Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-2007

Rivest-Shamir-Adleman encryption system cracking with the triangular number factoring technique

Brithon D. Ndenje [‡]
Department of Mathematics
Morogoro Teachers College
P. O. Box 691
00255
Morogoro

Buberwa M. Tibesigwa [†]
Department of Architecture and Art Design
College of Architecture and Construction Technology
Mbeya University of Science and Technology
P. O. Box 131
Mbeya City Council
Mbeya 00255
Tanzania

Mrindoko Nicholaus [§]
Department of Computer Science and Engineering
College of Information and Communication Technology
Mbeya University of Science and Technology
P. O. Box 131
Mbeya City Council
Mbeya 00255
Tanzania

[†] *ORCID-ID:* **0000-0003-4035-6717**
[§] *ORCID-ID:* **0009-0003-0181-2342**

[‡] *E-mail:* **brithonndeje1@gmail.com**
[†] *E-mail:* **btibesigwaezra@hotmail.com**
[§] *E-mail:* **nicholausmrindoko@gmail.com**

Isack E. Kibona *
Department of Mathematics and Statistics
College of Science and Technical Education
Mbeya University of Science and Technology
P. O. Box 131
Mbeya City Council
Mbeya 00255
Tanzania

Abstract

Challenges in composite number factorization are critical to the fields of information systems security and cryptography. This study meticulously examined the features of triangular numbers and systematically created a Factoring Table for both triangular and non-triangular numbers, enabling the factorization of any composite number. In turn, the study presents a novel number factorization algorithm, derived from this table and articulated through both a formula and instructions. Furthermore, the demonstration of primality testing was revealed to differentiate it from composite numbers. The specified algorithm can enhance the knowledge and security of key generation for the Rivest-Shamir-Adleman (RSA) system.

Subject Classification: *68R01, 97N70.*

Keywords: *Composite number, Cryptography, Factoring table, Primality.*

1. Introduction

In number theory, factoring composite numbers into primes is well known mathematical problem since ancient times [1]. Indeed, it is acceptable that factoring is still challenging up to date [2]. However, this challenge gives an advantage for safety in cryptography and network security [3].

Mathematicians have introduced both classical and quantum algorithms for factoring positive integers [4]. Among others, these algorithms foremost includes Fermat's factoring method [5], Trial division method (TDM), Pollard-Strassen method, General number field sieve (GNFS), and Shor's algorithm for quantum computers [6]. Nonetheless, none of these best known algorithms can simply attack RSA encryption system to break (factorize) large composite numbers (public keys) which are used to secure large part of network data from Bank transactions to social media like twitter, E-mails, WhatsApp, Facebook and TikTok [7], [8]. Moreover, medical practitioners use similar technology to protect patient's medical information such as medical image protection as detailed by Singh et al. [9], [10].

* *ORCID-ID:* **0000-0003-0479-5173**

* *E-mail:* **iechibona@gmail.com (Corresponding Author)**

This article introduces an alternative factoring method capable of decomposing any positive integer, regardless of its magnitude. This alternative appears to be straightforward and requires little mathematics background beyond the operations of addition, subtraction, multiplication, and division of whole numbers.

Finally, unlike other current mathematical algorithms, this one allows a Grade 9 student to quickly determine whether a particular number, say 23, is prime or composite [11]. Following all that, a method called Triangular Number Factoring Method (TNFM) has been introduced.

2. Literature review

The RSA (Rivest-Shamir-Adleman) encryption algorithm, introduced in 1977, has long been one of the foundational systems for secure communications on the internet [12]. It is frequently utilized for secure key exchange, digital signatures, and the encryption of sensitive information [10]. The difficulty of factoring large composite numbers, particularly those created by multiplying two huge prime numbers, is the basis for RSA's security [13]. To break RSA, divide the public key (N) into two prime components (p and q) [14], [15]. Once these primes are known, the private key can be recovered, demonstrating the importance of factorization in RSA cryptanalysis [16]. Therefore, effectively factoring these big numbers or identifying other flaws in the algorithm's design or underlying presumptions constitutes breaking RSA. There are continuous attempts to crack RSA, and traditional factorization methods like the Quadratic Sieve [17] and Pollard's rho [18] show differing complexities and efficiency and frequently have difficulties with larger integers . This overview of the literature looked at current research developments and tactics meant to undermine the RSA encryption scheme.

