Mesopotamian journal of Cybersecurity
Vol.5,No.2, **pp**. 538–562
DOI: https://doi.org/10.58496/MJCS/2025/033; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

Intelligent Threat Hunting: A Systematic Literature Review and Meta-Analysis of the RSA Cryptosystem

Daniel Asiedu [1,*], Patrick Kwabena Mensah [1], Peter Appiahene [2], Isaac Kofi Nti [1]

[1] *Department of Computer Science and Informatics, University of Energy and Natural Resources, Sunyani, Ghana.*
[2] *Department of Information Technology and Decision Sciences, University of Energy and Natural Resources, Sunyani, Ghana.*

ARTICLE INFO

Article history
Received 26 Jul 2024
Revised 10 May 2025
Accepted 31 May 2025
Published 25 Jun 2025

Keywords
Cryptanalysis
Threat Hunting
RSA
Deep Learning
Systematic Review

ABSTRACT

The RSA cryptosystem has received considerable acceptance because of its ability to withstand numerous attacks across diverse applications, and protecting digital information is essential. Historical and contemporary approaches to analyzing its algebraic security structure are essentially rooted in mathematical frameworks. Cryptanalysis with deep learning (DL) has become viable because of advancements in computing resources. However, this niche lacks systematic reviews and meta-analyses on DL-based cryptanalysis. This study marks the initial instance of a systematic review applying DL models to assess the structural challenges inherent in the RSA cryptosystem. The study presents a comprehensive analysis of 65 research papers covering five key RSA problem areas: factorization attack, weak private exponent attack, partial key exposure attack, key equation attack, and encryption scheme attack. The literature was assessed through quantitative and qualitative approaches via the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework for reporting. Through the examination carried out in this study, we develop a detailed research roadmap of previous studies on classical techniques applied to cryptanalysis operations with a specific focus on the RSA algebraic structure, along with the recognition of current challenges and recommended strategies for the utilization of DL methods in cryptanalysis tasks.

1. INTRODUCTION

Cryptography and cryptanalysis are the two main fields in cryptology. Cryptography is the study and practice of constructing secure communication protocols. In contrast to cryptography, cryptanalysis deconstructs the security of these particular frameworks. The two facets of cryptology have been locked in a timeless conflict throughout history. For decades, people and organizations have been trying to communicate securely in secret. To do this, they have elaborated on multiple increasingly intricate cryptosystems to protect their communications throughout several stages. Nevertheless, with every step forward in cryptography, new cryptanalytical methods and strategies have emerged to break these systems. The opportunities and challenges for the field will only ebb and flow as technology continues. This affair between cryptography and cryptanalysis has created some of the most fascinating stories in crypto history [1], [2], [3].

Such a cryptographic algorithm, often called a cipher, is just a mathematical function for encrypting and decrypting messages. Symmetric keys and public keys are two essential classes of such techniques. Symmetric key ciphers use a single private secret for encryption and decryption. However, the weakness of this cryptosystem is that it needs a secure prior key exchange between the sender and receiver before any message is sent. This barrier has driven the development of public key ciphers, which rely on a separate key set for encryption rather than for decryption [4]. Notably, public key cyphers have advanced cryptology considerably, providing a practical resolution to guarantee communications while handling the sharing-secret-key issue. These continually developing algorithms are revised to handle likely attacks better and safeguard data transmitted via untrusted channels [5]. The complex and mathematically robust algorithms used in public key ciphers make cryptanalysis an extremely challenging task in public key cryptography. Researchers have proposed diverse methods to analyze public-key systems via statistical and classification methods that can detect flaws in cryptographic schemes [6].

The RSA is the first practical public-key system widely used for secure data transmission. Many digital platforms have since incorporated RSA to maintain data privacy, establish integrity between parties exchanging messages, confirm whether user

*Corresponding author. Email: daniel.asiedu.stu@uenr.edu.gh

identities can be trusted, and prevent users from disavowing. RSA remains the first choice for implementing public-key cryptography in all practical deployments because of its peerless compatibility, security, and ease of integration. Its widespread use in TLS/SSL certificates, legacy systems, and hardware security modules (HSMs) provides end-to-end compatibility across industries from the web to financial services. The flexibility of RSA to support encryption, digital signatures, and key encapsulation makes it a one-stop solution for diverse cryptographic needs. Unlike elliptic curve cryptography (ECC), where careful selection of curve parameters is needed, RSA offers simple key management, reducing implementation risk. While ECC receives attention in resource-constrained devices, RSA's speedier signature verification and regulatory compliance make it essential for high-traffic servers and payment platforms. RSA also benefits from decades of optimization with speedy implementations in libraries such as OpenSSL and even hardware acceleration in modern processors [7], [8], [9], [10], [11].

The RSA is one of the most widely studied public key cryptosystems but has also previously been inspected for its vulnerabilities and features, which different authors provide. Nearly all known attempts to break the RSA cryptosystem have involved chipping away at this problem of reliance on factorization, which is core to RSA security. This process consists of factoring the RSA modulus (N), where N is a product of two prime numbers (p and q), performing timing attacks that exploit implementation weaknesses or executing chosen ciphertext attacks that leverage the protocol or padding flaws with RSA. The adversaries have made some assumptions to simplify these attack strategies. Although factorization algorithms exist, no nonquantum-based method is recognized for efficiently factoring an RSA modulus exceeding 1024 bits. Since then, state-of-the-art integer factoring has been developed by Boudot *et al*. in 2020. This was the largest integer ever factored at 829 bits, also called RSA-250 [12]. Most importantly, emerging quantum computing may significantly threaten RSA because its security relies entirely upon factorization, which is as complex as present technology yet far weak under potentially stronger technology. However, quantum algorithms have failed to solve particular classes of complicated mathematical problems related to noncommutative algebraic structures [13], [14].

While significant progress has been achieved in various domains by AI algorithms rooted in deep neural networks, its utilization in public key cryptography, specifically in RSA schemes for intelligent threat detection, is limited [15], [16]. The advancements in computing power have made DL methods viable and actively evolving, making them an immediately applicable tool for RSA-based cryptanalysis [17], [18], [19], [20], [21]. DL has been successfully applied in other areas of cryptography, and we seek to examine its relevance and effectiveness in this niche, which has received less attention. Numerous cryptographic challenges can be naturally construed as learning challenges, leading to cryptographic hardness assumptions that can produce inherently challenging distributions. Nevertheless, few studies have focused on cryptanalysis via DL, especially those that assess RSA algebraic structures. The existing successful attacks in this RSA area heavily rely on specialized mathematical and computational methods tailored to exploit RSA's structure rather than adopting a generalized pattern recognition strategy offered by DL. Modern research is currently focusing on how DL models can prove helpful in cryptanalysis, which, in future developments, may introduce new analytical viewpoints into public key cryptography. However, little has been done on the cryptanalysis of RSA systems with DL methods. Thus, it is essential to investigate RSA's underlying structures in such a DL setting.

The RSA has demonstrated strong resistance against traditional factorization and mathematical attacks, but DL now provides a new way to look for possible weaknesses. DL models are excellent at spotting nonlinear patterns and relationships in large datasets, which classical algorithms struggle with. This makes DL particularly attractive for cryptanalysis scenarios where the structure of the key material, usage patterns, or mathematical properties (e.g., shared primes or biased key generation) may expose hidden vulnerabilities. With DL, researchers can automate the search through large key spaces and spot issues that might present cryptographic problems, opening new ways of identifying threats beyond traditional methods. As cybersecurity threats become increasingly sophisticated and data-rich environments emerge (e.g., side-channel data, ciphertext patterns, or faulty signatures), DL-based cryptanalysis provides a promising frontier for advancing offensive and defensive cryptographic research. It also paves the way for combining DL with traditional mathematical methods to find new weaknesses hidden under classical assumptions [22], [23], [24].

As a contribution of this study to RSA cryptanalysis, past and present techniques employed to aid threat-hunting attacks will be thoroughly examined, classifying the relevant prior studies to develop a stance on certain prevalent RSA domains and research directions. The study will also contribute to identifying optimal techniques and potential research paths for adopting DL frameworks in RSA algebraic structure-based cryptanalysis contexts. We reviewed the relevant literature, especially the classical attack vectors, their limitations in assessing the vulnerabilities of RSA algebraic structures, and the need for intelligent attack algorithms inspired by DL to claim complete insecurity of the RSA cryptosystems. Understanding these specific fields will enable researchers to skillfully utilize DL models in cryptanalysis tasks.

The main aim of this SLR is to analyze the problem domains of the RSA cryptosystem, discuss different attack vectors, and assess the viability of using DL as an efficient tool to improve the current attack vectors. Our SLR findings enable us to construct a thorough research guide detailing prior studies on classical methodologies used in cryptanalysis operations,

specifically RSA algebraic structures and their variants, and identify existing issues and recommendations for integrating DL methods.

Our study is structured around four primary research questions (RQs) that contribute to establishing the core of our research agenda.

RQ1: What problem domain(s) of RSA tasks have been cryptanalyzed via classical methods?

A taxonomy of tasks, using various methods, will be systematically presented to understand the analysis of RSA algebraic problem domains. Moreover, the potential impact of these attack domains on the use of the cryptosystem will be successfully identified.

RQ2: What DL architectures are utilized in cryptanalysis operations?

RQ2 delves into various architectures employed in RSA threat-hunting tasks. We also examine the connection between selecting a specific architecture and the nature of the extracted features.

RQ3: What are the publication trends and growth of knowledge in RSA threat-hunting approaches?

Trends can be analyzed over different periods on the basis of the number of studies conducted. This information can indicate areas within the scientific community that require further exploration.

RQ4: What are the anticipated directions for prospective research in this domain?

RQ4 aimed to propose potential future goals for scholars and professionals using DL techniques to carry out threat-hunting activities within the context of public key cryptography. This research provided novice researchers with insights into the prevailing focus areas within this field.

With DL, RSA cryptosystems focused on deepening the operations of cryptanalysis and automation reflect a vital intersection of the current research in cryptanalysis and relevant DL. Therefore, researchers need an integrative view of the accomplishments, challenges, and opportunities to progress toward the significant research avenues where the fields overlap. To chart and direct research at the junction of DL and RSA algebraic-based cryptanalysis, a systematic literature review (SLR) was executed to pinpoint and methodically map the relationships between these domains.

2. RELATED RESEARCH

We aim to conduct an SLR to comprehend and summarize research on DL-based and classical methods or approaches for RSA threat-hunting tasks.

Preceding our work, several studies explored deep learning-based threat hunting in symmetric cryptosystems. [25] introduced the first deep learning-based key recovery attack on 11-round Speck32/64, paving the way for neural-supported cryptanalysis. The study assessed the potential of neural networks in creating statistical tests that effectively leverage differential characteristics of a weakened symmetric primitive, allowing for attacks with minimal data. The experiments demonstrated that neural networks could efficiently identify appropriate input differences within minutes on their computing system, thereby eliminating the need for prior manual cryptanalysis, a significant improvement over previous methods.

Park *et al*. introduced a unified cipher (UC) for translating ciphertext into plaintext across various ciphers via a singular DL architecture. The model is rooted in a unified, unsupervised DL approach focused on traditional substitution ciphers. By solely learning from data and lacking any prior information about some selected substitution ciphers, the proposed model exhibited an accuracy exceeding 97% [26]. Consequently, a generic cryptanalysis model based on DL was suggested, aiming to decipher the key of block ciphers on the basis of known plaintext-ciphertext pairs [27]. This paper demonstrates the applicability of DL-based cryptanalysis through lightweight block ciphers. The results illustrate the successful recovery of key bits through DL-based cryptanalysis, mainly when the key space is confined to 64 ASCII characters. Comparable attacks leveraging DL have been identified in various scholarly works [28], [29], [30], [31], [32], [33], [34].

To our knowledge, no prior work has focused on studying DL applications regarding RSA algebraic structures with a comprehensive analysis to investigate the impacts of potential DL attack vectors. In this context, the most related works are [35] and [36]. Imam *et al*. [35] systematically reviewed the benefits and limitations of RSA schemes in the literature. This includes reviewing the selection of adaptation methods and applications to RSA in different application fields and handpicking literature on particular constraints for each technique. Their work did not consider pairing the RSA cryptosystem with DL models for threat-hunting operations, which could lead to secure and efficient cryptographic solutions.

Similarly, [36] aims to provide an extensive overview of the RSA cryptosystem, specifying its importance in providing confidential information and addressing threats such as timing attacks. This study is limited in that it considers only timing attack vulnerability. This is six years after the present study.

Our research diverges, as we undertake a significant methodical analysis. Our SLR goes a step further by delving into additional factors outlining problem domains where threat-hunting tasks are focused and DL-based approaches, all of which were overlooked in prior studies. Along with an in-depth discussion, we again delineate numerous significant relationships that could assist future scholars in advancing novel DL solutions. Finally, we propose actionable steps for future scholars to investigate and further enhance various aspects of DL methodologies in the context of threat hunting.

3. METHODOLOGY

A rigorous evaluation procedure was designed to conduct a thorough and documented review. Under these circumstances, evaluation methods become central to the review process to weaken authors' influence, which can lead to potential biases. The PRISMA flow diagram, which is an essential tool because it follows the system Preferred Reporting Items for Systematic Reviews and Meta-Analyses [24], was used in this research work to guide our SLR structure by restricting exploration solely to relevant primary studies related to formulated questions. As a result, we followed the procedural steps identified in Table 1 for this review.

