A Cryptographic Encryption Scheme based on a Pythagorean Triplets Manufacturing Formula

Nadav Voloch
Computer Engineering department
Ruppin Academic Center
Emek Hefer, Israel
nadavv@ruppin.ac.il

Noa Voloch - Bloch
Raicol Crystals Ltd
Rosh Ha'Ayin, Israel
noavoloch@gmail.com

2024 14th International Conference on Advanced Computer Information Technologies (ACIT) | 979-8-3503-5004-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ACIT62333.2024.10712620

***Abstract*—In the past decades cryptography and specifically encryption schemes were vastly researched. This is due to the developments in technology, communication, and the rising needs to use better, more resilient encryption for different types of attacks, that are getting more sophisticated and use much more computational power than before. For these encryption schemes, there is usually a use of mathematical computation, and different problems that are hard to solve, thus creating stronger schemes. There has been a use also in different classical problems of mathematics like computing prime numbers, using elliptic curves and lattices. In this paper we suggest a novel safe encryption scheme, that is based on a formula for manufacturing Pythagorean triplets (where both perpendiculars and hypotenuse are integers). We present the decryption and encryption formulas along with several examples of their operation and encoding results we achieved with the algorithm.**

Keywords—Cryptography, Cybersecurity, encryption, Pythagorean triplets

I. Introduction

In recent years, the field of cryptography has seen significant advancements and research due to advancements in technology, communication, and the increasing need for resilient encryption methods. This is driven by the emergence of sophisticated attacks that require immense computational power to overcome. To develop stronger encryption schemes, mathematicians have explored various mathematical computations and classical problems that are deemed hard to solve. This paper focuses on proposing a novel and secure encryption scheme rooted in the concept of Pythagorean triplets, a fundamental aspect of number theory. Pythagorean triplets are sets of three integers that satisfy the famous Pythagorean theorem. By leveraging the inherent properties of Pythagorean triplets, we aim to create a robust encryption system that ensures the confidentiality of data. Our approach involves formulating a specific formula for generating Pythagorean triplets, where all the three sides (hypotenuse and both perpendiculars) are integers. We present the encryption and decryption formulas derived from this novel scheme, highlighting the key steps and operations involved.

To demonstrate the effectiveness and efficiency of our encryption algorithm, we provide several examples showcasing the encryption and decryption process, along with the resulting encoded data. By exploring this unique cryptographic encryption scheme based on Pythagorean triplets, we hope to contribute to the existing body of knowledge in the field of cryptography and provide an alternative approach that offers enhanced security measures.

This paper proceeds as follows: firstly, we provide a detailed background and related work to the research that on its foundation we based our paper, then we present the problem formulation, and our methodology of solving it, including our unique algorithm. Finally, we showcase our results and evaluate the algorithm examples of manifestation.

II. Background and Related Work

Cryptography is the science of secure communication, used to protect sensitive information from unauthorized access or modification. It has a long and fascinating history dating back thousands of years, with its roots in ancient civilizations such as Egypt and Greece. Today, cryptography plays a crucial role in modern society by securing electronic communication channels ([1]), financial transactions ([2]), personal data storage systems ([3]) and many other critical infrastructure components ([4]). With the rise of digital technologies and the increasing complexity of cyber threats faced by governments and businesses alike, cryptography continues to be at the forefront of research in computer science. Famous cryptographic applications include encryption techniques such as symmetric key encryption algorithms (e.g., AES [5]) and asymmetric key encryption algorithms (e.g., RSA [6]). These and more are used for various cryptographic protocols like SSL/TLS ([7]) that are commonly used for secure online communication over the internet. Most as all cryptographic applications include a mathematical scheme of some sort ([8], [9], [10]).

Some of these applications take advantage of a certain property of mathematical object, or some sort of natural complexity certain mathematical problems have and create a cryptographic scheme using these properties to encapsulate the plain data and encrypt it.