2.1 Mathematical approaches: Integer Factorization

To break RSA, just solve the integer factorization problem, which involves identifying the two prime factors of the big composite number used as the public modulus (N) [19]. However, the approach depends on Fermat's factorization technique [20]. Over decades, scholars have investigated many methods targeted at efficient factorisation, including:

Brute Force Factorization: For small keys, brute force attempts to factor the RSA modulus can work [21], but the time complexity grows exponentially with larger key sizes, making this method impractical for key sizes used in modern cryptography (2048-bit keys and beyond) [22].

Fermat's Factorization: When the RSA modulus's prime factors are near to one another, this technique performs well [23]. Although not generally effective for breaking properly generated RSA keys, it can exploit poor key generation practices [24].

General Number Field Sieve (GNFS): The most effective classical algorithm for factoring huge integers at the moment is the GNFS. [25], making

it the primary method used in attacks against RSA [26]. Significant factorization milestones thus include:

RSA-768: Factored in 2009 by a team of researchers using the GNFS, demonstrating the vulnerability of smaller key sizes [14].

RSA-250: Factored in 2020, representing a modulus with 250 decimal digits, another milestone using similar factorization techniques [27].

These successes have pushed the recommended RSA key sizes to 2048 bits or higher, beyond the reach of current factorization algorithms [28], [29].

2.2 *SHOR'S ALGORITHM: A Quantum Computing Technique*

One of the most often mentioned dangers to RSA is quantum computing. In 1994, Peter Shor introduced Shor's Algorithm, a quantum algorithm that can factor huge integers in polynomial time [30], which is exponentially quicker than classical techniques such as GNFS.

While no large-scale quantum computers exist yet to implement Shor's algorithm on RSA-sized integers [31], theoretical work suggests that once sufficiently large quantum computers are built, they could break RSA encryption within minutes or seconds. The quantum threat has sparked substantial interest in developing post-quantum cryptography [32], with the goal of transitioning to quantum-resistant algorithms before quantum computers become powerful enough to compromise current encryption standards [33].

2.3 *Side-Channel Attacks*

Instead of concentrating on cracking the fundamental mathematics, side-channel attacks, which take use of information that has been leaked during the encryption or decryption process [34], are another method of cracking RSA encryption.

Timing Attacks: These attacks take advantage of how long it requires an RSA implementation to encrypt or decrypt data. [35]. By measuring these time differences, an attacker can deduce information about the private key. Kocher (1996) first described such attacks in 1996 [36].

Attacks Using Power Analysis: These attacks examine how much power a gadget uses when doing cryptographic procedures [37]. By tracking variations in power consumption during encryption and decryption processes, Differential Power Analysis (DPA) can provide information on private keys [38].

Cache Timing Attacks: These leverage the behaviour of modern processors, particularly how the cache memory is accessed during cryptographic computations [39]. A well-timed cache analysis can expose sensitive data, including key bits.

Various countermeasures, such as blinding techniques and constant-time implementations, have been developed to mitigate side-channel attacks, but these remain practical threats, especially against poorly implemented RSA systems [40].

2.4 *Fault Attacks and Other Cryptanalytic Techniques*

Fault attacks try to alter the calculations so that the hidden key can be inferred by introducing flaws into the cryptographic process [41]. For RSA, one common fault attack is the *Bellcore Attack* [42], where induced faults during RSA signature generation can reveal the private key.

Another significant class of attacks is *Coppersmith's Attack.* It targets scenarios where some bits of the private key are known or where RSA is used with poorly chosen parameters, such as small public exponents or small private key leaks [43]. Coppersmith's method leverages lattice-based techniques to find small roots of polynomials, allowing an attacker to efficiently recover the private key under certain conditions [44].