TABLE I. PRISMA Framework Steps

Steps	Actions
1. Identification	- Select the papers according to the search strategies and the pertinent databases - Keywords, Search String, Databases, and Record Extracted
2. Screening	- Inclusion and Exclusion Criteria to exclude the irrelevant papers
3. Eligibility	- Perform Quality Assessment
4. Included	- Ultimate Number of papers Included

First, we searched for primary studies to help answer our synthesized research questions. We started by determining the timeframe. We chose a decade, from January 1st, 2014, to April 30th, 2024, which coincides with the start of our investigation. We then identified the outlets in our scope; we chose peer-reviewed and impactful journals. Using the PRISMA framework procedures (see Table 1), we crafted a search query to search for abstracts, titles, and keywords in the "Scopus" online database. We chose the Scopus database for this study because of its wide indexing of multidisciplinary, peer-reviewed literature, including content from IEEE, ACM, Elsevier, Springer, and other major publishers. Its advanced search and filtering tools also support reproducible systematic reviews. Although IEEE Xplore and the ACM Digital Library are recognized as leading sources in computing, their contents are indexed in Scopus, allowing us to capture relevant studies while maintaining a unified search strategy. This search string includes precise keywords such as "cryptanalysis", "threat hunting", "RSA", "Rivest Shamir Adleman", "public key cryptography", "deep learning", and "DL", which are related to our research questions. Many articles appeared from the search query, but we excluded some during title and abstract screening. To enhance the comprehensiveness of our search string in retrieving pertinent primary studies, we conducted empirical assessments on various search strings incorporating different derived terms. The efficacy of each string in retrieving relevant studies was evaluated to ascertain the most effective search approach. After executing the designated search string (Table 2) on the "Scopus" platform, 163 articles closely matching the search criteria were identified. Vital specifics such as titles, keywords, abstracts, DOIs, and other pertinent data from these articles were compiled into a comma-separated values file extracted from the Scopus repository. The sources were subsequently stored in Mendeley, a reference software used to facilitate the streamlining of our reference organization process toward achieving our research objectives.

TABLE II. THE SEARCH QUERY

TITLE-ABS-KEY ((cryptanaly* OR “threat hunting” OR “weakness*” OR “vulnerabilit*” AND (“RSA” OR “Rivest Shamir Adleman”) OR (“deep learning” OR “DL” OR “neural networks”)) AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND (LIMIT-TO (SRCTYPE, “j”)) AND (LIMIT-TO (DOCTYPE, “ar”)) AND (LIMIT-TO (LANGUAGE, “English”))

Additional publications were identified via Google and Google Scholar on the basis of our research's subject matter and objectives. A considerable number of duplicate articles were discovered across the online repositories. The duplication issue was effectively addressed via Mendeley's automated duplicate removal process. After removing duplicates, 153 records remained, all of which were screened against the inclusion and exclusion criteria. The papers were distributed among three authors to categorize them on the basis of a detailed reading of the abstract and title. One author then checked all the categorizations to resolve any discrepancies. In cases where discrepancies arose between one of the three authors and the additional author, the entire team collectively examined and deliberated the specific paper until a unanimous consensus was reached.

Ultimately, 76 reports were evaluated for eligibility (Figure 1). The criteria for exclusion and inclusion were applied to determine the relevance of each paper to our research topic. Our study excludes any report that satisfies the criteria outlined in Table 4 while including studies that satisfy the criteria in Table 3.

TABLE III. EXCLUSION CRITERIA

Exclusion
a. Articles from conferences, short communications, and workshop proceedings
b. Papers published beyond the timeframe considered in this study
c. The papers were in languages other than English

d. There were no full texts available
e. Papers that were outside the scope of RSA cryptosystem
f. Papers that did not solve some sort of RSA cryptanalysis task

TABLE IV. INCLUSION CRITERIA

Inclusion
a. The publications are in English
b. The abstracts feature original findings on the research areas
c. Papers relevant to our scope cryptanalyzed the RSA algebraic structure using classical method or DL-based approach

After the full-text screening, the reviewers excluded 17 reports in line with the criteria in Table 3. Upon the conclusion of the comprehensive systematic review, 65 papers were identified (Figure 3), comprising 59 studies that were part of the review, along with six reports from Google Scholar and Google (Figure 3). A secondary reviewer subsequently verified the included papers to ensure the accuracy of the extracted data. Each author was designated as a secondary assessor to validate the accuracy of the primary studies (65 articles) extracted by the other reviewers and to ascertain their relevance to the RQs.

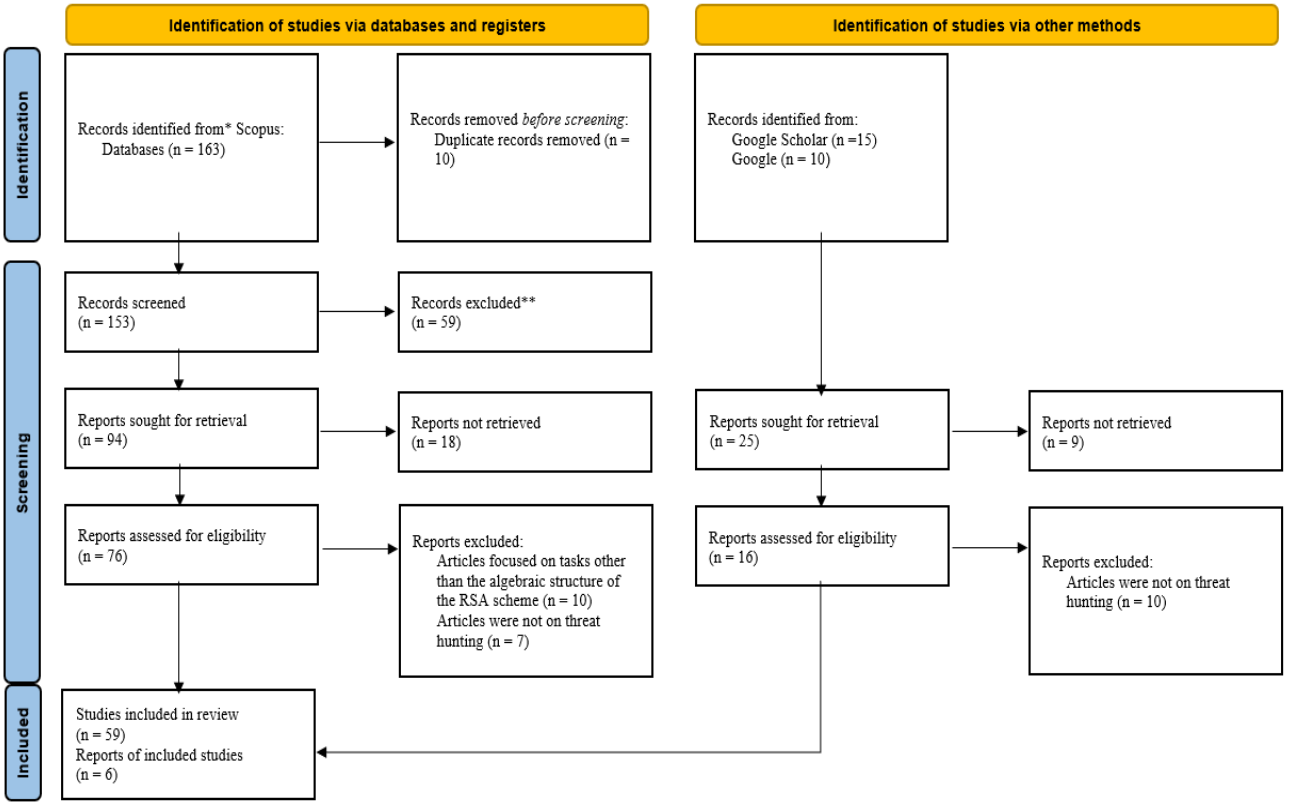

Fig. 1. The PRISMA schematic of the primary articles

4. RESULTS AND DISCUSSION

In the subsequent sections of this SLR, we examine the data comprehensively and deliberate on the outcomes relevant to our RQs derived from the study's findings.
RQ1: What problem domain(s) of RSA tasks have been cryptanalyzed via classical methods?

4.1 RSA Algorithm

The security of RSA relies on the fact that it is difficult to factor the sizeable composite number (n) into its prime factors (p and q). Encryption uses the public key (e, n). Nevertheless, decryption uses only the private key (d, n) as long as n is large enough to be impossible to factor via classical algorithms. If an attacker can factor n, they can obtain the private key d and break the whole system.

TABLE V. RSA ALGORITHM

Key Creation:
1. Select two distinct large prime numbers as p and q
2. Compute n = p × q: n is the product of p and q
3. Compute $\phi(n)$: $\phi(n)$ =$(\mathbf{p-1}) \times (\mathbf{q-1})$
4. Choose Shared Exponent e: 1 < e < $\phi(n)$ and gcd(e, $\phi(n)$) = 1
5. Compute the Secret Exponent d: $d \times e \equiv 1$ (mod ϕ(n))
Public Key: (e, n)
Private Key: (d, n)
Encryption Function:
the sender uses the recipient's public key (e, n)
$C \equiv m^e \pmod n$
Decryption Function:
the recipient uses their private key (d, n)
$M \equiv c^d \pmod n$

The following sections analyze and discuss the categories of problem areas and the various methods proposed by researchers to assess the security of the RSA scheme (see Table 5).

4.2 Problem Domain Classification

Numerous RSA cryptanalysis techniques have been proposed in scholarly works; however, none have yet claimed a complete compromise of the large number. RSAs are subject to various attacks, such as mathematical attacks, factorization attacks, attacks exploiting vulnerabilities in public/private key pairs, and attacks arising from improper system implementations. Building upon existing research, the literature has been categorized into distinct domains. In this context, "Domain" refers to the areas within which the RSA cryptosystem has been primarily examined for threat-hunting activities since its inception. In the study of 65 papers conducted in this SLR, five distinct domains were discovered to have been subjected to threat-hunting tasks. The volume of primary studies chosen to define various domains of RSA threat hunting include classifications such as "Factorization", "Weak/Small Public and Private Exponents", "Partial Key Exposure", "Key Equation", and "Encryption Scheme", as indicated in Table 6. Figure 2 visually summarizes our domains within these 65 primary studies across 10 years. On the basis of the domain distributions shown in Figure 3, it is apparent that "Factorization" is the most popular for threat hunting in the context of the RSA cryptosystem. It constitutes 40 primary papers, followed by the "weak/small private exponent" domain (16). The least explored domains include the "Partial Key Exposure" (5 papers), the Key Equation (2 papers) and the Encryption Scheme (2 papers).

TABLE VI. YEARLY DISTRIBUTION OF PRIMARY STUDIES IN THE STUDY PROBLEM DOMAINS

Domains	Papers	Year		Domains	Papers	Year
Factorization	[37]	2014		**Weak Private Keys**	[38]	2015
	[39]	2014			[40]	2015
	[41]	2014			[42]	2018
	[43]	2015			[44]	2019
	[45]	2015			[46]	2019
	[47]	2016			[48]	2019
	[49]	2016			[50]	2019
	[51]	2016			[52]	2019
	[53]	2016			[54]	2019
	[55]	2016			[56]	2019
	[57]	2017			[58]	2019
	[57]	2017			[59]	2020
	[60]	2017			[61]	2021
	[62]	2018			[63]	2023
	[64]	2018			[65]	2023
	[66]	2018			[67]	2024
	[68]	2019				
	[69]	2019		**Partial Key Exposure**	[70]	2019
	[71]	2019			[72]	2020
	[73]	2020			[74]	2020
	[75]	2020			[76]	2021
	[77]	2020			[78]	2023
	[79]	2020				
	[80]	2020		**Key Equation**	[81]	2020

	[82]	2020			[83]	2023
	[84]	2020				
	[85]	2020		**Encryption Scheme**	[86]	2018
	[87]	2020			[88]	2021
	[89]	2021				
	[90]	2021				
	[91]	2021				
	[92]	2021				
	[93]	2022				
	[94]	2022				
	[95]	2022				
	[96]	2022				
	[97]	2022				
	[98]	2022				
	[99]	2022				
	[100]	2024				

As Table 6 shows, many factorization attack papers appeared between 2016, 2020 and 2022, reflecting a veritable explosion of contributions that examine various approaches to the RSA factorization problem. This space is the locus of the central attack in one of the primary attacks on RSA. The RSA algorithm depends on the computational hardness of the prime factorization problem. The chronologies of papers in other areas provide some clues as to patterns of cryptanalytic concentration. For example, although the maturity of factorization attacks was apparent earlier (2014-2017), other attack strategies, such as weak private keys and partial key exposure, gained research interest (2019-2023). This transition is a natural part of the dynamic history of cryptanalysis, in which traditional attacks have become fully mastered and new vulnerabilities have appeared, possibly owing to the advent of new computational techniques.

This finding demonstrates how exponentially harder RSA cryptanalysis is becoming in systems of any size where automated attack methods are necessary. The recent deluge of papers on fundamental key equations and encryption algorithms (published almost exclusively between 2020 and 2023) indicates an anticipatory change in research priorities to the search for deeper algebraic and structural vulnerabilities in RSA. Indeed, the breadth of fields covered by the article is evidence of multifaceted RSA vulnerability. The problems with RSA security highlight the need for complete crypto audits. However, as new methods, including DL, are applied to the cryptanalysis of RSA, it is essential to examine such methods globally for all attack classes to guarantee complete security.

