iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77686

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Cryptographic Utility of Quadratic Diophantine Equation $z^2 = n + 1$ in Secure Encoding Protocols

S. Shanmuga Priya[1], G. Janaki[2]
[1]*PG & Research Department of Mathematics, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy Tamil Nadu, India.*
[2]*PG & Research Department of Mathematics, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy Tamil Nadu, India.*

Abstract: ***This study explores the cryptographic utility of the quadratic Diophantine equation $z^2 = n + 1$. By utilizing the integer solutions of this relation, a secure framework is established for key generation and authentication, bridging the gap between Diophantine analysis and encoding.***
Keywords: Diophantine equation, quadratic, perfect square, cryptography, Integer solution.

I. INTRODUCTION

Among all number theorists, Diophantine equations are very well known and widely applied in the areas of network security and cryptography. Every day, many researchers solve a great number of Diophantine equations. The construction of Diophantine triples and special Diophantine triples is an attractive concept. The sequence $q_1 = \frac{1}{16}, q_2 = \frac{33}{16}, q_3 = \frac{68}{16}, q_4 = \frac{105}{16}$ was discovered by Diophantus of Alexandia. It satisfies the condition $q_i\, q_j = S^2 - 1, \forall\ i,j = 1,2,3,4$ where S is the rational number. The construction of an integer sequence has been a topic of many studies. The first theorem established by Cipu M, Filipin A, and Fujita Y in [1] indicates that any Diophantine triple whose second largest term is between the square and four times the square of the smallest one can be uniquely extended to a Diophantine quadruple by adding an element that is larger than the largest element in the triple. Park J proved the extensibility of $D(-1)$ pair under some constraints using the previous result of the solution of Pellian equation developed by the $D(-1)$ triplets in [2] . Adzaga N, Filipin A, Jurasic A proved that the set $\{2, b, c\}$ cannot be extended to irregular Dio-4 tuples for $2 < b < c$ in .[3] . But they achieved some families of c's which will depend on b's. Adzaga N, Dujella A, Kreso D, Tadic P proved the result in [4] that there are infinite families of Dio-triples which are D(n)-triples for two distinct as well as three distinct "n" with $n \neq 1$. Rihane SE, Luca F, Togbe A. of [5] proved that there are no Diophantine 4 tuples formed by pell numbers. In [6] , Zhang and Grossman proved necessary and sufficient criteria for the existence of integer z' by taking into account the Diophantine triples $\{e_1, e_2, e_3\}$ such that $e_j\, e_k + z' = c^2$ and $\forall\ k \neq j$ where $z' \in Z$. In [7], Bacic and Filipin found the extensibility of D(4) pairings by means of a pellian equation; but Earp – Lynch of [8] generalized the result to distinguish between the solutions of pellian equations for $D(l^2)$ dio-3 tuples.

Bonciocat NC, Cipu M, Mignotte M. of [9] made a novel research work on Diophantine quadruples. With the extra condition that $b_1 < b_2 < b_3$ with $b_1 = 3b_1$, Adedji KN, He B, Pinter A, Togbe of [10] treated the extensibility of the Diophantine 3-tuple $\{b_1, b_2, b_3\}$ and arrived at a conclusion that a quadruple cannot be formed from such a set. Further, they proved the regularity of every Diophantine triple that comprises the set $\{b_1, 3b_1\}$ and arrived at the same conclusion for $b_2 = 8b_1$. In [11], Saranya C, Janaki G found the half companion sequences of special Diophantine triplets that are formed using centered square numbers of ranks $n, n+1, n+2, n+3$ whereas Sangeetha V, Anupreethi T, Somanath M.of [12] formed the special Dio triples for different types of numbers of few ranks. In [13], Shanmuga Priya and Janaki found the half companion sequences of centered (4m+2)- Gonal numbers of Generalized ranks. Diophantine equations and D(m)-triples provide many theorems and results, but their applications are also very important. Many applications in cryptography have been found for their work. Encryption using various algorithms such as DES, AES is well known from [14]. The generalized pell's equation is used for Key generation in public key cryptography, which is found in [15]. Some other application of Diophantine equations and multiple encryption can be found from [16]. Nevertheless, the strength of an encryption algorithm is generally recognized to depend on key elements such as the secrecy of the key, processing time, and storage use.