2.5 *Recent Trends and Future Directions*

As of 2023, RSA remains secure when implemented correctly with sufficiently large key sizes (2048 bits or greater) and robust mitigation against side-channel attacks [45]. However, improvements in computing power (including quantum computation) and the development of new cryptanalytic techniques continue to raise worries about its long-term viability [46].

Post-Quantum Cryptography (PQC): Efforts are ongoing to build cryptographic methods that are secure against quantum assaults [47]. In July 2022, the US National Institute of Standards and Technology (NIST) unveiled the first batch of post-quantum algorithms that may potentially replace RSA and other susceptible methods in the face of quantum computing breakthroughs [48].

Hybrid Cryptographic Systems: Some researchers propose hybrid systems where RSA is combined with quantum-resistant algorithms, allowing a gradual transition to PQC while still benefiting from RSA's established security and efficiency [49].

Arnold's Factorization Algorithm: This algorithm targets semi-prime numbers and presents a three-step approach for factorizing large semi-primes in polynomial time. It has been demonstrated to factor semi-primes up to 12 digits using mathematical software, highlighting its potential to influence RSA security by enhancing factorization efficiency [50].

Preselected Integer Factorization: This method employs a sieve method in conjunction with polynomial selection to produce pairs of relationships. Subsequently, these pairings are employed to generate a matrix, which is then reduced to produce square numbers. This reduction process facilitates the factorization of large numbers, which has the potential to decrypt RSA passwords and compromise the encryption system[51] .

To sum up, the security of RSA encryption, while still robust for many current applications, faces growing challenges from both classical and quantum-based cryptanalysis. Quantum computing, in particular, poses a significant future threat, as Shor's algorithm could render RSA insecure once practical quantum computers become available. In the meantime, factorization attacks and side-channel attacks continue to improve, requiring careful implementation of RSA systems to maintain their security. The rise of post-quantum

cryptography represents a critical area for future research as cryptographers seek to pre-emptively address the vulnerabilities RSA will face in a post-quantum world.

While Samojluk [52] employed the properties of triangular numbers to construct public keys, this study did the inverse, demonstrated factorization of any composite number (public keys) based on properties of triangular numbers . We consider this not only as another way of consideration in the security of the public keys but also knowledge contribution in RSA encryption.

3. Material and Methods

3.1 *Triangular number factoring method (TNFM) and primality test*

Triangular numbers: are whole numbers represented as the half of a product of the two consecutive natural numbers, or are whole numbers expressed as a sum of the first n natural numbers. Examples: 1, 3, 6, 10, 15, 21, and so on. These are triangular numbers, and their general function denoted, $\Delta = \frac{n(n+1)}{2}$ where $\Delta = f(n)$ symbolize a triangular number.

3.1.1 Application of the properties of triangular numbers

Triangular numbers have unique properties which distinguishes them from other composite integers [53], that's to say: subtracting successively 1, 2, 3... up to n from $\frac{n(n+1)}{2}$ it ends up with zero. For example; $\frac{7(7+1)}{2} = \frac{7(8)}{2} = 28$ or 28= 1+2+3+4+5+6+7 then through subtraction steps (Fig. 1), 28 ends in zero.

1st step: 28-1=27
2nd step: 27-2=25
3rd step: 25-3=22
4th step: 22-4=18
5th step: 18-5=13
6th step: 13-6=7
7th step: 7-7=0

Figure 1
Subtraction Steps

This property (Fig. 1) helps to check the triangularity of a composite number i.e. if a given positive integer is a triangular number, it must end up in zero. Also, the property is used to find nth position of a triangular number.

One of the methods to find the nth position of a triangular number is by plugging the triangular number into $\Delta = \frac{n(n+1)}{2}$ and solving a quadratic equation, $n^2 + n - 2\Delta = 0$.