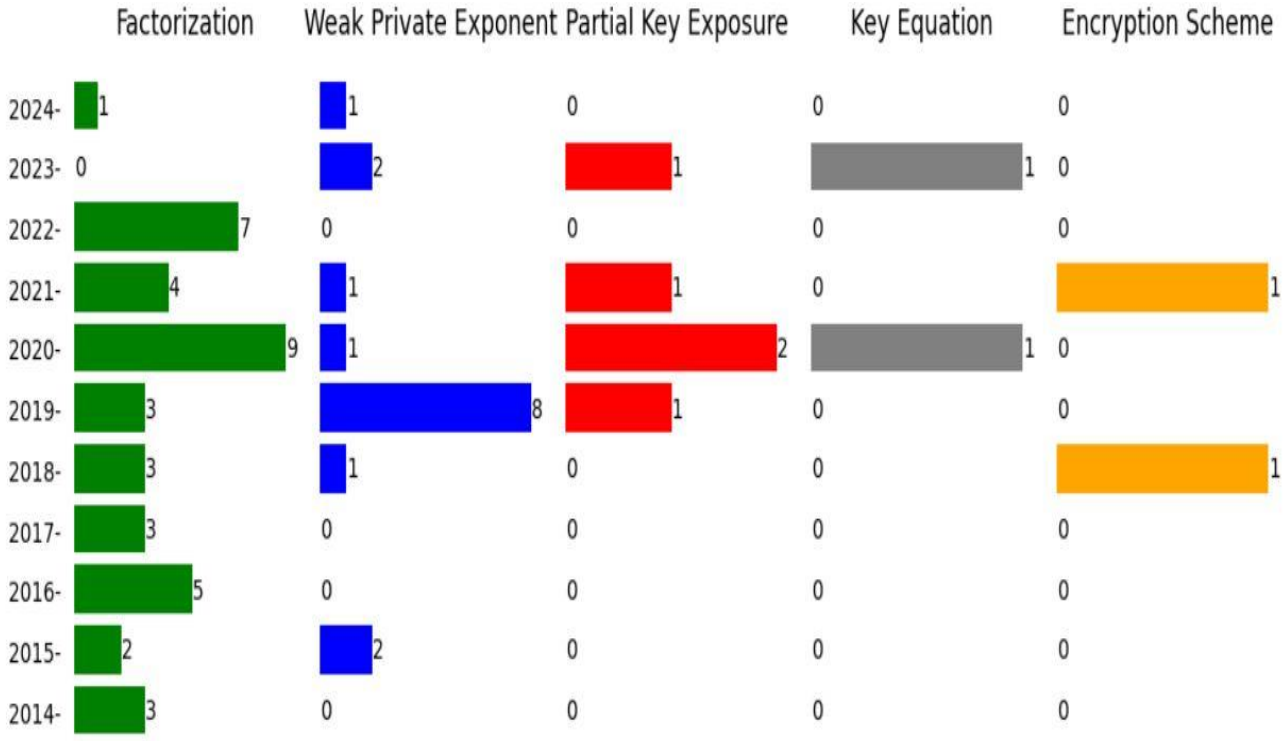

Fig. 2. Distribution of all primary studies by domain and year

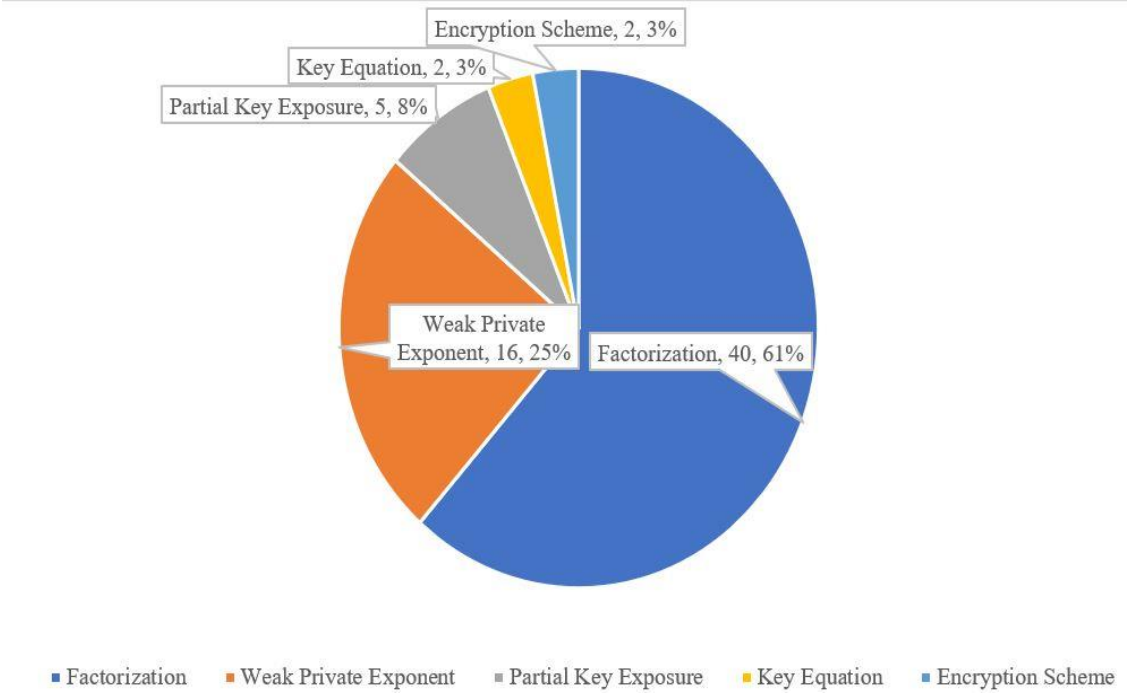

Fig. 3. Distribution of the domains in all the primary studies

4.3 Methods Used

This section comprehensively evaluates the literature on the algorithms employed in threat hunting within RSA problem domains and several variants. The discussion then goes into each of the named domains, summarizing the goals of the proposals and the conclusions that follow from the separate analysis of relevant papers, all related to the RQs. The first, starting with the domain in which there are many algorithms, is factorization, and then, there is a progression to the last domain, the encryption scheme. In addition, a table with an algorithmic analysis has been added at the end of the section to help clarify the methods used by each author.

- **Factorization task**

The integer factorization problem (IFP) is a number-theoretic problem that is difficult to solve. Within the RSA cryptosystem, N typically results from multiplying two prime numbers of equal size, which are carefully selected to prevent easy guessing or factorization via modern computational capabilities. Knowing the factorization of N, it becomes easier to calculate d (a private exponent) and then, in turn, $\varphi(N)$ as well. The basis of the RSA cryptosystem rests on the intrinsic difficulty of the IFP, which means that these mathematical puzzles are challenging to solve in polynomial time. Attempts to breach the robust modulus N through factorization pose significant computational hurdles, as breaking it down into prime factors p and q remains a task believed to be beyond feasibility for larger values of N.
This study identified 23 unique IFP algorithms. The coppersmith's lattice-based algorithm is the most commonly used algorithm and is asymptotically faster than the existing algorithms are, followed by continued fractions, the genetic algorithm, and lattice basis reduction. Table 7 provides a comprehensive analysis of the IFP algorithms. Figure 4 shows a bar chart of the IFP algorithms and the reported frequency of their use on factorization problems in the primary studies.

- **Weak/Small private keys tasks**

RSA security relies on a trapdoor function; it is difficult to factor the secret key d from the public key $\{e, N\}$, where the symbol d represents trapdoor information. The small secret exponent d is unique because RSA signatures can be computed much faster. However, if the factorization of N is practical, Euler's Totient Function of N can be calculated, $\varphi(N)$, which in turn allows the secret key d to be determined. The choice of a small value of the decryption exponent could render the whole system insecure. To perform cryptanalysis on RSA based on the weak private exponent, the lattice reduction technique, which is based on Coppersmith's method, is the most popular algorithm, followed by the continued fractions method in this study. Refer to Table 8 and Figure 5 for the detailed analysis and visual breakdown, respectively.

- **Partial key exposure tasks**

An adversary can reconstruct the complete private key d within a linear period $(elog(e))$, given that e represents the public key exponent if the adversary possesses knowledge of the $(k/4)$ least significant bit of the private key d. In scenarios where e is small, the exposure of merely a quarter of $d's$ bits lead to the retrieval of the entire private key. Furthermore, leaking a specific number of least significant bits (LSBs) in the case of shared primes, combined with a proportionally similar number of most significant bits (MSBs) in the private exponents, can also recover the complete private key. The study identified five algorithms, such as the Coppersmith lattice-based algorithm, the Dickman theorem, the extended Takayasu-Kunihiro algorithm, the extended Jochemsz-May algorithm and the Boneh-Durfee attack, which are applicable under the stated conditions. Refer to Table 9 for a detailed analysis.

- **Key equation tasks**

The sizes of the private and public key exponents cannot exceed the modulus N because the keys are generated within the range of 1- $\varphi(N)$. In two significant studies (refer to Table 10), the key equation was examined, and various attacks were suggested on the basis of Coppersmith's interval and multiple key generation techniques, ultimately exposing vulnerabilities within the RSA cryptosystem.

- **Encryption scheme tasks**

The conventional RSA system features a public common modulus, enabling the communicating parties to use the public exponent to achieve the inverse result known as the private key exponent. The double encryption attack method can exploit this susceptibility to a man-in-the-middle (MITM) attack. Our research identified two primary studies that focused on the general encryption scheme pattern to identify vulnerabilities via fixed-point attacks and mathematical inductions. A breakdown of these findings is presented in Table 11.

TABLE VII. ALGORITHM ANALYSIS OF THE FACTORIZATION TASK

Methods	Feature	Papers	Year		Methods	Feature	Papers	Year
Coppersmith's Lattice-Based	RSA	[37]	2014		Coppersmith's Lattice-Based	RSA	[75]	2020
Coppersmith's Lattice-Based	Multi Prime RSA	[39]	2014		Continued Fractions	Variant: $N=p^2q$	[77]	2020
Quadratic Sieve Algorithm	RSA	[41]	2014		Genetic Algorithm	RSA	[79]	2020
Coppersmith's Lattice-Based	Prime Power RSA	[43]	2015		Fermat's attack	Cubic Pell Equation RSA	[80]	2020
Brute-force	ESRKGS RSA	[45]	2015		Number Field Sieve	RSA	[82]	2020
Generic Ring Algorithm (GRA)	RSA	[47]	2016		Random Reconstruction Algorithm (RRA)	RSA	[84]	2020
Induction	ESRKGS RSA	[49]	2016		Rabin's algorithm	RSA	[85]	2020
Bernstein's Algorithm	ISO 9796-2	[51]	2016		Euclidean Algorithm	RSA	[87]	2020
Interval and Double Walks	Semismooth RSA	[53]	2016		Fermat's Difference of Squares	RPRIME RSA	[89]	2021
Genetic Algorithm	RSA	[55]	2016		Kraitchik's Algorithms	RPRIME RSA	[89]	2021
Lattice Basis Reduction	Dual RSA	[57]	2017		Continued Fractions	RSA	[90]	2021
Coppersmith's Lattice-Based	$N = p^r q^l$	[101]	2017		Coppersmith's Lattice-Based	RSA	[91]	2021
General Number Field Sieve method (GNFSM)	RSA	[60]	2017		Jochemsz-May Strategy	Variants: $N=p^2q$	[92]	2021
Coppersmith's Lattice-Based	RSA	[62]	2018		Quadratic Root	RSA	[93]	2022
Coppersmith's Sublattice-based	RSA	[64]	2018		Quantum Annealing	RSA	[94]	2022
Boneh's Lattice Factorization	Rebalanced RSA	[66]	2018		Coppersmith's Lattice-Based	Cubic Pell Equation RSA	[95]	2022

Elliptic Curve Method (ECM)	RSA	[68]	2019		Joint Modulus	RSA	[96]	2022
Simultaneous Diophantine Approximations	$N_s = p_s q_s$ RSA	[69]	2019		Continued Fractions	Cubic Bell Equation RSA	[97]	2022
Lattice Basis Reduction	$N_s = p_s q_s$ RSA	[69]	2019		Coppersmith's Lattice-Based	CRT-RSA	[98]	2022
Continued Fractions	$N = p^2 q$	[71]	2019		Coppersmith's Lattice-Based	RSA	[99]	2022
Continued Fractions	Variant: $q < p < \lambda q$	[73]	2020		Continued Fractions	$N = p^2 q$ RSA	[100]	2024