Pythagorean triplets are sets of three positive integers that satisfy the famous Pythagorean theorem – $a^2 + b^2 = c^2$, where 'a', 'b' and 'c' represent the lengths of the sides of a right-angled triangle. These integer solutions have fascinated mathematicians for thousands of years due to their unique properties and applications in various fields such as number theory ([11]), geometry ([12]), and cryptography ([13]).

The study of Pythagorean triplets has been traced back to ancient civilizations such as Babylonian and Indian cultures who used them for practical purposes like constructing buildings with right angles. The Greek philosopher Pythagoras is also credited with developing many properties related to these triplets that are still studied today.

The use and combination of Pythagorean triplets in different uses is explored in papers such as [14] and [15], and for the early stages of this research, a basic scheme plan to devise was planned in [16], and some of the scheme ideas were developed in [17] and [18].

III. Methodology

A. The formula for manufacturing pythagorean triplets

The formula for manufacturing Pythagorean triplets is quite simple by nature, and for odd 'a' side (perpendicular)

lengths was developed by Pythagoras himself around 540 BC, and the formula for even 'a' side lengths was later developed by Plato, around 380 BC. The basic assumption is that for any given length of side 'a', that is ≥ 3, and an integer himself, of course, there will be a Pythagorean triplet by using this formula an odd 'a' side length:

$$b = \frac{a^2-1}{2}\,;c = b + 1 \qquad (1)$$

And for the case of even 'a' side length, the formula is:

$$b = (\frac{a}{2})^2 - 1\,;c = b + 2 \qquad (2)$$

The mathematical manufacturing of integer triplets reassures that by using this formula in encryption we can create an accurate encoding scheme.

B. Encryption/Decryption with the formula

For the purpose of encryption and decryption we have devised two algorithms that their scheme is based on the formulas in the previous subsection, along with another private key, that will be denoted here as $P_k = n$, and will be also used as another factor in the formula's scheme for decryption, as the power of the resulted hypotenuse in the encryption process and the root degree, accordingly, in the decryption process.

Both the encryption and decryption processes are depicted together in Fig.1, as we can see the encryption in the upper part of the figure, and the decryption process in its lower part, and in the decryption, we have to choose by two resulting options, only one would be integer, thus using our knowledge of the Pythagorean scheme, having all the sizes as integers.

The encryption and decryption algorithms, that their operation is also described in Fig.1 are as follows:

PythagorianEncryprion (Plaintext a, Private Key n)

If a is odd

$b \leftarrow \frac{a^2-1}{2}$

$c \leftarrow b+1$

else

$b \leftarrow (\frac{a}{2})^2 - 1$

$c \leftarrow b+2$

Cyphertext $ct \leftarrow c^n$

Return ct

PythagorianDecryprion (Cyphertext ct, Private Key n)