Given a triangular number, the differences after successive subtraction of natural numbers from it are called residues.

A residue at any subtraction step can be factorized. For example, suppose one want to factorize 22. Since 22 is the difference at a third subtraction step

from a triangular number, 28 that is 22 is a residue at a third step and its prime factors can be calculated by taking 3 (because 22 appeared at a third step) and taking care of the two factors which are consecutive natural numbers whose half of their product is 28 i.e. 7 and 8. Note that, always the factoring pair, has two consecutive natural numbers, one is an odd and the other is an even. To complete the factoring process, do the following:

Add 3 to a larger number (8), if the answer is an odd number take it as a factor of 22. If the answer is an even, then its half is a factor of 22. Next, subtract 3 from a smaller number (7), if the answer is an odd number take it as a factor of 22. If the answer is an even, its half is a factor of 22. So, the first factor of 22 is 8+3=11, and the second factor of 22 is ((7-3)/2) =4/2=2. Therefore, the factors of 22 are 11 and 2.

Flipping the same concept into a Table 1 which is a part of a list of all positive integers systematically arranged in order of increasing triangular and non-triangular numbers. On this factoring table, 22 can be factorized by using its subtraction step (a = 3) as it appears in a third diagonal. In this context, a diagonal sequence with triangular numbers is considered as a zero diagonal. A number a = 3 and m = 22 is then substituted into $d^2 + (2a + 1)d - 2m = 0$, resulting into d = -11 or 4. Consider the absolute values of the roots, d_1 and d_2, by dividing by 2 any even root, the resulting values are the factors of 22. That is, take the absolute value of -11 as factor of 22 and half of 4 as another factor of 22.

3.1.2 Factoring table properties

Table 1 systematically places triangular numbers in the diagonal assigned as zero diagonal, it is the only diagonal with triangular numbers. This table is part of an infinite size of the table that can be developed to include any existing triangular number. It is important to note that the zero diagonal is the only diagonal possessing zero in its lowest number.

3.1.2.1 First and subsequent diagonals

Like the zero diagonal, the first, second and so on diagonals have 1, 2, and so on respectively entries in their first entry. In the first diagonal, adding a first triangular number to the numbers completes triangularity of the numbers in this diagonal. Similarly, the second diagonal illustrates the same (adding a second triangular number completes the triangularity of all numbers in the second diagonal). It is clear that numbers in the third diagonal reveals the same and so on. Therefore, given any number outside the zero diagonal numbers, there exist a triangular number that can be added to it to complete triangularity.

3.1.2.2 The role of a and d values

The ‘a’ are entries in the first vertical column at the far left, the values correspond to the ath position triangular number that can be added to the numbers in this diagonal to make them complete triangularity. The ‘d’ are entries in the first row and one of the longest rows (there are only two longest

rows). The ds' are factor carrying values. That is, pick any number in the table, a number in the ds along with numbers on its left provides the factors to this number. In addition, the formula: $d^2 + (2a + 1)d - 2m = 0$ were developed by the author based on the role of a and d values, where m is any number in 3.1.

To sum up, while the zero diagonal ensures all triangular number to be listed in this table, the second vertical column ensures that all positive integers are accommodated in this table.