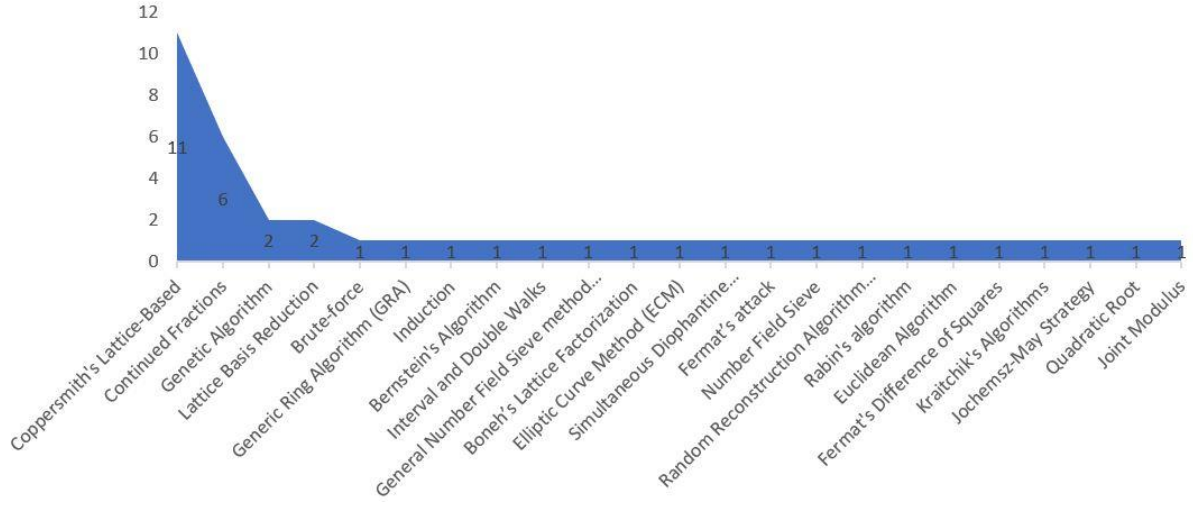

Fig. 4. IFP algorithms in all considered RSAs and their variants

TABLE VIII. ALGORITHM ANALYSIS OF THE WEAK PRIVATE KEYS TASK

Method	**Feature**	**Papers**	**Year**		**Method**	**Feature**	**Papers**	**Year**
Coppersmith's Lattice-Based	RSA	[38]	2015		Coppersmith's Lattice-Based	RSA	[56]	2019
Baby-step Giant-step	RSA	[40]	2015		Coppersmith's Lattice-Based	RSA	[58]	2019
Continued Fractions	singular cubic curves, Gaussian integers, Lucas sequences	[42]	2018		Lattice Basis Reduction	CT-RSA	[59]	2020
Coppersmith's Lattice-Based	CRT-RSA	[44]	2019		Coppersmith's Lattice-Based	Cubic Bell RSA	[61]	2021
Continued Fractions	RSA	[46]	2019		Euler Totient	RSA	[63]	2023
Coppersmith's Lattice-Based	CRT-RSA	[48]	2019		Carmichael Functions	RSA	[63]	2023
Extended Blömer-May's	RSA	[50]	2019		Binary Search	RSA	[65]	2023
Small Prime Difference	RSA	[52]	2019		Coppersmith's Lattice-Based	CP-RSA	[67]	2024
Continued Fractions	RSA	[54]	2019					

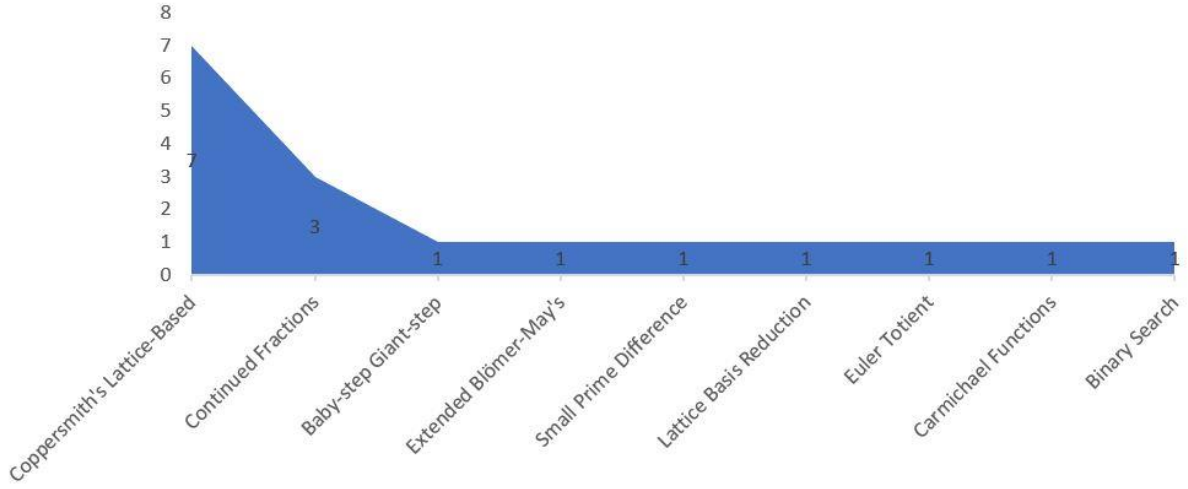

Fig. 5. Weak/small private keys algorithms in all considered RSAs and their variants

TABLE IX. ALGORITHM EVALUATION OF THE PARTIAL KEY EXPOSURE TASK

Method	Feature	Papers	Year
Coppersmith's Lattice-Based	RSA	[70]	2019
Dickman's Theorem	CRT-RSA	[72]	2020
Extended Takayasu-Kunihiro's Attacks	RSA	[74]	2020
Extended Jochemsz-May	$N=p^2q$	[76]	2021
Boneh-Durfee's Attack	RSA	[78]	2023

TABLE X. ALGORITHM EVALUATION OF THE KEY EQUATION TASK

Method	Feature	Papers	Year
Coppersmith's Interval	RSA, Multi Prime	[81]	2020
Multiple key Generation	RSA	[83]	2023

TABLE XI. ALGORITHM ANALYSIS OF THE ENCRYPTION SCHEME TASK

Method	Feature	Papers	Year
Fixed-Point Attack	RSA	[86]	2018
Induction	Jain Singh's identity-based RSA	[88]	2021

Tables 7 to 11 show the progression and modification of various techniques to capitalize on vulnerabilities in the RSA cryptosystem. These tables clarify key observation trends, including but not limited to the evolution of RSA attacks about factorization, private keys that are not strong enough, partial key leakage, the key equation, and the encryption scheme.

Across all the examined domains, Coppersmith's Lattice-Based and Continued Fraction attacks emerge as the most frequently employed strategy in the factorization attacks and the weak private keys attacks, as illustrated in Table 7 and Table 8, respectively. The versatility of these attacks is relatively high; they are not limited to conventional RSA only but include some of its variants, such as Multi Prime RSA, Prime Power RSA, and CRT-RSA. Such methods remain among the most effective mechanisms successful in factorizing the highest modulus owing to their capacity to exploit the algebraic properties of RSA and its variants. Hence, these methods have gained more attention recently than earlier methods, such as the quadratic sieve algorithm [29], the generic ring algorithm (GRA) [35], the genetic algorithm [43], the GNFSM [48], and the elliptic curve method (ECM) [56].

The specific uses of Coppersmith's method for weakening RSA involve situations where the shared exponent e is relatively small or when there is partial leakage of the private key. One of the advantages of Coppersmith's method is that it offers provable assurances to locate all roots that fall below a specific limit X within polynomial time comparable to the bit length. Coppersmith's attack exploits small RSA private exponents by modelling the problem as a lattice reduction task. Intuitively, it shortens noisy mathematical vectors to reveal hidden patterns, enabling efficient recovery of weak keys.

The most notable use case of Coppersmith's method in threat hunting is the enhancement of Wiener's well-known attack on RSA private exponents $d < N^{1/4}$ [49] and $d < N^{0.292}$ [34], [38], [42], [47].

Attacks of this type have also been devised for the RSA cryptosystem's secret exponents on the basis of the Chinese remainder theorem [32], [36]. This method is again successful on a modified RSA based upon the cubic Pell's equation [49]. This attack illustrated how to resolve the issue with bivariate modular congruence $x(y^2 + ay + b) + 1 \equiv 0 \; mod \; e$, which led to the presentation of the small private exponent attack against this RSA variant. The authors disclosed an efficient factorization of RSA for moduli of length 1024 bits when $d < N^{0.292}$. Nevertheless, the lattice technique by Coppersmith's attack with the secret exponent $d \geq N^{0.292}$ lacks efficiency and may not be applicable.

The continued fraction method can also break RSA with weak secret exponents. One such attack has polynomial time if $e < N = p.q, GCD(p-1, q-1)$ is small, p and q have roughly the same number of bits, and $d < \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$. On the other hand, when choosing a large $GCD(p-1, q-1)$ or in cases where $e > (pq)^{\frac{3}{2}}$, the continued fraction attack does not work.

Another attack based on the continued fraction method was proposed in [78]. For a parameter t, the proposed attack can break the RSA cryptosystem when $d < \sqrt{t(2\sqrt{2} + 8/3)} \;\; N^{0.75}/\sqrt{e}$, completing a time complexity of $O(tlog(N))$ with a modulus N of 1024 bits. This type of attack is beneficial when e is significantly smaller than N. However, adapting the attack in the case where $e \approx N$, which is more than Boneh-Durfee's limit, is considered an open problem.

In [79], the authors attacked a modulus of the type $N = p^2 q$. They showed that if $N - \left(\left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}\right)$, which is considered a reasonable estimate for $\varphi(N)$, is inserted into equation $ed - k\varphi(N) = 1$, then the parameters k and d can be determined among the equation $\frac{e}{N - \left(\left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}\right)}$ and continue to fraction converge, which makes it possible to find p and q in polynomial time. Nonetheless, the attack would not be feasible when the prime factors are unbalanced; such factors are generally defined as $q < p < \delta q$, where $\delta > 2$. The attack only focuses on the case when the prime factors are balanced; that is, the sizes of p and q in bits are in the proportion defined as $q < p < 2q$.

A new binary search-inspired method for finding the MSBs of p has been proposed [53]. This method successfully attacked the RSA system with a 1024-bit modulus for $d \leq N^{0.292}$ on the basis of nontrivial and inspiring multivalued-continuous occurrence. However, less effective results, $d \leq N^{0.287}$, were achieved once the new attack was used on the RSA with a 2048-bit modulus. In other words, the attack's effectiveness decreases with larger RSA moduli, such as 2048 bits, indicating a challenge in breaking through the theoretical upper bound for practical RSA attacks. Techniques such as quantum annealing [82] exemplify the increasing impact of quantum algorithms and innovative approximations that leverage weak keys. This emerging attack signifies a transition in RSA cryptanalysis toward increasingly specialized, adaptive methods beyond classical approaches.

As shown in Table 9, the leaking part of the decryption exponent could enable an adversary to factor the RSA modulus. Such an attack is called partial key exposure. A notable attack against RSA was developed by Takayasu and Kunihiro [58], where the method of coppersmith, which uses lattice-based approaches, identifies small solutions for modular equations in polynomial time, given either MSBs or LSBs of d. Following this, additional attacks [60], [62], [64], [66] have shown that RSA and its variants are susceptible to partial key exposure attacks in specific situations. The seriousness of these attack vectors highlights the importance of generating keys securely.

The interval methods [69] and multiple key generation [71] attacks, as presented in Table 10, depict how such weaknesses in the fundamental key generation equation may be adapted to form a realistic attack. Such attacks are less discussed but are gaining more traction, revealing more in-depth algebraic relationships in RSA. These techniques reflect a more subtle appreciation of the more profound mathematical properties supporting RSA and point toward attacks that target equation-based dependencies between public and private keys, such as offering alternate factorization routes or recovery methods for weak keys. Continuing research in these areas is apt to expose previously unknown vulnerabilities in the RSA cryptosystem.

The methods presented in Table 11 are targeted directly at encryption schemes; examples are fixed-point [74] and induction attacks against Jain Singh's identity-based RSA [76]. Note that most of these methods explicitly indicate that attacks against fundamental encryption schemes can be as powerful as those against key generation or factorization. The above observation provides an important lesson: not only can the keys be compromised, but the schemes for managing encryption and decryption can also be significant attack points. A necessary consequence is that encryption schemes based on RSA need to be designed with resilience considerations in mind to counter direct and indirect attacks.

For many years of investigations into reversing the RSA system, several informative attacks have emerged, yet no fatal attack has been identified. Nearly all of these issues stem from improper system usage, poor parameter selection, or implementation errors. The threats uncovered thus far highlight the dangers to evade when executing RSA. One could assert that the RSA system remains a secure option, and its application with attack techniques remains safe. This assertion is based on the observation that despite ongoing detailed analysis of the RSA algorithm, no method has been found that can entirely

compromise it. Ultimately, it revolves around identifying specific vulnerabilities that alert us of how to select parameters for RSA implementation.

RSA is on the verge of constant evolution, with a very marked trend in the adaptation of classical techniques to modern cryptographic settings and in the development of specialized algorithms suited to particular variants of RSA. The more progress cryptanalysts make, the more all these different methodologies will be required in devising secure versions of RSA that are resistant to both classical and novel forms of attack. Given all the points discussed, RSA is regarded as a secure cryptographic system with careful parameter choice and without any attack vectors inspired by DL.

RQ2: What DL architectures are utilized in cryptanalysis operations?

Surprisingly, among all 65 primary papers reviewed in this study, no DL model was used to assess the security structure of the RSA scheme or its variants across the five domains revealed, indicating a lapse in RSA DL-based cryptanalysis. We refer the reader to Tables 7, 8, 9, 10, and 11 for all the details of the methods employed thus far.

One of the main issues regarding deploying DL techniques for RSA is the complexity and mathematics behind the system. The system's difficulty in devising any algorithm to factor large prime numbers makes it challenging to perform pattern recognition or approximation, which are the strengths of DL networks. It becomes difficult to view RSA adversarial attacks as a problem to be solved, even in the case of supervised and unsupervised learning, which would produce values to be utilized by DL.