Plaintext pt ← *null*

$c \leftarrow \sqrt[n]{ct}$

$a_1 \leftarrow \sqrt{4c-4}$

$a_2 \leftarrow \sqrt{2c-1}$

If a_1 is int

$pt \leftarrow a_1$

else

$pt \leftarrow a_2$

Return pt

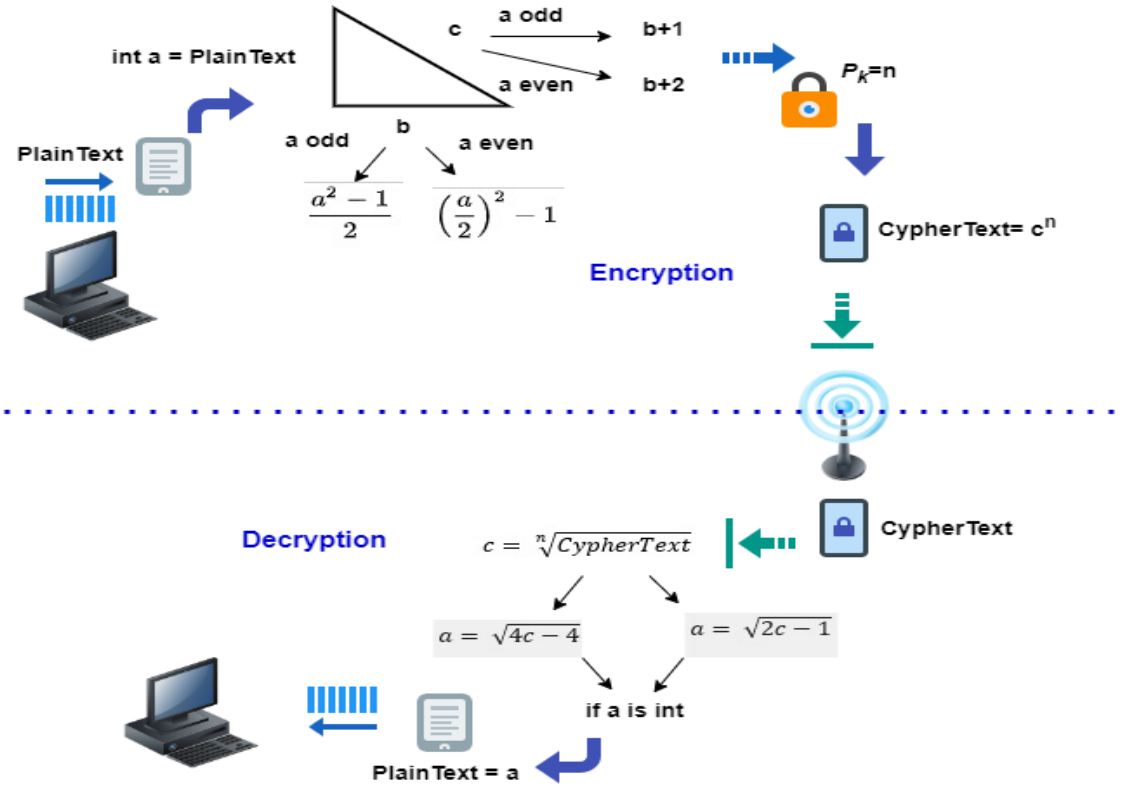

Fig. 1. Encrytion and decryption process using a pythagorean triplets formula

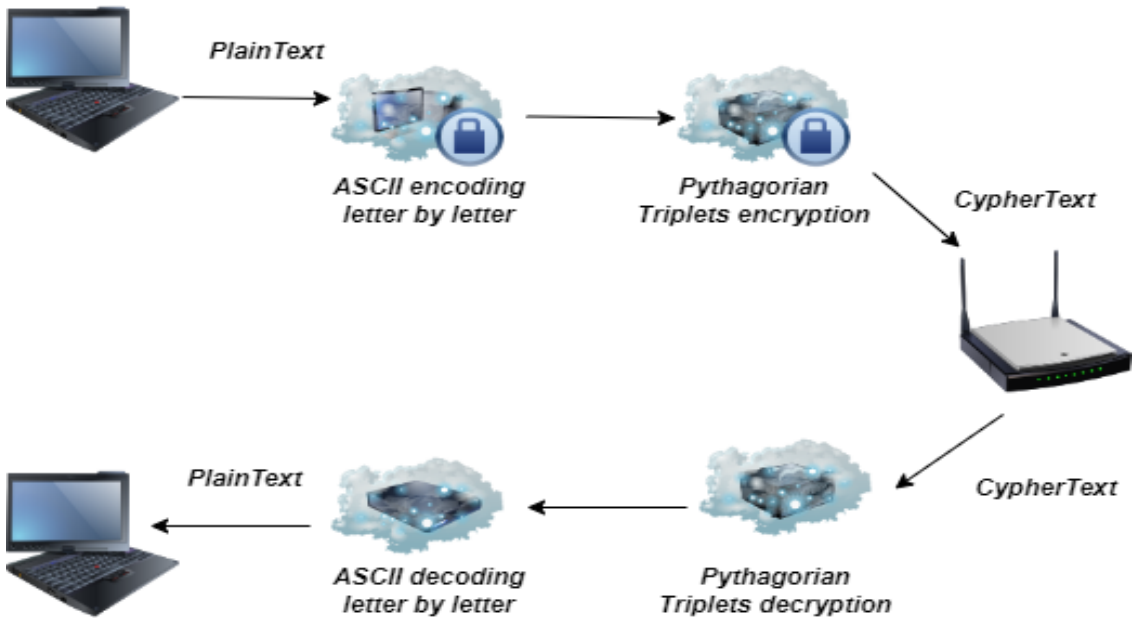

Fig. 2. The complete process of encoding and Pythagorian Triplets encryption of plaintext to cyphertext and the the other way round