In this article, an effort is made to find the application of the Diophantine triples obtained from the work [13].

II. PRELIMINARIES

Consider the Quadratic Diophantine Equation

$$z^2 = n + 1$$

This implies,

$$z = \sqrt{n+1}$$

The integer solution of the above equation exists if and only if $n + 1$ is a perfect square.

Alphabets	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code (z)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

III. ENCODING THE MESSAGE

For secure data exchange, the sender and recipient use a mutually agreed-upon numerical coding method (Table 1).

Table 1

The sender wants to send a message " **HEN COME**" to the receiver.

From the table 1, code for each letter in the message can be considered as follows.

$$\text{H} \rightarrow z = 8 \Rightarrow z^2 = 64 = 63 + 1 \Rightarrow n = 63$$
$$\text{E} \rightarrow z = 5 \Rightarrow z^2 = 25 = 24 + 1 \Rightarrow n = 24$$
$$\text{N} \rightarrow z = 14 \Rightarrow z^2 = 196 = 195 + 1 \Rightarrow n = 195$$
$$\text{C} \rightarrow z = 3 \Rightarrow z^2 = 9 = 8 + 1 \Rightarrow n = 8$$
$$\text{O} \rightarrow z = 15 \Rightarrow z^2 = 225 = 224 + 1 \Rightarrow n = 224$$
$$\text{M} \rightarrow z = 13 \Rightarrow z^2 = 169 = 168 + 1 \Rightarrow n = 168$$
$$\text{E} \rightarrow z = 5 \Rightarrow z^2 = 25 = 24 + 1 \Rightarrow n = 24$$

Alphabets	**H**	**E**	**N**	**C**	**O**	**M**	**E**
z	8	5	14	3	15	13	5
n	**63**	**24**	**195**	**8**	**224**	**168**	**24**

Utilizing "/" to separate the words, the message HEN COME is encoded as

63.24.195 /8.224.168.24

IV. DECODING THE MESSAGE

The received message "**63.24.195 /8.224.168.24**" can be decoded as follows:

$$n = 63 \Rightarrow z^2 = 64 \Rightarrow z = 8 \rightarrow \text{H}$$
$$n = 24 \Rightarrow z^2 = 25 \Rightarrow z = 5 \rightarrow \text{E}$$
$$n = 195 \Rightarrow z^2 = 196 \Rightarrow z = 14 \rightarrow \text{N}$$
$$n = 8 \Rightarrow z^2 = 9 \Rightarrow z = 3 \rightarrow \text{C}$$
$$n = 224 \Rightarrow z^2 = 225 \Rightarrow z = 15 \rightarrow \text{O}$$
$$n = 168 \Rightarrow z^2 = 169 \Rightarrow z = 13 \rightarrow \text{M}$$
$$n = 24 \Rightarrow z^2 = 25 \Rightarrow z = 5 \rightarrow \text{E}$$

Thus, the message "**63.24.195 /8.224.168.24**" is decoded as "HEN COME"

V. EXPERIMENTAL DATA

This process of encoding and decoding is carried out in python programming software and the output is shown in the following figures 1 and 2.