Table 1

The Factoring Table

a/d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0																					
	1																				
1		3																			
	2		6																		
2		5		10																	
	3		9		15																
3		7		14		21															
	4		12		20		28														
4		9		18		27		36													
	5		15		25		35		45												
5		11		22		33		44		55											
	6		18		30		42		54		66										
6		13		26		39		52		65		78									
	7		21		35		49		63		77		91								
7		15		30		45		60		75		90		105							
	8		24		40		56		72		88		104		120						
8		17		34		51		68		85		102		119		136					
	9		27		45		63		81		99		117		135		153				
9		19		38		57		76		95		114		133		152		171			
	10		30		50		70		90		110		130		150		170		190		
10		21		42		63		84		105		126		147		168		189		210	
	11		33		55		77		99		121		143		165		187		209		231
11		23		46		69		92		115		138		161		184		207		230	
	12		36		60		84		108		132		156		180		204		228		
12		25		50		75		100		125		150		175		200		225			
	13		39		65		91		117		143		169		195		221				
13		27		54		81		108		135		162		189		216					
	14		42		70		98		126		154		182		210						
14		29		58		87		116		145		174		203							
	15		45		75		105		135		165		195								
15		31		62		93		124		155		186									
	16		48		80		112		144		176										
16		33		66		99		132		165											
	17		51		85		119		153												
17		35		70		105		140													
	18		54		90		126														
18		37		74		111															
	19		57		95																
19		39		78																	
	20		60																		
20		41																			
	21																				
21																					
$d^2 + (2a + 1)d - 2m = 0$																					

General rule: Given the triangular number, to find the factors of the residue, add the subtraction step of a residue (R) to a larger number, and subtract it from a smaller number of the given triangular number. If the answer is an odd, take it as a factor of a residue and if the answer is an even, its half is a factor, the two becomes the factors of the residue.

3.2 *Completing the triangular*

Completing the triangular number is the key to this algorithm. If for any given composite number, you can complete the triangular then you have factorized it. Deduction from Table 1, captioned as Triangular Table: Every composite number (m) need addition of a triangular number to complete it into triangular number, Therefore, all composite numbers can be factorized.

4. Discussion and Conclusions

4.1 *Discussion*

This study has demonstrated applications of triangular numbers focusing on factorizing composite numbers. Clearly, applications are beyond factoring issues, that is triangular number properties may apply to test the primality of a number and location of composite number in the Factoring Table (Table 1). Systematically, a composite number, m can be factorized following the steps as indicated.

4.1.1 Steps for factoring a composite number, $\boldsymbol{m}$:

i. Calculate $2\boldsymbol{m}$
ii. Generate a sequence of terms between $\boldsymbol{m}$ and $2\boldsymbol{m}$ by adding successively 1,2,3,4,5,6... to $\boldsymbol{m}$
iii. Calculate the Greatest Triangular Number (GTN) less than $\boldsymbol{m}$ (GTN < $\boldsymbol{m}$): That is successively, subtract 1,2,3,4,5, 6... from $\boldsymbol{m}$ until you get the Least Positive Residue (LPR), this is a number of which no more subtraction can be made to make the difference of a positive integer. Then, $GTN = \boldsymbol{m} - LPR$
iv. Calculate n from $n^2 + n - 2GTN = 0$. Then, $n =$ Total number of subtracting steps.
v. Identify all triangular numbers between $\boldsymbol{m}$ and $2\boldsymbol{m}$ using the next natural numbers to n.
vi. Compare the two sequences generated in step ii and v respectively. Here, choose the Least Common Triangular number (LCT) or the Greatest Common Triangular number (GCT) of the two sequences. Note; if neither LCT nor GCT does exist, then $\boldsymbol{m}$ is a prime.
vii. Calculate a triangular completing number, Δ from $\boldsymbol{m} + \Delta = LCT$, so, $\Delta = LCT - \boldsymbol{m}$
viii. Calculate a from $a^2 + a - 2\Delta = 0$

ix. Solve for d from: $d^2 + (2a + 1)d - 2\boldsymbol{m} = 0$.The absolute values of the roots d_1 and d_2 virtually provides the factors of m.

x. Thus, choose as factors of $\boldsymbol{m}$ a set,$\left\{|\frac{d_1}{2}|, |d_2|\right\}$ if d_1 is even or $\left\{|d_1|, |\frac{d_2}{2}|\right\}$ if d_2 is even.

4.1.2 Primality test

Testing the primality of $k \geq 5$, consider the following steps.

i. Generate a sequence of k terms using $kn - \frac{n(n-1)}{2}$, for $n = 1, 2, 3, \ldots, k$

ii. Divide every term by k and take all remainders

iii. If the sum of all remainders is triangular then k is prime.