IV. Results

For the purpose of this research, we have devised a Python based program that implements both the encryption and decryption algorithms presented above. This software can be seen in [19].

We have several examples of its operation and encoding results, with different plaintexts and cyphertext created by the algorithm, and implemented by the program, and are presented in Table I.

As we can see the plaintexts in the example are quite simple and can easily be ASCII codes that represent alphabet letters, creating a dictionary, that could be easily encoded into cyphertext using the algorithms.

Every letter has to encoded and decoded separately, thus creating turning complete plaintext sentences into long cyphertext codes. The process is depicted in Fig.2 where we can see the combination of ASCII encoding with the Pythagorean Triplets encryption to cyphertext, and then the other way round. As for these results, presented in Table I, the small-scale examples are presented just for the convenience of presentation, and any sort of private key *n* can be chosen, as for any kind of plaintext, to create large-scale cyphertexts. This means, of course, that we can add even another layer of encryption, depending on the method we choose to manipulate the numbers of the basic plaintext, creating maybe a multiplication of it, or even a power, making the scheme more secure, and even harder to break without knowing the method and the private key, of course.

TABLE I. Cyphertexts and Plaintexts Created by the Pythagorean Triplets Algorithm

CypherText	***n***	***c***	***b***	***PlainText(a)***
4913000	3	170	168	26
274625	3	65	63	16
440711081	3	761	760	39
1815848	3	122	120	22
1506138481	4	197	195	28
2773505125	3	1405	1404	53
321419125	3	685	684	37
18609625	3	265	264	23
2608757776	4	226	224	30
442050625	4	145	144	17
9597924961	4	313	312	25
844596301	5	61	60	11
10793861	3	221	220	21
11881376	5	26	24	10
1732323601	3	1201	1200	49
5929741	3	181	180	19
1349232625	3	1105	1104	47
389017000	3	730	728	54
148877000	3	530	528	46
1349232625	3	1105	1104	47

V. Comparison with other Methods and Limitations

The Pythagorean Triplets Encryption Scheme is a novel encryption method based on the mathematical properties of Pythagorean triplets. This method contrasts with established encryption schemes like RSA ([20]), AES ([21]), and ECC ([22]) by using integer-based operations. While RSA and ECC rely on complex mathematical problems (factoring large primes and elliptic curve logarithms, respectively), and AES uses a substitution-permutation network, the Pythagorean Triplets approach offers a new layer of complexity. It requires a private key and specific triplets, potentially providing enhanced security, although its practical effectiveness and robustness against modern cryptographic attacks need thorough evaluation. Another aspect is the private key *n,* that is an unlimited integer, and can be changed and varied according to the complexity desire of the user. Meaning a higher complexity can be achieved by choosing large powers. The full comparison of our scheme to these known encryption methods in several aspects is presented in Table II.

Encrypting each message character individually using Pythagorean triplets can be highly inefficient for large messages due to the large number of operations required. To handle this practical limitation, several strategies can be employed. One approach is to use block encryption, where multiple characters are grouped together into a block and the entire block is encrypted as a single unit, reducing the number of encryption operations. Another strategy is hybrid encryption, which combines symmetric and asymmetric encryption: the message is encrypted using a fast symmetric key algorithm like AES, and then the symmetric key is encrypted using the Pythagorean triplets' scheme. Stream encryption is another option, where a pseudo-random key stream generated by the Pythagorean triplets is XORed with the plaintext message. Additionally, optimizing the Pythagorean triplets' encryption algorithm itself through efficient mathematical computations and coding practices can enhance performance. Parallel processing techniques can also be utilized to encrypt multiple characters or blocks simultaneously, further improving efficiency.