Another challenge is the unavailability of relevant data to train DL techniques for practice in this area. Most of the time, effective models of DL call for large volumes of data to be trained, which often results in millions of labelled data points. In most cases, very specialized methods are used when performing RSA cryptanalysis, and the data required to train DL systems are not available for larger key sizes. There is a scarcity of labelled datasets comprising RSA key pairs and related cryptographic artifacts, which are crucial for supervised learning models. Unlike side-channel datasets, no public repository of RSA-encrypted samples at varying key lengths exists. The RSA's large key sizes (typically 1024, 2048 or 4096 bits) pose severe computational challenges. Training deep neural networks for such large key spaces requires considerable memory, computing power, and time, which often goes beyond typical research setups.

It is common knowledge that most research on DL has been carried out within the scope of side-channel attacks, and trimming work has been performed in conventional RSA cryptanalysis using DL. This is because most of the research done in conventional RSA cryptanalysis has used mathematical techniques, ignoring algorithmic techniques that are premised on challenges such as those focusing on DL.

Despite these advantages, DL is still a viable method in this niche for many reasons: the complexity and scaling of cryptographic systems, as are the computational tasks, are on the rise, which leaves some areas that may be hard for the traditional approach. DL, which can learn from big datasets and find meaning in high-dimensional data, offers significant benefits for solving cryptographic problems, especially when the issues are in a form that is hard to solve within conventional mathematical solutions owing to the issue of size or dimension. The main strength of DL models, specifically transformers, recurrent neural networks (RNNs), and graph neural networks (GNNs), is their ability to scale. In contrast to classical cryptanalysis techniques, which frequently necessitate considerable manual fine-tuning or specific algorithmic modifications on the basis of the keys' sizes, DL models can be generalized across a diverse range of RSA key sizes. After the models are trained, they can be deployed to evaluate a dataset of RSA keys for attacking many encryptions simultaneously. This scalability is essential because RSA key usage is increasing (beyond 1024 bits), and the use of classical approaches is becoming prohibitive in computation cost and, at times, hard to implement.

DL architectures can handle large volumes of encrypted data and reveal patterns or structural flaws that classical techniques cannot. For example, RNNs are particularly adept at examining sequences of cryptographic operations, which is a critical part of modular computations in RSA. Improvements in the GANs offer good prospects for creating artificial datasets, which will be used in training DL models, hence offering capabilities to forecast and profile encryption systems. Moreover, advancements in transfer learning allow easy progress in the design of DL systems, which are aimed primarily at focusing on one cryptanalytic problem to cover other issues, making them useful for the new cryptographic systems that have been developed.

Although the use of DL in RSA cryptanalysis, especially its algebraic structure, is at the formative stages, the fast development of such DL architectures substantiates the justification for ongoing exploration and prospective future success.

RQ3: What are the publication trends and growth of knowledge in RSA threat hunting approaches?

4.4 Trends in Research Publications

Over time, the number of research papers on threat-hunting methods related to the RSA and its variants has expanded. Between 2014 and 2017, threat-hunting activities experienced increasing and decreasing trends (Figure 6), but they started to achieve traction after 2018. Over the span from 2014-2017, fifteen papers represented 23.08% of the primary papers studied. Until 2020, the field experienced an abrupt exponential increase in publications. The number of publications in the

area increased from five to twelve in 2019, with an additional growth of one in 2020. The number of publications plateaued or slightly decreased between 2021 and 2023. Two papers were recorded on the basis of the study timeline of 2024.
On the basis of the study findings, the primary papers were positioned according to the popularity of the publishing media. Elsevier BV and Institute of Electrical and Electronics Engineers Inc. had the most papers, with five each (15.38%), followed by the Multidisciplinary Digital Publishing Institute (MDPI), Multidisciplinary Digital Publishing Institute (MDPI) AG and Elsevier Ltd., with four each (18.46%), Little Lion Scientific, with 3 (4.62%), Springer, Institute of Electronics, Information and Communication, Engineers (IEICE), Malaysian Abstracting and Indexing System, Taylor and Francis Ltd., Universiti Putra Malaysia, Springer New York LLC, Akademi Sains and Malaysia and Blackwell, with two each (21.54%). These thirteen publishers published 60% (39) of the articles (see Figure 7). The remaining publishers each contributed solely one article.

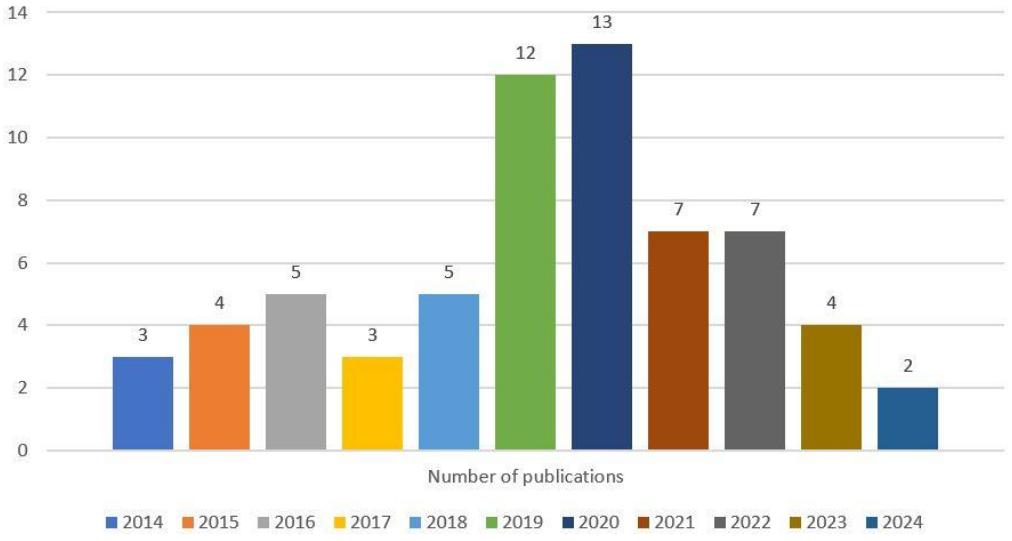

Fig. 6. Trends in research publications

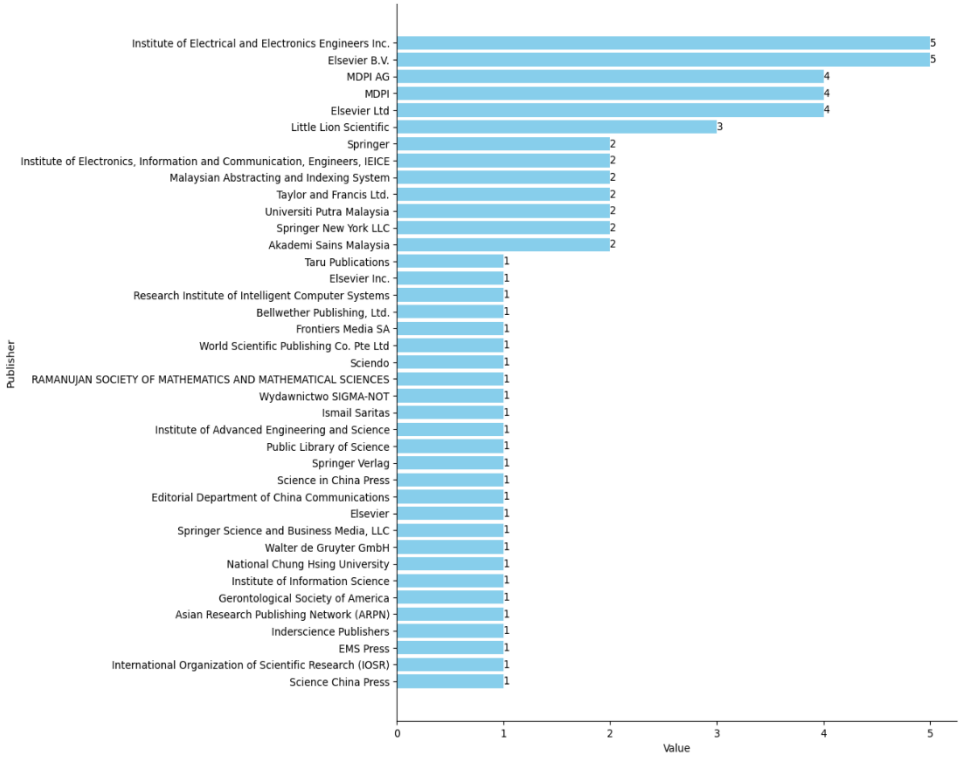

Fig. 7. Publication media on the basis of primary papers

4.5 Analysis Network Virtualization Maps

- **Bibliographic Coupling of Countries**

A bibliometric analysis was conducted on countries to ascertain the quantity of publications attributed to each country and subsequently to assess the extent of collaboration among these countries. A threshold of 2 documents and ten citations was established for each country via VOSviewer software. Among the 20 countries, only 8 surpassed this threshold. The cumulative strength of coauthorship connections with other countries was computed for these eight countries. The eight countries exhibiting the highest total link strength were identified. China stood out with the most publications, with 18 documents accompanied by 157 citations, resulting in a total link strength of 534. The following, in rank order after China in its publication index, is Malaysia, with 17 documents and 65 citations, which attained a link strength of 223; India had ten papers and an impressive 130 citations.
Moreover, Japan, France, Turkey, Australia, and Jordan reported the fourth-highest number of documents, ranging from 2-9. Most astonishingly, contributions from African countries were minimal, as they even failed to produce up to 2 papers and ten citations, which is very basic. This implies how Africa is behind this field of research (see Table 12).

TABLE XII. BIBLIOGRAPHIC COUPLING OF COUNTRIES

No	Country	Documents	Citations	Total link strength
1	China	18	157	534
2	Japan	9	79	467
3	France	8	60	223
4	Malaysia	17	65	223
5	India	10	130	146
6	Turkey	2	16	76
7	Australia	2	30	21
8	Jordan	2	17	0

Concerning the link between countries, the automated calculation of this link was carried out via VOSviewer software. China exhibited the most robust link, with a value of 534, followed by Japan with 467, whereas Australia showed the weakest link at 21. Nevertheless, all countries were interconnected, indicating satisfactory research collaboration, except for Jordan, which lacked connections with other countries. The visualization of the network also highlights two distinct clusters: cluster 1, composed of Australia, France, Malaysia, and Turkey, and cluster 2, which includes China, India, and Japan (refer to Fig. 8).

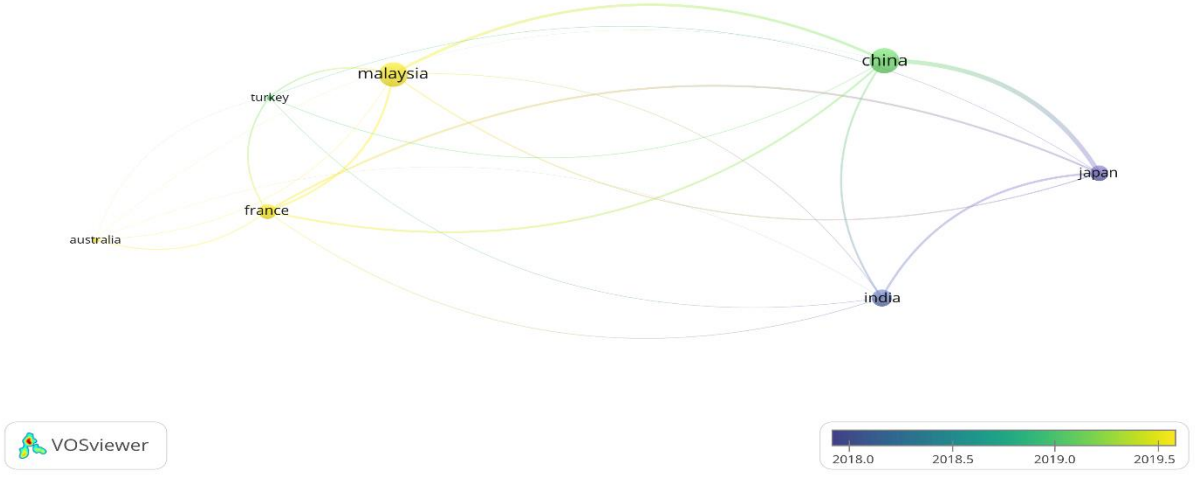

Fig. 8. Country network visualization map

- **Bibliographic coupling of sources**

According to the bibliographic analysis, 38 contributors were identified in the research area (journals). With VOSviewer software, a threshold was established with a minimum requirement of 2 documents and ten citations. Out of the 38 sources,

only 10 fulfilled this threshold. These sources undoubtedly represent the essential sources in the research carried out in this area. Notably, all ten sources prominently feature either cryptanalysis or RSA within their titles. The data presented in Table 13 reveal that the Journal of Theoretical and Applied Information Technology presented the highest document count, followed by IEEE Access, Mathematics, the Journal of Discrete Mathematical Sciences and Cryptography, and the Journal of Information Security and Applications.