A sequence of k terms is simply be picked from the factoring table.

Example: Test the primality of 5. We first let $k = 5$ From the factoring table: the sequence is 5,9,12,14 and 15.

Dividing every term by 5 the remainders are 0,4,2,4,0

The sum of remainders is $4 + 2 + 4 = 10$

Here, 10 is a triangular number, therefore, 5 is a prime number.

5. Conclusion

The relation between factorizing a composite number and triangularity of a number systematically were studied by placing triangular number and non-triangular number in a table, called Factoring Table. It was observed that all positive integer which are non-triangular numbers require addition of another triangular number to become triangular number. Any composite number exists in the Factoring Table following the fact that all positive integers including zero can be placed in the table The numbers in the Factoring Table were systematically arranged such that choosing any composite number, two numbers 'a' and 'd' on the vertical and horizontal respectively are assigned to the given number. The two numbers could represent the prime components of a composite number, $\boldsymbol{m}$ as shown in the Factoring Table. The three a, d, and $\boldsymbol{m}$ are coupled in the relation $d^2 + (2a + 1)d - 2\boldsymbol{m} = 0$, the factors of $\boldsymbol{m}$ are in a set $\left\{|\frac{d_1}{2}|, |d_2|\right\}$ if d_1 is even or $\left\{|d_1|, |\frac{d_2}{2}|\right\}$ if d_2 is even. The Factoring Table respond beyond factors of a composite number to at least include triangularity completion and primality test. Therefore, at least the Factoring Table can reveal the factors of a composite number. Nevertheless, future may come up with more lessons about the Factoring Table.

Competing Interests

The authors declare that they have no competing interests.

References

[1] D. M. Bressoud, *Factorization and primality testing*. Springer Science & Business Media (2012).

[2] S. Goldwasser and S. Micali, 'Probabilistic encryption & how to play mental poker keeping secret all partial information', in *Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali*, pp. 173–201 (2019).

[3] J. Katz and M. Yung, 'Threshold cryptosystems based on factoring', in Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002 Proceedings 8, Springer, pp. 192–205 (2002).

[4] A. O. Pittenger, An introduction to quantum computing algorithms, vol. 19. Springer Science & Business Media (2012).

[5] P. Sharma, A. K. Gupta, and A. Vijay, 'Notice of violation of IEEE publication principles: Modified integer factorization algorithm using V-Factor method', in 2012 Second International Conference on Advanced Computing & Communication Technologies, *IEEE*, pp. 423–425 (2012).

[6] S. Y. Yan and S. Y. Yan, 'Quantum Algorithms for Integer Factorization', *Quantum Comput. Number Theory*, pp. 59–119 (2015).

[7] B. Kaliski, 'The mathematics of the rsa public-key cryptosystem', RSA Lab. (2006).

[8] A. E. Mezher, 'Enhanced RSA cryptosystem based on multiplicity of public and private keys', *Int. J. Electr. Comput. Eng.,* vol. 8, no. 5, p. 3949 (2018).

[9] K. D. Singh, P. Singh, G. L. Saini, and D. Panwar, 'Privacy-preserving cryptographic solutions for medical image protection : The secure force algorithm and intelligent encryption systems', *J. Discrete Math. Sci. Cryptogr.* (2024), doi: https://doi.org/10.47974/JDMSC-1926.

[10] Y. V. Lakshmi, K. Naveena, M. Ramya, N. Pravallika, T. Sindhu, and V. Namitha, 'Medical image encryption using enhanced Rivest Shamir adleman algorithm', in 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), *IEEE*, pp. 1–5 (2023).

[11] K. Ahmad, A. Kamal, and K. A. B. Ahmad, 'Prime number', in Emerging Security Algorithms and Techniques, Chapman and Hall/CRC, pp. 27–45 (2019).

[12] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, 'A secure hybrid RSA (SHRSA)-based lightweight and efficient personal messaging communication protocol', Digit. Twin Technol. Smart Cities, pp. 191–212 (2020).