TABLE II. Comparative analysis of the Pythagorean Triplets Encryption Scheme with RSA, AES, and ECC

Feature	ECC	AES	RSA	Pythagorean Triplets Encryption
Basis	Algebraic structure of elliptic curves	Substitution-permutation network	Mathematical difficulty of factoring large primes	Pythagorean triplets (integer sets satisfying $a^2+b^2=c^2$)
Algorithm Type	Public key (asymmetric)	Symmetric key (block cipher)	Public key (asymmetric)	Private key (integer-based operations)
Key Management	Requires key pairs (public and private)	Uses a symmetric key	Requires key pairs (public and private)	Requires a private key and specific triplets
Security	High security with shorter key lengths	Strong cryptographic properties	Well-understood, robust security	Novel approach, less studied in cryptography
Performance	Efficient for key generation and operations	Highly efficient for large data	Computationally intensive but manageable	Depends on efficiency of triplet generation
Applications	Mobile devices, secure web communications, cryptocurrencies	Encrypting large volumes of data	SSL/TLS, digital signatures	Secure communication, integer-based operations
Examples of Use	Mobile and IoT devices, blockchain	Government communications, secure data storage	Secure web traffic, data encryption	Proposed novel encryption scheme
Strengths	High security with smaller keys, efficient	Fast and efficient, widely used	Widely adopted, robust against many attacks	Potential new layer of complexity and security
Limitations	Requires elliptic curve knowledge, complex implementation	Symmetric key distribution challenges	Requires larger keys for higher security	Needs thorough evaluation for practical use

VI. Efficiency, Time Complexity and Robustness Against Attacks

The efficiency and time complexity of the proposed Pythagorean Triplets Encryption Scheme are crucial factors in determining its practical applicability, especially for large-scale data encryption. The scheme relies on generating Pythagorean triplets and performing integer-based operations for encryption and decryption. The time complexity of generating Pythagorean triplets is relatively low, as it involves simple arithmetic operations.

However, the overall efficiency can be impacted by the need to handle each character or block of data individually. For small messages or when encrypting individual characters, the computational overhead is minimal, making the scheme relatively efficient. However, as the size of the message increases, the number of required operations grows linearly, leading to potential inefficiencies. The use of a private key $P_k=n$ in the encryption process, where ciphertext ct is computed as c^n, and the corresponding decryption process, which involves calculating the root of the ciphertext, introduces additional computational steps.

These steps, although polynomial in nature, can become significant when dealing with very large messages or high values of n. To address this, the scheme can benefit from optimizations such as block encryption, where multiple characters are grouped and encrypted as a single unit, thereby reducing the total number of encryption operations. Furthermore, the algorithm can be enhanced through parallel processing techniques, enabling simultaneous encryption of different blocks, thus improving throughput. The proposed method's efficiency is also influenced by the hardware capabilities, as modern processors with high computational power can handle the required arithmetic operations more swiftly. In summary, while the Pythagorean Triplets Encryption Scheme presents a novel approach with a relatively straightforward time complexity for generating triplets, its practical efficiency for large-scale encryption depends on leveraging optimizations like block encryption, parallel processing, and algorithmic enhancements to manage the computational load effectively.

The resistance of the Pythagorean Triplets Encryption Scheme to cryptanalysis is a pivotal aspect in evaluating its robustness and security. This scheme's novel approach, leveraging the mathematical properties of Pythagorean triplets, inherently provides a certain level of complexity that can thwart basic cryptanalytic efforts. However, to thoroughly understand its security, one must analyze its resistance against common cryptographic attacks such as ciphertext analysis and statistical attacks. Ciphertext analysis, which involves examining the ciphertext to deduce patterns or correlations that might reveal the plaintext, can be challenging against this scheme due to the unique nature of the triplet-based encryption. Each triplet's generation and the use of a private key introduce significant variability, making it difficult for an attacker to predict the relationship between the ciphertext and the plaintext. Furthermore, since the encryption involves exponentiation and root extraction based on the private key, the resultant ciphertext exhibits non-linear properties that are not easily decipherable through simple analytical techniques.