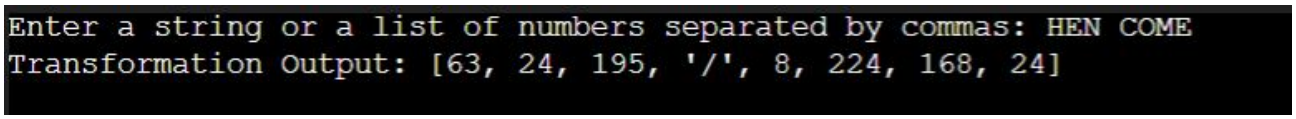


Fig 1. Output for Encoding

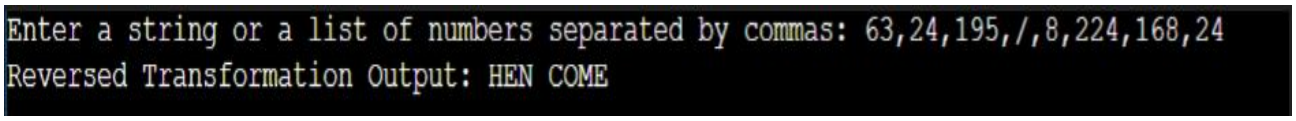


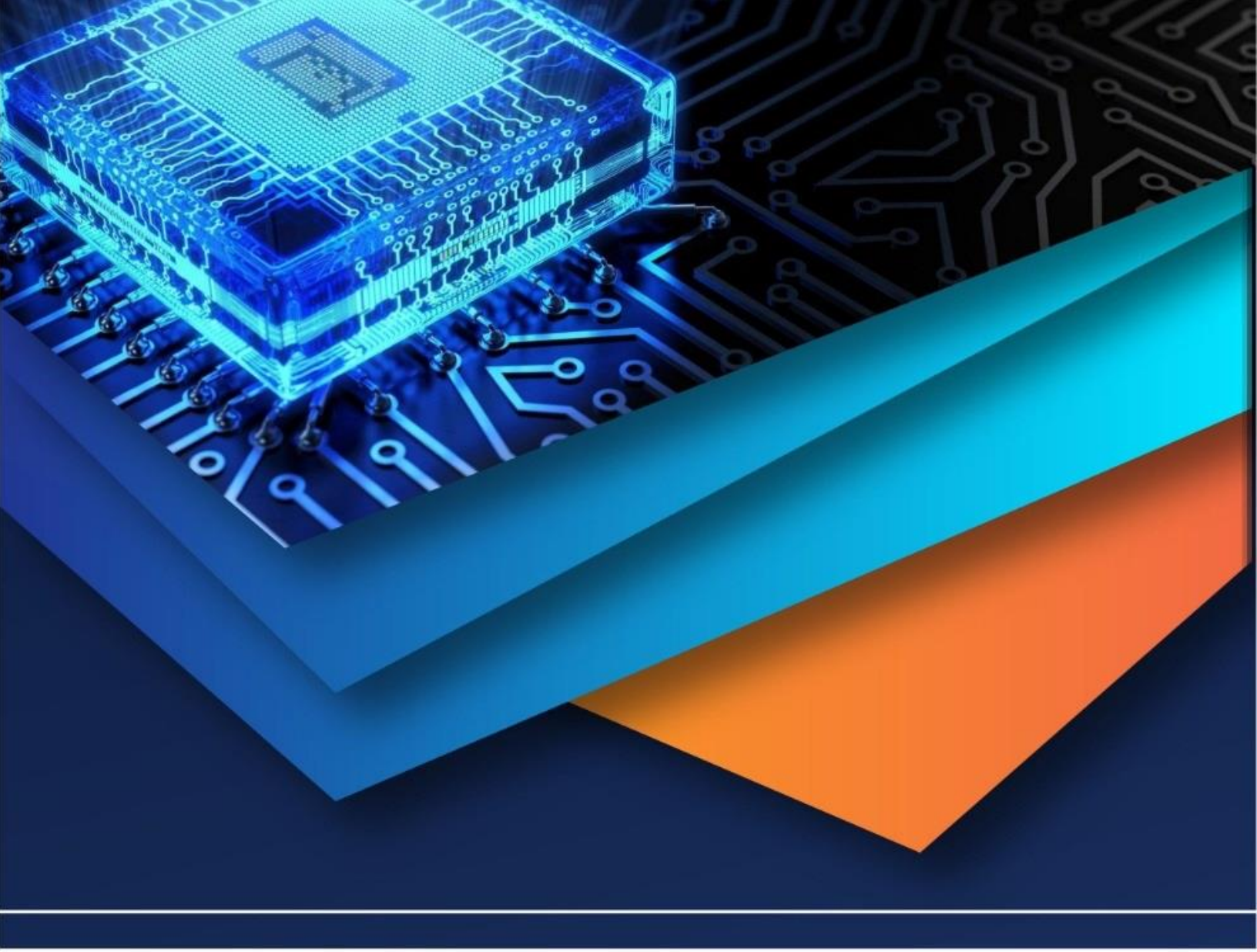
Fig 1. Output for Decoding

VI. CONCLUSIONS

Ultimately, the integration of the relation $z^2 = n + 1$ into cryptographic utility marks a significant step toward diversifying the mathematical foundations of cybersecurity. As digital threats evolve, the reliance on such elegant, yet complex, number theory relations will be essential in maintaining the integrity of global secure communications.