On the other hand, regarding citation counts, the Journal of Information Security and Applications recorded the highest number of citations compared with all other included journals, especially the Journal of Discrete Mathematical Sciences and Cryptography, which was second. Therefore, one could posit that the Journal of Information Security and Applications; the Journal of Discrete Mathematical Sciences and Cryptography; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences; IEEE Access; and Designs, Codes, and Cryptography have had the most substantial influence within this research domain. Except for the Journal of Discrete Mathematical Sciences and Cryptography, the Journal of Theoretical and Applied Information Technology, and the Journal of Information Security and Applications, the remaining sources clearly exhibit notable connections (see Fig. 9).

TABLE XIII. TOP 10 SOURCES

No	Source	Documents	Citations	Total Link Strength
1	IEEE Access	3	17	29
2	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	2	18	28
3	Designs, Codes, and Cryptography	2	16	27
4	Theoretical Computer Science	2	15	25
5	Mathematics	3	11	23
6	Journal Of Cryptology	2	13	17
7	Cryptography	2	11	14
8	Journal Of Discrete Mathematical Sciences and Cryptography	3	54	4
9	Journal Of Theoretical and Applied Information Technology	4	11	4
10	Journal Of Information Security and Applications	3	106	1

Fig. 9. Source network visualization map

- **Network of keyword clusters**

A co-occurrence analysis of keywords was performed to ascertain the directions and development of research in threat hunting and RSA. The selection of keywords delineates the extent of any research inquiry. A network of keyword groupings was established on the basis of 333 keywords. The study set a minimum threshold of 3 instances of co-occurrence of a keyword, which, in turn, led to 33 keywords that had such co-occurrences. The analysis identified four major clusters. Eleven keywords were in the first cluster, the second cluster consisted of 11 keywords, the third cluster had 6 keywords, and the fourth cluster had 5 keywords. To promote a meaningful discussion, the clusters are shown in different colors to correspond with the timeframe in which these terms were thought to be active (see the visualization map in Fig. 10). Some of the notable terms in this cluster are cryptanalysis, cryptography, and RSA, as shown in Table 14.

TABLE XIV. TOP 10 COOCCURRING KEYWORDS

No	Keyword	Occurrences	Total Link Strength
1	Cryptanalysis	34	109
2	Cryptography	28	107
3	RSA	23	77
4	Public Key Cryptography	9	30
5	Continued Fraction	8	26
6	Factorization	8	35
7	Continued Fractions	6	20
8	Coppersmith's Method	6	21
9	RSA Moduli	6	20
10	Algorithms	5	21

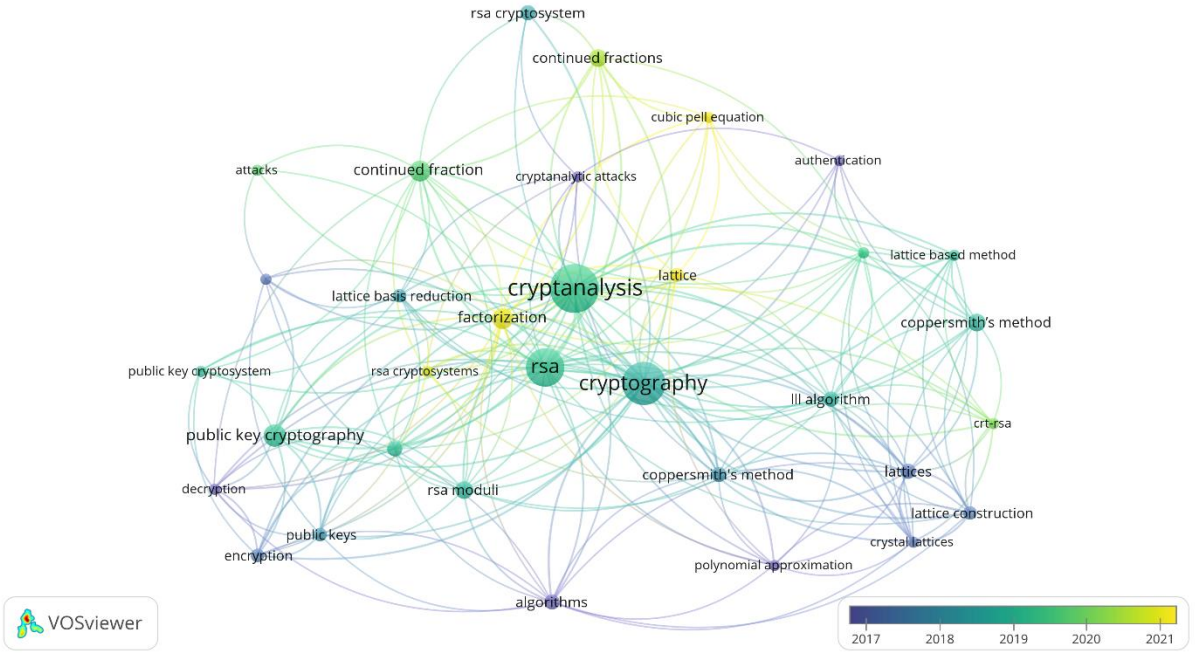

Fig. 10. Overlay visualization map of cooccurring keywords

- **Cocitation Networks of Authors**

This analysis seeks to uncover the relationships and connections between authors frequently referenced together. A network illustrating cocitation relationships among authors was established on the basis of 1075 authors. Considering a minimum threshold of 20 citations per author, 26 authors use this threshold. The bibliometric visualization in Figure 11 displays a map featuring three thematic clusters that have emerged from the cocitation connections among authors. May stands out as a prominent figure with the highest number of citations (111 citations), trailed by Kunihiro (67 citations) and Boneh (60 citations) within Cluster 1 (highlighted in red) and Cluster 3 (depicted in blue).

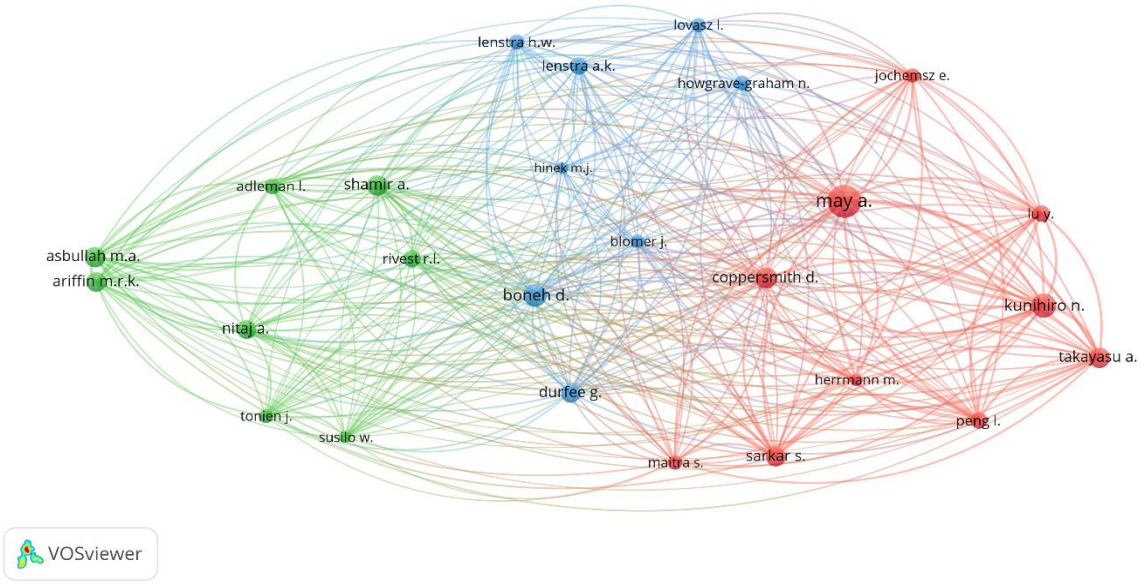

Fig. 11. Cocitation of authors

RQ4: What are the anticipated directions for prospective research in this domain?

Although the adoption of mathematical techniques has expanded significantly since 2018 for evaluating the vulnerabilities of the RSA cryptosystem, the modern world is increasingly inclined towards technological advancements with significant implications. As computational power advances, the anticipation of more sophisticated cyberattacks grows. Hence, to safeguard RSA from all possible threats, it is essential to look into the algebraic structure of RSA and how it can be used to neutralize all other forms of threat. Many researchers have also started looking for DL-based methods to handle the threat detection problem quickly and more effectively [102], [103], [104], [105]. It is evident from Tables 6, 7, 8, 9, and 10 that no existing algorithms based on the primary articles have employed DL approaches in conducting threat hunting under the RSA cryptosystem.

Recent work, such as Gohr's DL-based differential cryptanalysis of the Speck32/64 cipher, has demonstrated that neural networks outperform classical distinguishers in recognizing subtle patterns. Although symmetric and asymmetric ciphers differ significantly, such results suggest that DL may similarly uncover exploitable structures in the RSA system. Hence, researchers must carefully evaluate the different aspects of the established frameworks, such as the preferred learning methods, DL designs, hyperparameter settings, optimization strategies, and training processes, while considering the flexibility of a specific framework for a particular RSA-related task or the potential need to develop a new framework.

Factorization attacks are still among the most critical aspects of RSA security analysis. The essence of RSA security is based on the assumption that it is difficult to factorize large composite numbers randomly generated via two large prime numbers. Future works may investigate the design of factorization attacks that integrate RNNs or transformer-based architectures. RNNs, which are optimized for sequential data processing, can be used to evaluate numbers and sequences in various ways to predict their prime factors or find relationships between the factors in the modulus. In the same way, attention-based networks such as transformers can be employed to narrow down certain features in a vast collection of RSA keys. These models' ability to model long-range correlations could assist in these cases by framing the attacks through susceptible modulus factors. This is especially true when the factors are shared or the randomness in generating primes is low.

The incorporation of long short-term memory (LSTM) networks could improve Fermat's factoring technique. The rationale behind this method is the ability to express any odd number as the product of two numbers represented in the form of $n = x^2 - y^2$. This can simply be rephrased as $n = (x + y)(x - y)$. In this strategy, however, the best result is achieved when there is a slight difference between the two factors of the prime number n. Otherwise, it tends to be less productive when the factors are further apart. LSTM can learn long-range dependencies and facilitate more precise predictions of sequences of x and y values that are proximate to the solution.

In attacks targeting RSA moduli that exhibit common factors, conventional techniques such as the greatest common divisor (GCD) algorithm can reveal common factors present between pairs of moduli; however, a message-passing neural network (MPNN), a specific variant of a graph neural network (GNN), can extend this analysis across significantly larger datasets among multiple moduli. MPNNs are well suited for problems involving graph data, as they can efficiently find all the relationships between different nodes (in this case, the RSA modulus) and work with big data more effectively. MPNNs facilitate the transmission of information among interconnected nodes (i.e., moduli with the potential for shared factors) within the graph. The standard prime factors can function as "hidden connections" between moduli, and MPNNs can iteratively refine the representations of the nodes through the process of passing messages, thereby enabling the network to learn patterns indicative of commonality.

When the private exponent, denoted as d, is small, Wiener's theorem shows that d can be retrieved via a continued fraction method, contingent upon the condition that $d < N^{0.25d}$. The small magnitude of d results in a diminished search space, rendering the RSA cryptosystem susceptible to cryptanalytic attacks. While simple, vanilla RNNs can automate and potentially amplify this attack by predicting small d values predicated on the interrelations between the components of the public keys, specifically e and N. They are a good starting point for exploring sequential data in RSA public keys.

Variational autoencoders (VAEs) are generative models capable of learning complex distributions. They prove particularly advantageous for modelling uncertainty in the data and can produce new instances that closely mimic the training dataset. In the context of RSA partial key exposure attacks, VAEs can be trained on a dataset of RSA keys to learn the distribution of key components and reconstruct missing bits from partially exposed keys. The model can utilize the exposed segment of a private key, in conjunction with N and e, as inputs to predict the missing portion of the private key.

The reinforcement learning (RL) architecture, most notably the deep Q-network (DQN) and proximal policy optimization (PPO) architectures, could play a pivotal role in shaping adaptive attack strategies. For example, the DQN can be applied to small private exponent attacks, whereby the model learns the optimal set of guesses or transformations that converge on the possible solutions as quickly as possible. Techniques such as PPO can dynamically adapt and support policy gradient methods for partial key exposure attacks by leveraging better predictions of the missing bits of a private key in real time.

Moreover, actor–critic frameworks such as the advantage actor–critics (A2C) could offer advantages in scenarios where RSA keys are generated with particular patterns or predictable structures. For example, in prime factorization challenges involving weak primes (such as those that share bits), an actor–critic model could steer the exploration of potential factors, utilizing learned relationships between bit patterns and factor candidates to narrow the search space effectively.

We also recommend hybrid approaches in RSA cryptanalysis, as they offer a promising pathway. For instance, lattice reduction can shrink the key search space (e.g., identifying $d < N^{0.3}$). Then, an RNN can be applied to classify keys as vulnerable or predict likely candidates (inspired by Gohr's 'distinguisher' paradigm), mirroring how classical sieving accelerates DL in number field sieve factoring to bridge the strengths of classical and AI-driven cryptanalysis.

Further studies into the following areas during the training phase are needed to improve the optimization of DL models across larger RSA keyspaces:

The ability to produce such synthetic datasets is the greatest need, especially for larger RSA keyspaces. This is achievable through developing algorithms capable of generating a variety of key pairs, including those with unique cryptographic properties, to improve model training. Large keyspaces require a good memory management approach. Mixed-precision training can help reduce memory usage significantly without affecting the model's performance, especially for RSA key sizes larger than 1024 bits. In addition, frameworks such as TensorFlow and PyTorch support distributed training, which helps speed up model convergence.