[13] K. Balasubramanian and M. P. Pitchai, 'A survey of fermat factorization algorithms for factoring RSA composite numbers', *Multidiscip. Sci. J.* (2023), [Online]. Available: https://api.semanticscholar.org/CorpusID:267163601

[14] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, 'Systematic and critical review of rsa based public key cryptographic schemes: Past and present status', *IEEE Access*, vol. 9, pp. 155949–155976 (2021).

[15] P. Riess and J. Shawe-Taylor, 'The RSA Public Key Cryptosystem' (1989). [Online]. Available: https://api.semanticscholar.org/CorpusID:60326110

[16] A. P. U. Siahaan, 'Factorization Hack of RSA Secret Numbers', *Int. J. Eng. Trends Technol.* (2016), doi: 10.14445/22315381/IJETT-V37P204.

[17] J. M. Smiljanic and P. Ivanis, 'Attacks on the RSA cryptosystem using integer factorization' (2011). doi: 10.1109/FOR.2011.6143608.

[18] D. A. Buell, 'How to Factor a Number' (2021). doi: 10.1007/978-3-030-73492-3_11.

[19] A. S. Shatnawi, M. M. Almazari, Z. AlShara, E. Taqieddin, and D. Mustafa, 'RSA cryptanalysis—Fermat factorization exact bound and the role of integer sequences in factorization problem', *J. Inf. Secur. Appl.*, vol. 78, p. 103614 (2023).

[20] P. Shiu, 'Fermat's method of factorisation', Math. Gaz., vol. 99, no. 544, pp. 97–103 (2015).

[21] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, 'The return of coppersmith's attack: Practical factorization of widely used RSA moduli', in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1631–1648 (2017).

[22] P. Singh et al., 'Understanding RSA Algorithm in Cryptography' (2024).

[23] K. Somsuk and S. Kasemvilas, 'Possible prime modified fermat factorization: New improved integer factorization to decrease computation time for breaking rsa', in Recent Advances in Information and Communication Technology: Proceedings of the 10th International

Conference on Computing and Information Technology (IC2IT2014), Springer, pp. 325–334 (2014).

[24] D. Boneh and M. K. Franklin, 'Efficient generation of shared RSA keys', J ACM, vol. 48, pp. 702–722 (2001).

[25] P. Sarkar and S. Singh, 'New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields', in Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35, Springer, pp. 429–458 (2016).

[26] Y. Dasari and V. Dondeti, 'RSA security in cloud computing: A distributed model for integrated GNFS with Black Wiedemann algorithm for integer factorization', 4TH Int. Sci. Conf. ALKAFEEL Univ. ISCKU 2022 (2023), [Online]. Available: https://api.semanticscholar.org/CorpusID:266519173

[27] H. Arukala, 'Factorization in Cybersecurity: a Dual Role of Defense and Vulnerability in the Age of Quantum Computing' (2024).

[28] S. Joshi, A. K. Bairwa, A. P. Pljonkin, P. Garg, and K. Agrawal, 'From Pre-Quantum to Post-Quantum RSA', Proc. 6th Int. Conf. Netw. Intell. Syst. Secur. (2023), [Online]. Available: https://api.semanticscholar.org/CorpusID:265158671

[29] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, 'Post-quantum RSA', in Post-Quantum Cryptography (2017). [Online]. Available: https://api.semanticscholar.org/CorpusID:31025145

[30] A. Ekert and R. Jozsa, 'Quantum computation and Shor's factoring algorithm', Rev. Mod. Phys., vol. 68, no. 3, p. 733 (1996).

[31] J. Laflamme, 'Implementing the Castryck-Decru attack on SIDH with general primes', Master's Thesis, University of Waterloo (2024).

[32] V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, 'Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography', *Comput. Commun.*, vol. 176, pp. 99–118 (2021).