Statistical attacks, which exploit frequency analysis and other statistical properties of the ciphertext to infer the plaintext, are also mitigated by this scheme. In traditional ciphers, certain characters or blocks may appear more frequently, which can be a vulnerability. However, the Pythagorean Triplets Encryption Scheme disperses the frequency distribution due to the mathematical transformations involved in generating the triplets and encoding the ciphertext. The randomness introduced by the Pythagorean triplets, coupled with the private key's influence on the encryption process, ensures that even identical plaintext characters or blocks are likely to produce distinct ciphertexts. This significantly complicates any attempts to apply frequency analysis or identify statistical patterns that could lead to successful decryption without the key.

Moreover, the scheme's resistance is further enhanced by the potential to employ additional cryptographic techniques, such as padding and salting, which can introduce extra layers of randomness and security.

By incorporating these methods, the encryption process can obscure any residual patterns that might otherwise be exploited in a statistical attack. Overall, while the Pythagorean Triplets Encryption Scheme presents a unique and theoretically sound approach to encryption, its practical resistance to cryptanalysis relies on the inherent complexity of the triplet generation and the robust handling of plaintext variability. Continuous evaluation and potential integration of supplementary cryptographic measures will be essential to fortify its defenses against advanced cryptanalytic techniques and ensure comprehensive security in real-world applications.

VII. Conclusion and Future Work

In conclusion, this paper introduces a novel cryptographic encryption scheme based on the properties of Pythagorean triplets. By leveraging the inherent mathematical structure of these triplets, we have developed robust encryption and decryption formulas that ensure the confidentiality and security of data.

The implementation of these formulas in a Python-based program has demonstrated their effectiveness through various examples. Our results confirm that the proposed encryption scheme can accurately encode plaintext into ciphertext and decode it back to plaintext using the generated Pythagorean triplets.

The Pythagorean Triplets Encryption Scheme presents a unique approach to cryptographic security by utilizing integer-based operations, contrasting with traditional schemes such as RSA, AES, and ECC.

While our initial results are promising, indicating the potential of this method in providing enhanced security, further evaluation is necessary to assess its robustness against modern cryptographic attacks.

Future work will focus on several key areas:

1. **Application in Various Domains**: We plan to explore the application of this encryption scheme in different fields, such as traffic navigation, secure communications, and data storage. Integrating the Pythagorean Triplets Encryption Scheme with existing technologies could provide additional layers of security in these domains.
2. **Algorithm Optimization**: Enhancing the efficiency of the encryption and decryption algorithms is crucial for

practical use. We aim to implement block encryption and parallel processing techniques to improve performance, especially for large-scale data encryption.

3. **User-Friendly Software Development**: Developing a comprehensive, user-friendly program that includes ASCII decoding and a graphical interface will facilitate wider adoption. This program will allow users to input natural language sentences, automatically encrypt them using the Pythagorean Triplets method, and choose suitable private keys randomly.
4. **Security Analysis**: Conducting extensive security analyses to evaluate the scheme's resistance to various types of cryptographic attacks, such as ciphertext analysis and statistical attacks, will be a priority. Understanding the scheme's strengths and potential vulnerabilities will guide further refinements to enhance its robustness.
5. **Integration with Other Cryptographic Methods**: Investigating the combination of the Pythagorean Triplets Encryption Scheme with other cryptographic methods could yield hybrid solutions that leverage the strengths of multiple approaches. For instance, integrating this scheme with symmetric key algorithms like AES could enhance overall security and efficiency.
6. **Experimental Validation**: Performing large-scale experimental validations and benchmarking against established encryption methods will provide valuable insights into the practical applicability and performance of the proposed scheme.