Studies on automated hyperparameter tuning via Hyperopt or Optuna will help determine the best configuration parameters. This will be important in tuning the hyperparameters to scale the DL models to larger key spaces. Furthermore, in the application of curriculum learning, initially, less complicated cryptographic problems are presented before more complex problems are presented later. Such an approach should enable the models to cope more effectively with the issues resulting from the large RSA keyspace.

Although significantly improving the scalability and pattern recognition of the systems developed within the DL model, these merits come at the price of increased computational resource consumption. Nevertheless, effective hardware acceleration methods and effective model synthesis techniques have been advanced to mitigate these computational challenges. In particular, model compression techniques such as pruning and quantization should be focused on, as they help lower the computational cost.

As cryptographic design paradigms shift toward resource-constrained environments such as the IoT, such as those offered by lightweight cryptographic systems, the DL models we have proposed in this study could, in future work, be adapted to assess the security of lightweight cryptographic design paradigms [106], [107], [108], [109], particularly those utilizing asymmetric primitives [110], [111], [112]. ECC and postquantum schemes such as the CRYSTALS-Kyber are gaining prominence because of their efficiency and smaller key sizes. These systems, however, also exhibit structural

vulnerabilities. ECC and RSA share specific algebraic vulnerabilities, such as susceptibility to side-channel attacks on scalar multiplication and the risks associated with weak parameter generation. This line of research could enable a unified framework for intelligent cryptanalysis across diverse cryptographic paradigms.
To summarize, the research directions above facilitate a trajectory for researchers to investigate and formulate DL models designed explicitly for cryptographic analysis, especially given the weaknesses in the RSA algebraic structure that are not present in the existing classical approaches. This continues to be an essential and active area of research in information security to protect cyberspace against more sophisticated cryptanalytic threats.

- **Ethics: Dual-Use Risk and Mitigation**

This study recognizes that using DL in cryptanalysis can be a double-edged sword. The main aim is to improve security and strengthen encryption, but these techniques could be misused. To address this issue, any tools, models, or datasets created will be used only in academic, government, or authorized cybersecurity research settings. It is important to have controlled access and responsible sharing practices to avoid potential misuse.

- **Limitations of the Study**

This study focuses primarily on reviewing attacks on RSA primitives and algebraic structures, such as factorizations, weak private exponents, partial key exposures, encryption schemes, and key equation attacks, and highlights the potential of DL for RSA cryptanalysis. In particular, this study does not focus on other aspects of RSA cryptanalysis, such as side-channel attacks, fault analysis, timing attacks or other techniques that do not rely on algebraic primitives. The study does not provide practical implementations or empirical simulations of the suggested DL models applied to cryptographic tasks. These tasks are recommended for further studies.

5. CONCLUSION

The present work comprehensively reviewed the application of DL models as the basis for attacking the algebraic structure of RSA systems, emphasizing the transition from classical cryptanalysis techniques toward more advanced DL techniques. While previous studies have concentrated on classical methods such as the Coppersmith Lattice-Based, Continued Fractions, Quadratic Sieve Algorithm and Fermat factoring methods, this review identifies the untapped potential of DL models in augmenting these attacks. In this study, no DL model has been employed to enhance the RSA algebraic threat-hunting task. By highlighting the ability of DL architectures such as RNNs, LSTM networks, transformer models, GNNs and GANs to generate and process large datasets, detect patterns, and handle sequential data, we illustrate how DL models can expedite and automate RSA attacks in areas such as shared common primes, partial key exposure, weak private exponent recovery, encryption schemes, key equations and modulus factorization. Researchers can improve the capacity and accuracy of cryptanalytic operations via the use of DL. This presents avenues to eliminate the limitations of the classical methods as we move towards larger key sizes.
We propose the following immediate next steps to operationalize DL in RSA cryptanalysis. First, we advocate benchmarking VAEs on synthetic RSA datasets to evaluate their ability to cluster weak keys (e.g., $d < N^{0.3}$) in latent space, leveraging the synthetic data pipeline detailed in this study. Second, as suggested, the hybrid lattice-RNN framework requires rigorous validation against the classical methods on large key sizes, quantifying trade-offs between computational speed and detection accuracy to assess practical viability. Finally, researchers should pay attention to training and validation of the DL architectures described in this study to determine their performance in breaching RSA systems and, as a result, help design better security systems to guarantee the long-term sustainability of the RSA scheme. Enhancing RSA cryptanalysis via AI reinforces current systems and informs transition strategies toward postquantum cryptographic standards by identifying potential vulnerabilities before quantum attacks become viable. By identifying algebraic attack thresholds (e.g., d bounds) optimized with DL, we provide actionable criteria for key generation audits.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

There was no financial support from any source.

Acknowledgement

We thank the research team at the Department of Computer Science and Informatics, University of Energy and Natural Resources, Sunyani, Ghana, for their comments and suggestions.

References

[1] R. Renner Renner@Ethz.Ch and R. Wolf, 'Quantum Advantage in Cryptography', *AIAA Journal*, vol. 61, no. 5, pp. 1895–1910, May 2023, doi: 10.2514/1.J062267.

[2] S. Bhattacharya, 'Cryptology, Cryptography, and Cryptoanalysis-Past, Present and Future Role in Society', 2019. [Online]. Available: www.researchpublish.com

[3] H. Li and Y. Wang, 'The History of Cryptography and Its Applications', *International Journal of Social Science and Education Research*, vol. 5, p. 2022, 2022, doi: 10.6918/IJOSSER.202203_5(3).0056.

[4] F. Lalem, A. Laouid, M. Kara, M. Al-Khalidi, and A. Eleyan, 'A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques', 2023, doi: 10.3390/app.

[5] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, 'A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review', Apr. 01, 2023, *MDPI*. doi: 10.3390/s23084117.

[6] Y. Salami, V. Khajehvand, and E. Zeinali, 'Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges', 2023.

[7] C. Ma, 'Exploring RSA Cryptography: Principles and Applications in Image Encryption and Microcontroller Security', *Applied and Computational Engineering*, vol. 94, no. 1, pp. 203–209, Nov. 2024, doi: 10.54254/2755-2721/94/2024MELB0091.

[8] M. Ding, 'Analyzing the Research and Application of the RSA Cryptosystem in the Context of Digital Signatures', *Transactions on Computer Science and Intelligent Systems Research*, vol. 5, pp. 26–34, Aug. 2024, doi: 10.62051/j2p6g984.

[9] O. Sarjiyus and M. Hamidu, 'Improved Card Payment Security Using RSA Cryptography', *International Journal of Applied Science and Mathematical Theory E*, vol. Vol. 11 No. 2 2025, 2025, doi: 10.56201/ijasmt.vol.11.no2.2025.pg45.70.

[10] K. Somsuk, 'The special algorithm based on RSA cryptography for signing and verifying digital signature', *Heliyon*, vol. 11, no. 4, Feb. 2025, doi: 10.1016/j.heliyon.2025.e42481.

[11] V. N. H. Kollipara, S. K. Kalakota, S. Chamarthi, S. Ramani, P. Malik, and M. Karuppiah, 'Timestamp Based OTP and Enhanced RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices', *Journal of Cyber Security and Mobility*, vol. 12, no. 1, pp. 77–102, 2023, doi: 10.13052/jcsm2245-1439.1214.

[12] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, 'Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment', *In Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40 (pp. 62-91). Springer International Publishing.*, Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.06197

[13] J. Liu, H. Zhang, and J. Jia, 'Cryptanalysis of schemes based on polynomial symmetrical decomposition', *Chinese Journal of Electronics*, vol. 26, no. 6, pp. 1139–1146, Nov. 2017, doi: 10.1049/cje.2017.05.005.

[14] J. Tomčala, 'On the Various Ways of Quantum Implementation of the Modular Exponentiation Function for Shor's Factorization', *International Journal of Theoretical Physics*, vol. 63, no. 1, Jan. 2024, doi: 10.1007/s10773-023-05532-4.

[15] Y. Afaq and A. Manocha, 'Blockchain and Deep Learning Integration for Various Application: A Review', 2024, *Taylor and Francis Ltd.* doi: 10.1080/08874417.2023.2173330.

[16] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, 'A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning', *Archives of Computational Methods in Engineering*, vol. 27, no. 4, pp. 1071–1092, Sep. 2020, doi: 10.1007/s11831-019-09344-w.

[17] Y. Hou, J. Liu, S. Han, Z. Ma, X. Ye, and X. Nie, 'Improving deep learning-based neural distinguisher with multiple ciphertext pairs for speck and Simon', *Sci Rep*, vol. 15, no. 1, p. 13696, Apr. 2025, doi: 10.1038/s41598-025-98251-1.

[18] Y. Lu, Y. Guo, W. Liu, W. Chen, Q. Yan, and B. Yu, 'Enhanced Neural Distinguisher Model for Efficient Differential Cryptanalysis', *IEEE Internet Things J*, pp. 1–1, 2025, doi: 10.1109/JIOT.2025.3566051.

[19] Z. Hou, J. Ren, and S. Chen, 'Improved machine learning-aided linear cryptanalysis: application to DES', *Cybersecurity*, vol. 8, no. 1, p. 22, Apr. 2025, doi: 10.1186/s42400-024-00327-4.

[20] O. Jeong, E. Ahmadzadeh, and I. Moon, 'Comprehensive Neural Cryptanalysis on Block Ciphers Using Different Encryption Methods', *Mathematics*, vol. 12, no. 13, p. 1936, Jun. 2024, doi: 10.3390/math12131936.

[21] V. Radhakrishnan, V. Rodda, S. Sowmiya, A. R. Sarker, R. Palanikumar, and R. Asokan, 'Deep Learning-Driven Cryptanalysis in Modern Encryption Systems', in *2025 International Conference on Visual Analytics and Data Visualization (ICVADV)*, IEEE, Mar. 2025, pp. 226–230. doi: 10.1109/ICVADV63329.2025.10960919.

[22] O. Jeong, E. Ahmadzadeh, and I. Moon, 'Comprehensive Neural Cryptanalysis on Block Ciphers Using Different Encryption Methods', *Mathematics*, vol. 12, no. 13, Jul. 2024, doi: 10.3390/math12131936.
[23] K. Kumar, S. Tanwar, and S. Kumar, 'Deep-Learning-based Cryptanalysis through Topic Modeling', *Engineering, Technology and Applied Science Research*, vol. 14, no. 1, pp. 12524–12529, Feb. 2024, doi: 10.48084/etasr.6515.
[24] H. Grari, K. Zine-Dine, A. Azouaoui, and S. Lamzabi, 'deep Learning-Based Cryptanalysis of a Simplified AeS Cipher', *International Journal of Information Security and Privacy*, vol. 16, no. 1, 2022, doi: 10.4018/IJISP.300325.
[25] A. Gohr, 'Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2019, pp. 150–179. doi: 10.1007/978-3-030-26951-7_6.
[26] S. Park, H. Kim, and I. Moon, 'Automated Classical Cipher Emulation Attacks via Unified Unsupervised Generative Adversarial Networks', *Cryptography*, vol. 7, no. 3, Sep. 2023, doi: 10.3390/cryptography7030035.
[27] J. So, 'Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers', *Security and Communication Networks*, vol. 2020, 2020, doi: 10.1155/2020/3701067.
[28] M. F. Idris, J. Sen Teh, J. L. S. Yan, and W. Z. Yeoh, 'A Deep Learning Approach for Active S-Box Prediction of Lightweight Generalized Feistel Block Ciphers', *IEEE Access*, vol. 9, pp. 104205–104216, 2021, doi: 10.1109/ACCESS.2021.3099802.
[29] H. Grari, K. Zine-Dine, A. Azouaoui, and S. Lamzabi, 'deep Learning-Based Cryptanalysis of a Simplified AeS Cipher', *International Journal of Information Security and Privacy*, vol. 16, no. 1, 2022, doi: 10.4018/IJISP.300325.
[30] R. Focardi and F. L. Luccio, 'Neural Cryptanalysis of Classical Ciphers', 2018.
[31] M. Danziger and M. A. A. Henriques, 'Improved cryptanalysis combining differential and artificial neural network schemes', in *2014 International Telecommunications Symposium, ITS 2014 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Nov. 2014. doi: 10.1109/ITS.2014.6948008.
[32] S. Fan and Y. Zhao, 'Analysis of des Plaintext Recovery Based on BP Neural Network', *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/9580862.
[33] X. Hu and Y. Zhao, 'Research on Plaintext Restoration of AES Based on Neural Network', *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/6868506.
[34] B. Zahednejad and L. Lyu, 'An improved integral distinguisher scheme based on neural networks', *International Journal of Intelligent Systems*, vol. 37, no. 10, pp. 7584–7613, Oct. 2022, doi: 10.1002/int.22895.
[35] 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', 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3129224.
[36] B. K and D. S.S, 'An Overview of Cryptanalysis of RSA Public key System', *International Journal of Engineering and Technology*, vol. 9, no. 5, pp. 3575–3579, Oct. 2017, doi: 10.21817/ijet/2017/v9i5/170905312.
[37] A. Takayasu and N. Kunihiro, 'Better lattice constructions for solving multivariate linear equations modulo unknown divisors', *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 6, pp. 1259–1272, 2014, doi: 10.1587/transfun.E97.A.1259.
[38] M. Zheng, H. Hu, and Z. Wang, 'Generalized cryptanalysis of RSA with e < N0.5', *Science China Information Sciences*, vol. 59, no. 3, p. 32108, Mar. 2015, doi: 10.1007/s11432-015-5325-7.
[39] N. Ojha and S. Padhye, 'Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key', 2014.
[40] X. Meng and X. Zheng, 'Cryptanalysis of RSA with a small parameter revisited', *Inf Process Lett*, vol. 115, no. 11, pp. 858–862, Jul. 2015, doi: 10.1016/j.ipl.2015.06.013.
[41] A. Abubakar *et al.*, 'Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) Cryptosystem: Issues and Challenges', *J Theor Appl Inf Technol*, vol. 10, no. 1, 2014, [Online]. Available: www.jatit.org
[42] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, 'Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves', *Journal of Information Security and Applications*, vol. 40, pp. 193–198, Jun. 2018, doi: 10.1016/j.jisa.2018.04.006.
[43] M. C. Zheng and H. G. Hu, 'Cryptanalysis of Prime Power RSA with two private exponents', *Science China Information Sciences*, vol. 58, no. 11, Nov. 2015, doi: 10.1007/s11432-015-5409-4.
[44] L. Peng and A. Takayasu, 'Generalized cryptanalysis of small CRT-exponent RSA', *Theor Comput Sci*, vol. 795, pp. 432–458, Nov. 2019, doi: 10.1016/j.tcs.2019.07.031.
[45] M. Thangavel, P. Varalakshmi, M. Murrali, and K. Nithya, 'An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)', *Journal of Information Security and Applications*, vol. 20, pp. 3–10, Feb. 2015, doi: 10.1016/j.jisa.2014.10.004.