[33] N. Sood, 'Cryptography in Post Quantum Computing Era', *SSRN Electron. J.* (2024), [Online]. Available: https://api.semanticscholar.org/CorpusID:267673425

[34] R. Primas, P. Pessl, and S. Mangard, 'Single-trace side-channel attacks on masked lattice-based encryption', in Cryptographic Hardware

and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, Springer, pp. 513–533 (2017).

[35] X. Lou, T. Zhang, J. Jiang, and Y. Zhang, 'A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography', *ACM Comput. Surv. CSUR,* vol. 54, no. 6, pp. 1–37 (2021).

[36] P. C. Kocher, 'Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems', in Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16, Springer, pp. 104–113 (1996).

[37] B. Hettwer, S. Gehrer, and T. Güneysu, 'Applications of machine learning techniques in side-channel attacks: a survey', *J. Cryptogr. Eng.,* vol. 10, no. 2, pp. 135–162 (2020).

[38] P. C. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, 'Introduction to differential power analysis', *J. Cryptogr. Eng.,* vol. 1, pp. 5–27 (2011).

[39] J. Kaur and S. Das, 'A survey on cache timing channel attacks for multicore processors', *J. Hardw. Syst. Secur.,* vol. 5, no. 2, pp. 169–189 (2021).

[40] A. Bauer, E. Jaulmes, V. Lomné, E. Prouff, and T. Roche, 'Side-channel attack against RSA key generation algorithms', in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 223–241 (2014).

[41] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, 'Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures', *Proc. IEEE*, vol. 100, pp. 3056–3076 (2012).

[42] Á. Kiss, J. Krämer, P. Rauzy, and J.-P. Seifert, 'Algorithmic countermeasures against fault attacks and power analysis for RSA-CRT', in Constructive Side-Channel Analysis and Secure Design: 7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers 7, Springer, pp. 111–129 (2016).

[43] M. Mumtaz and L. Ping, 'Forty years of attacks on the RSA cryptosystem: A brief survey', *J. Discrete Math. Sci. Cryptogr.,* vol. 22, no. 1, pp. 9–29 (2019).

[44] Y. Lu, L. Peng, and N. Kunihiro, 'Recent Progress on Coppersmith's Lattice-Based Method: A Survey', in CREST Crypto-Math Project

(2017). [Online]. Available: https://api.semanticscholar.org/CorpusID:67692742

[45] M. R. Albrecht, M. Haller, L. Mareková, and K. G. Paterson, 'Caveat implementor! Key recovery attacks on MEGA', in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 190–218 (2023).

[46] E. O. Sodiya, U. J. Umoga, O. O. Amoo, and A. Atadoga, 'Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets', *Glob. J. Eng. Technol. Adv.* (2024), [Online]. Available: https://api.semanticscholar.org/CorpusID:268012290

[47] P. S. R. Henrique and R. Prasad, 6G: the road to the future wireless technologies 2030. River Publishers (2022).

[48] C. Beaver, 'Adventures in cryptology: Exploration-worthy project topics', *PRIMUS*, vol. 34, no. 1, pp. 13–31 (2024).

[49] J. Howe, T. Prest, and D. Apon, 'SoK: How (not) to design and implement post-quantum cryptography', in Cryptographers' Track at the RSA Conference, Springer, pp. 444–477 (2021).

[50] R. Omollo and A. Okoth, 'Factorization Algorithm for Semi-primes and the Cryptanalysis of Rivest-Shamir-Adleman (RSA) Cryptography', *Asian J. Res. Comput. Sci.* (2024), doi: 10.9734/ajrcos/2024/v17i6458.

[51] Y. Min, Z. Wang, and Q. Meng, 'Preselected integer factorization-based RSA (Rivest, Shamir and Adleman) password cracking system and method' (2014).

[52] A. Samojluk, 'About special properties of triangular numbers for immediate factorization', *Tech. Sci.* (2022), doi: 10.31648/ts.7278.

[53] V. Hoggatt Jr and M. Bicknell, 'Triangular numbers', *Fibonacci Q,* vol. 12, pp. 221–230 (1974).

Received December, 2024