Through these future endeavors, we aim to advance the field of cryptography by providing an alternative, mathematically grounded encryption method that offers robust security measures. Continuous research and development will be essential to fully realize the potential of the Pythagorean Triplets Encryption Scheme and its contributions to secure communication and data protection. An interesting research direction is to explore different communication schemes that need solutions of encryption, with different types of communication protocols, and not just trivial ones, as described in [23].

ACKNOWLEDGMENTS

The authors wish to acknowledge Ruppin Academic Center for its support in the different stages of this research.

REFERENCES

[1] Saraireh, S. (2013). A secure data communication system using cryptography and steganography. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *5*.

[2] Rivest, R. L. (2005, July). Perspectives on financial cryptography. In *Financial Cryptography: First International Conference, FC'97 Anguilla, British West Indies February 24–28, 1997 Proceedings* (pp. 145-149). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. *Information Sciences*, *387*, 103-115.

[4] Breiling, B., Dieber, B., Pinzger, M., & Rass, S. (2021). A cryptography-powered infrastructure to ensure the integrity of robot workflows. *Journal of Cybersecurity and Privacy*, *1*(1), 93-118.

[5] Dworkin, M. J., Barker, E. B., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Dray Jr, J. F. (2001). Advanced encryption standard (AES).

[6] Rivest, R. L. (1985). RSA chips (past/present/future). In *Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, April 9–11, 1984 3* (pp. 159-165). Springer Berlin Heidelberg.

[7] Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. *Applied Computing and informatics*, *10*(1-2), 68-81.

[8] Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

[9] Buchmann, J. (2004). *Introduction to cryptography* (Vol. 335). New York: Springer.

[10] Koblitz, N. (2007). The uneasy relationship between mathematics and cryptography. *Notices of the AMS*, *54*(8), 972-979.

[11] Kubota, K. K. (1972). Pythagorean triples in unique factorization domains. *The American Mathematical Monthly*, *79*(5), 503-505.

[12] Bonsangue, M. V. (1997). A geometrical representation of primitive Pythagorean Triples. *The Mathematics Teacher*, *90*(5), 350-354.

[13] Kak, S., & Prabhu, M. (2014). Cryptographic applications of primitive Pythagorean triples. *Cryptologia*, *38*(3), 215-222.

[14] Kak, S. (2010). Pythagorean triples and cryptographic coding. arXiv preprint arXiv:1004.3770.

[15] SRIDEVI, K., & Thiruchinapalli, S. (2023). Cryptographic coding to define Binary Operation on Set of Pythagorean triples. Materials Today: Proceedings, 80, 2027-2031.

[16] Voloch, Benjanin (1996), Ben Gurion University of the Negev, & Baruch, Moshe (2005), The Hebrew University of Jerusalem, Israel. Private communication.

[17] Voloch, N. (2017). MSSP for 2-D sets with unknown parameters and a cryptographic application. *Contemp. Eng. Sci.*, *10*(19), 921-931.

[18] Voloch, N., Birnbaum, E., & Sapir, A. (2014, December). Generating error-correcting codes based on tower of Hanoi configuration graphs. In *2014 IEEE 28th Convention of Electrical & Electronics Engineers in Israel (IEEEI)* (pp. 1-4). IEEE.

[19] https://github.com/nadavvoloch/PythagorianTripletEncription

[20] Rivest, R. L. (1985). RSA chips (past/present/future). In Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, April 9–11, 1984 3 (pp. 159-165). Springer Berlin Heidelberg.

[21] Dworkin, M. J., Barker, E. B., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Dray Jr, J. F. (2001). Advanced encryption standard (AES). NIST.

[22] Koblitz, N. (2007). The uneasy relationship between mathematics and cryptography. Notices of the AMS, 54(8), 972-979.

[23] Voloch, N., & Hajaj, M. M. (2022, November). Handling Exit Node Vulnerability in Onion Routing with a Zero-Knowledge Proof. In International Conference on Information Integration and Web (pp. 399-405). Cham: Springer Nature Switzerland.