REFERENCES

[1] Cipu M, Filipin A, Fujita Y. Diophantine pairs that induce certain Diophantine triples. Journal of Number Theory. 2020 May 1;210:433-475. Available from: https://doi.org/10.1016/j.jnt.2019.09.019
[2] Park J. The extendibility of Diophantine pairs with property $ D (-1) $. Korean Journal of Mathematics. 2020 Sep 14;28(3):539-554. Available from: https://doi.org/10.11568/kjm.2020.28.3.539
[3] Adzaga N, Filipin A, Jurasic A. The extensibility of the Diophantine triple {2, b, c}. ANALELE STIINTIFICE ALE UNIVERSITATII OVIDIUS CONSTANTA-SERIA MATEMATICA. 2021 Jan 1;29(2):5-24. Available from: https://doi.org/10.2478/auom-2021-0016
[4] Adzaga N, Dujella A, Kreso D, Tadic P. Triples which are D (n)-sets for several n's. Journal of number theory. 2018 Mar 1;184:330-341. Available from: https://doi.org/10.1016/j.jnt.2017.08.024
[5] Rihane SE, Luca F, Togbe A. There are no Diophantine quadruple of Pell numbers. International journal of Number Theory. 2022;18(01):27–45. Available from: https://doi.org/10.1142/S179304212250004X
[6] Zhang Y, Grossman G. On Diophantine triples and quadruples. Notes Number Theory Discrete Math. 2015 Jan 1;21(4):6-16. Available from: https://nntdm.net/papers/nntdm-21/NNTDM-21-4-06-16.pdf
[7] Baćić L, Filipin A. The extensibility of $ D (4) $-pairs. Mathematical Communications. 2013 Nov 19;18(2):447-456. Available from: https://hrcak.srce.hr/file/163349
[8] Earp-Lynch B, Earp-Lynch S, Kihel O. On certain D (9) and D (64) Diophantine triples. Acta Mathematica Hungarica. 2020 Dec;162(2):483-517. Available from: https://link.springer.com/article/10.1007/s10474-020-01061-2
[9] Bonciocat NC, Cipu M, Mignotte M. There is no Diophantine D (− 1) D(-1)-quadruple. Journal of the London Mathematical Society. 2022 Jan;105(1):63-99. https://doi.org/10.1112/jlms.12507.
[10] Adedji KN, He B, Pinter A, Togbe A. On the Diophantine pair {a, 3a}. Journal of Number Theory. 2021 Oct 1;227:330-351. https://doi.org/10.1016/j.jnt.2021.03.011.
[11] Saranya C, Janaki G. Half Companion Sequences of Special Dio 3-Tuples Involving Centered Square Numbers. International Journal of Recent Technology and Engineering (IJRTE). 2019;8(3):3843–3845. Available from: https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5083098319.pdf
[12] Sangeetha V, Anupreethi T, Somanath M. Construction of Special Dio—triples. Indian Journal of Science and Technology. 2023 Oct 25;16(39):3440-3442. Available from: https://doi.org/10.17485/IJST/v16i39.1735.
[13] S. Shanmuga Priya, G. Janaki, A Unified Approach to Half-Companion Sequences in Diophantine Triples with Centered (4m+2)-Gonal Numbers, Boletim da Sociedade Paranaense de Matemática. 2026 Feb. 44(4). 1-9. https://doi.org/10.5269/bspm.79958.
[14] William Stallings, Cryptography and Network Security, Pearson, 7th edition, 2016.
[15] Koblitz, Neal, A survey of number theory and cryptography, Number Theory,Springer, 2000
[16] Raghunandan, KR and Ganesh, Aithal and Surendra, Shetty and Bhavya, Khanna, Key generation using generalized Pell's equation in public key cryptography based on the prime fake modulus principle to image encryption and its security analysis, Cybernetics and Information Technologies, 20(3), 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY