 2.

Table 2. Neutrosophic One-Round ZKP of DL problem.

Step		Peggy(P)	Victor(V)
0	Setup	**g, p, b, x**	**g, p, b**
1	V generates a random **y**		**y**
2	V sends $\boldsymbol{c \equiv g^y(mod\ p)}$ to P	$\boldsymbol{c}$	$\boldsymbol{c \equiv g^y(mod\ p)}$
3	P sends $\boldsymbol{r \equiv c^x(mod\ p)}$ to V	$\boldsymbol{r \equiv c^x(mod\ p)}$	**r**
4	V verifies that $\boldsymbol{r \equiv b^y(mod\ p)}$		

Step 1. Given the neutrosophic numbers (described previously): **p**, **g**, **b**, **x**.

Step 2. Victor chooses a neutrosophic number **y** = $y_1 + y_2I$.

Step 3. Victor computes $\boldsymbol{c \equiv g^y(mod\ p)}$, and sends **c** to Peggy. **c** is given by:

$$(g_1 + g_2I)^{(y_1+y_2I)} = {g_1}^{y_1}(mod\ p_1) + I[\ (g_1 + g_2)^{y_1+y_2}(mod\ p_1 + p_2) - {g_1}^{y_1}(mod\ p_1)\ ]$$

Step 4. Peggy sends to Victor, **r**, $\boldsymbol{r \equiv c^x(mod\ p)}$

Step 5. Victor verifies that $\boldsymbol{r \equiv b^y(mod\ p)}$

$$\boldsymbol{r \equiv c^x(mod\ p) \equiv g^{yx}(mod\ p) \equiv g^{xy}(mod\ p) \equiv b^y(mod\ p)}$$

$$\boldsymbol{r} \equiv {g_1}^{y_1x_1}(mod\ p_1) + I[\ (g_1 + g_2)^{(y_1+y_2)(x_1+x_2)}(mod\ p_1 + p_2) - {g_1}^{y_1x_1}(mod\ p_1)\ ]$$

$$\boldsymbol{r} \equiv {g_1}^{x_1y_1}(mod\ p_1) + I[\ (g_1 + g_2)^{(x_1+x_2)(y_1+y_2)}(mod\ p_1 + p_2) - {g_1}^{x_1y_1}(mod\ p_1)\ ]$$

$$\boldsymbol{r \equiv b^y(mod\ p)}$$

The Neutrosophic One-Round ZKP is the first ZKP using Neutrosophic number theory, and it opens a new research area to evaluate the potentiality of Neutrosophic cryptographic ZKP schemes against quantum-computer attacks, as well as, MemComputing digital machines attacks.

5 | Conclusion

We introduced the first Neutrosophic ZK protocol, the Neutrosophic One-Round Zero Knowledge Proof considering the Discrete Logarithm Problem. The use of Neutrosophy in the field of ZKP can, potentially, help improve the privacy and security of communications under insecure channels.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contributions

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Smarandache, F. A unifying field in Logics: Neutrosophic Logic. In Philosophy. American Research Press, 1-141, 1992.
[2] Kandasamy, W.B.V, and Smarandache, F. Basic Neutrosophic algebraic structures and their applications to fuzzy and Neutrosophic models. Hexis, 2004.
[3] Smarandache, F. Introduction to neutrosophic statistics. 2014.
[4] Wang, H.; Smarandache, F.; Zhang, Y.; and Sunderraman, R. 2010. Single valued SVNS sets, Multisp Multistruct 4: 410–413.
[5] Ceven, Y.; Tekin, S., Some Properties of Neutrosophic Integers. Kırklareli University Journal of Engineering and Science, Vol. 6, pp.50-59, 2020.
[6] El-Hefenaway, N., Metwally, M.A., Ahmed, Z.M., El-Henawy, I.M. A review on the applications of neutrosophic sets. J. Comp. Theor. Nanoscience, 13, 936-944, 2016.
[7] Ceven Y, Cetin, O. The greatest common divisors and the least common multiples in Neutrosophic integers. J. Natural & Applied Sciences, 27(3), 411-416, 2023.
[8] Sankari H, Abobala M. Neutrosophic linear Diophantine equations with two variables. Neutrosophic Sets and Systems, 38: 399-408, 2020.
[9] Abobada M. Foundations of Neutrosophic number theory. Neutrosophic Sets and Systems, 39: 120-132, 2021.
[10] Merkepci M, and 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.
[11] Merkepci M, Abobala M, Allouf A. The applications of fusion neutrosophic number theory in public key cryptography and the improvement of RSA algorithm. Fusion: Practice and Applications (FPA). 2023; 10(2):69-74.
[12] Merkepci M, Abobala M. Security model for encrypting uncertain based on refined Neutrosophic integers algorithm. Fusion: practice and applications (FPA), v. 10(2):34-41, 2023.
[13] Allouf A, 'An Era of Cryptography Based on Neutrosophic Number Theory', the Role of Cybersecurity in the Industry 5.0 Era [Working Title]. IntechOpen, Jul. 04, 2024. Doi: 10.5772/intechopen.114975.
[14] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126.
[15] Diffie W, Hellman M, New directions in cryptography. IEEE Transactions on Information Theory, 22(6): 644–654, 1976.
[16] Miller V, Use of Elliptic Curves in Cryptography. Advances in Cryptology — CRYPTO '85 Proceedings, 1986, 85: 417–426.
[17] Koblitz N, Elliptic curve cryptosystems. Mathematics of Computation. 1987, 48(177): 203–209.
[18] Duplys, P, Schmitz, R. TLS cryptography in-depth. Packt Publishing 2023.
[19] Petrenko A, Petrenko S. Applied quantum cryptoanalysis. River Publishers. 2023.
[20] https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
[21] Di Ventra M. Memcomputing: fundamentals and applications. Oxford University Press, USA, 2022.
[22] Sharp TA, Khare R, Pederson E and Traversa FL, "A Memcomputing approach to prime factorization," 2023 IEEE International Conference on Rebooting Computing (ICRC), San Diego, CA, USA, 2023, pp. 1-10.

[23] Zhang Y-H, Di Ventra M. Implementation of digital MemComputing standard electronic components. 2023. https://arxiv.org/pdf/2309.12437v1.
[24] Almuhammadi S and Neuman C. Security and privacy using one-round zero-knowledge proofs, Seventh IEEE International Conference on E-Commerce Technology (CEC'05), Munich, Germany, 2005, pp. 435-438.
[25] Abobala M. Partial foundation of neutrosophic number theory. Neutrosophic Sets and Systems. 2021; 39: 120-132.
[26] Goldreich O, Micali S, Rackoff C, The knowledge complexity of interactive proof-systems, in Proc. of the Seventeenth Annual ACM Symposium on Theory of Computing, STOC '85. New York, NY, USA: Association for Computing Machinery, 1985, p. 291–304
[27] Goldreich O, Micali S, Wigderson A, Proofs that yield nothing but their validity and a methodology of cryptographic protocol design, in 27th Annual Symposium on Foundations of Computer Science, 1986, p.174–187.
[28] Ben-Or M, Goldreich O, Goldwasser S, Hastad J, Kilian J, Micali S, Rogaway P, Everything provable is provable in zero-knowledge, in Advances in Cryptology—CRYPTO'88: Proceedings 8. Springer, 1990, p. 37–56.
[29] Bitansky N, Canetti R, Chiesa A, Tromer E, From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. IACR Cryptology ePrint Archive, vol. 2011, p. 443.
[30] Groth J, Short pairing-based non-interactive zero-knowledge arguments, in Advances in Cryptology ASIACRYPT 2010, M. Abe, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 321–340.
[31] Bitansky N, Canetti R, Chiesa A, Tromer E, From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. Proc. 3rd Innovations in Theoretical Comp. Science Conf. on - ITCS '2012. ACM. pp. 326–349.
[32] Bünz B; Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G, Bulletproofs: Short Proofs for Confidential Transactions and More. 2018 IEEE Symposium on Security and Privacy (SP). pp. 315–334.
[33] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M, Scalable, transparent, and post-quantum secure computational integrity, Cryptology ePrint Archive, Paper 2018/046, https://eprint.iacr.org/2018/046.
[34] Morais E, Koens T, Van Wijk C, Koren A, A survey on zero knowledge range proofs and applications, SN Applied Sciences, 1:1–17, 2019.
[35] Sun X, Yu FR, Zhang P, Sun Z, Xie W, Peng X, A survey on zero-knowledge proof in blockchain, IEEE network, 35 (4): 198–205, 2021.
[36] Lavin R, Liu X, Mohanty H, Norman L, Zaarour G, Krishnamachari B. A survey on the applications of Zero-Knowledge Proofs. 2024, https://arxiv.org/html/2408.00243v1.
[37] Zhan R, Xue R, Liu L, Security and privacy on blockchain, ACM Computing Surveys (CSUR), 52(3):1-34, 2019 https://arxiv.org/abs/1903.07602.
[38] Abobala M, Hatip A. An algebraic approach to neutrosophic Euclidean geometry. Neutrosophic Sets and Systems, 43:114-123.

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.