[46] S. I. Abubakar, M. R. K. Ariffin, and Asbullah, 'A New Improved Bound for Short Decryption Exponent on RSA Modulus N = pq using Wiener's Method', 2019.
[47] D. Aggarwal and U. Maurer, 'Breaking RSA Generically is Equivalent to Factoring', *IEEE Trans Inf Theory*, vol. 62, no. 11, pp. 6251–6259, Nov. 2016, doi: 10.1109/TIT.2016.2594197.
[48] A. Takayasu, Y. Lu, and L. Peng, 'Small CRT-Exponent RSA Revisited', *Journal of Cryptology*, vol. 32, no. 4, pp. 1337–1382, Oct. 2019, doi: 10.1007/s00145-018-9282-3.
[49] E. Lüy, Z. Y. Karatas, and H. Ergin, 'Comment on "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)"', *Journal of Information Security and Applications*, vol. 30, pp. 1–2, Oct. 2016, doi: 10.1016/j.jisa.2016.03.006.
[50] R. R. M. Tahir, M. A. Asbullah, and M. R. K. Ariffin, 'The Blömer-May's Weak Key Revisited', *ASM Science Journal*, vol. 12, no. 5, pp. 143–149, 2019.
[51] J. S. Coron, D. Naccache, M. Tibouchi, and R. P. Weinmann, 'Practical Cryptanalysis of ISO 9796-2 and EMV Signatures', *Journal of Cryptology*, vol. 29, no. 3, pp. 632–656, Jul. 2016, doi: 10.1007/s00145-015-9205-5.
[52] M. R. K. Ariffin, S. I. Abubakar, M. A. Asbullah, and F. Yunos, 'New cryptanalytic attack on rsa modulus n = pq using small prime difference method', *Cryptography*, vol. 3, no. 1, pp. 1–25, Mar. 2019, doi: 10.3390/cryptography3010002.
[53] J. Weng, Y.-Q. Dou, and C.-G. Ma, 'The Attack of the RSA Subgroup Assumption *', *JOURNAL OF INFORMATION SCIENCE AND ENGINEERING*, vol. 32, pp. 597–610, 2016, doi: 10.1688/JISE.2016.32.3.5.
[54] M. A. Asbullah and M. R. K. Ariffin, 'Another proof of Wiener's short secret exponent', *Malaysian Journal of Science*, vol. 38, pp. 67–73, 2019, doi: 10.22452/mjs.sp2019no1.6.
[55] S. Zoubir and A. Tragha, 'Uses of Genetic Algorithm in Cryptanalysis of RSA', *IOSR Journal of Computer Engineering (IOSR-JCE)* , vol. 18, no. 3, pp. 48–52, 2016, doi: 10.9790/0661-1803014852.
[56] T. Mefenza and D. Vergnaud, 'Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting', *Gerontologist*, vol. 59, no. 4, pp. 1194–1213, Aug. 2019, doi: 10.1093/comjnl/bxz040.
[57] L. Peng, L. Hu, Y. Lu, J. Xu, and Z. Huang, 'Cryptanalysis of Dual RSA', *Des Codes Cryptogr*, vol. 83, no. 1, pp. 1–21, Apr. 2017, doi: 10.1007/s10623-016-0196-5.
[58] M. Mumtaz and L. Ping, 'Forty years of attacks on the RSA cryptosystem: A brief survey', *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 1, pp. 9–29, Jan. 2019, doi: 10.1080/09720529.2018.1564201.
[59] M. Mumtaz and L. Ping, 'Remarks on the cryptanalysis of common prime RSA for IoT constrained low power devices', *Inf Sci (N Y)*, vol. 538, pp. 54–68, Oct. 2020, doi: 10.1016/j.ins.2020.05.075.
[60] M. Thangavel and P. Varalakshmi, 'Improved secure RSA cryptosystem for data confidentiality in cloud', 2017. [Online]. Available: https://azure.microsoft.com/en-in/documentation/articles/storage-encrypt-decrypt-
[61] M. Zheng, N. Kunihiro, and Y. Yao, 'Cryptanalysis of the RSA variant based on cubic Pell equation', *Theor Comput Sci*, vol. 889, pp. 135–144, Oct. 2021, doi: 10.1016/j.tcs.2021.08.001.
[62] Y. Aono, M. Agrawal, T. Satoh, and O. Watanabe, 'On the optimality of lattices for the coppersmith technique', *Applicable Algebra in Engineering, Communications and Computing*, vol. 29, no. 2, pp. 169–195, Mar. 2018, doi: 10.1007/s00200-017-0336-9.
[63] M. M. Almazari, E. Taqieddin, A. S. Shatnawi, and Z. Al-Shara, 'An evaluation of the RSA private keys and the presence of weak keys', *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 8, pp. 2273–2284, 2023, doi: 10.47974/JDMSC-1670.
[64] P. A. Kameswari and L. Jyotsna, 'An attack bound for small multiplicative inverse of ϕ(N) mod e with a composed prime sum p + q using sublattice based techniques', *Cryptography*, vol. 2, no. 4, pp. 1–15, Dec. 2018, doi: 10.3390/cryptography2040036.
[65] Q. Li, Q. Zheng, and W. Qi, 'Practical attacks on small private exponent RSA: new records and new insights', *Des Codes Cryptogr*, vol. 91, no. 12, pp. 4107–4142, Dec. 2023, doi: 10.1007/s10623-023-01295-5.
[66] C. J. Padmaja and B. Srinivas, 'ON THE USAGE OF ARYABHATTA REMAINDER THEOREM FOR IMPROVED PERFORMANCE OF RPRIME RSA', *J Theor Appl Inf Technol*, vol. 15, p. 9, 2018, [Online]. Available: www.jatit.org
[67] M. Zheng, 'Revisiting Small Private Key Attacks on Common Prime RSA', *IEEE Access*, vol. 12, pp. 5203–5211, 2024, doi: 10.1109/ACCESS.2024.3349633.
[68] A. Nitaj and E. Fouotsa, 'A new attack on RSA and Demytko's elliptic curve cryptosystem', *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 3, pp. 391–409, Apr. 2019, doi: 10.1080/09720529.2019.1587827.
[69] S. I. Abubakar, M. R. K. Ariffin, and M. A. Asbullah, 'Successful Cryptanalytic Attacks Upon RSA Moduli N = pq', *Malaysian Journal of Mathematical Sciences*, vol. 13, no. S, 2019.

[70] A. Takayasu and N. Kunihiro, 'Partial key exposure attacks on RSA: Achieving the Boneh–Durfee bound', *Theor Comput Sci*, vol. 761, pp. 51–77, Feb. 2019, doi: 10.1016/j.tcs.2018.08.021.

[71] N. Nek, A. Rahman, M. Rezal, K. Ariffin, and M. A. Asbullah, 'Successful Cryptanalysis upon a Generalized RSA Key Equation', *ASM Science Journal*, vol. 12, pp. 191–202, 2019, Accessed: May 07, 2024. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071509052&partnerID=40&md5=01d25ac5cba94490bfa8dd80a4bc13f9

[72] A. H. Abd Ghafar, M. R. Kamel Ariffin, S. M. Yasin, and S. H. Sapar, 'Partial key attack given msbs of crt-rsa private keys', *Mathematics*, vol. 8, no. 12, pp. 1–20, Dec. 2020, doi: 10.3390/math8122188.

[73] W. N. A. Ruzai, M. R. K. Ariffin, M. A. Asbullah, Z. Mahad, and A. Nawawi, 'On the improvement attack upon some variants of RSA cryptosystem via the continued fractions method', *IEEE Access*, vol. 8, pp. 80997–81006, 2020, doi: 10.1109/ACCESS.2020.2991048.

[74] K. Suzuki, A. Takayasu, and N. Kunihiro, 'Extended partial key exposure attacks on RSA: Improvement up to full size decryption exponents', *Theor Comput Sci*, vol. 841, pp. 62–83, Nov. 2020, doi: 10.1016/j.tcs.2020.07.004.

[75] M. Zheng, N. Kunihiro, and H. Hu, 'Lattice-based cryptanalysis of RSA with implicitly related keys', *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103A, no. 8, pp. 959–968, Aug. 2020, doi: 10.1587/transfun.2019EAP1170.

[76] N. N. H. Adenan, M. R. Kamel Ariffin, S. H. Sapar, A. H. Abd Ghafar, and M. A. Asbullah, 'New jochemsz-may cryptanalytic bound for RSA system utilizing common modulus N = p2q', *Mathematics*, vol. 9, no. 4, pp. 1–13, Feb. 2021, doi: 10.3390/math9040340.

[77] N. N. A. Rahman, M. A. Asbullah, M. R. K. Ariffin, S. H. Sapar, and F. Yunos, 'Cryptanalysis of rsa key equation of N=p2mq for small |2q - P| using continued fraction', *Malaysian Journal of Science*, vol. 39, no. 1, pp. 72–80, Feb. 2020, doi: 10.22452/mjs.vol39no1.6.

[78] O. Pujeri, U. Pujeri, T. Baraskar, and P. Parlewar, 'Implementation of Novel Symmetric Encryption Algorithm to secure Information-Two Layer DNA-RSA Hybrid Cryptosystem', *International Journal of Intelligent Systems and Applications in Engineering IJISAE*, vol. 2023, no. 10s, pp. 94–102, 2023, [Online]. Available: www.ijisae.org

[79] D. Rachmawati, H. A. Tamara, S. Sembiring, and M. A. Budiman, 'RSA PUBLIC KEY SOLVING TECHNIQUE BY USING GENETIC ALGORITHM', *J Theor Appl Inf Technol*, vol. 15, p. 15, 2020, [Online]. Available: www.jatit.org

[80] K. R. Raghunandan, A. Ganesh, S. Surendra, and K. Bhavya, '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*, vol. 20, no. 3, pp. 86–101, Sep. 2020, doi: 10.2478/cait-2020-0030.

[81] H. M. Bahig, D. I. Nassr, A. Bhery, and A. Nitaj, 'A Unified Method for Private Exponent Attacks on RSA Using Lattices', *International Journal of Foundations of Computer Science*, vol. 31, no. 2, pp. 207–231, Feb. 2020, doi: 10.1142/S0129054120500045.

[82] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimeh, 'A new RSA public key encryption scheme with chaotic maps', *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1430–1437, 2020, doi: 10.11591/ijece.v10i2.pp1430-1437.

[83] G. A. Zimbele and S. A. Demilew, 'Hidden Real Modulus RSA Cryptosystem', *International Journal of Computing*, vol. 22, no. 2, pp. 238–247, 2023, doi: 10.47839/ijc.22.2.3094.

[84] A. H. Abd Ghafar, M. R. Kamel Ariffin, and M. A. Asbullah, 'A new LSB attack on special-structured RSA primes', *Symmetry (Basel)*, vol. 12, no. 5, May 2020, doi: 10.3390/SYM12050838.

[85] D. Vergnaud, 'Comment on "Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things"', *IEEE Internet Things J*, vol. 7, no. 11, pp. 11327–11329, Nov. 2020, doi: 10.1109/JIOT.2020.3004346.

[86] Y. Wang, H. Zhang, and H. Wang, 'Quantum polynomial-time fixed-point attack for RSA', *China Communications*, vol. 15, no. 2, pp. 25–32, Feb. 2018, doi: 10.1109/CC.2018.8300269.

[87] D. Poulakis, 'An application of Euclidean algorithm in cryptanalysis of RSA', *Elemente der Mathematik*, vol. 75, no. 3, pp. 114–120, Jul. 2020, doi: 10.4171/em/411.

[88] I. Elashry, 'Cryptanalysis of Jain-Singh's identity-based RSA encryption', *Information Security Journal*, vol. 30, no. 1, pp. 57–61, 2021, doi: 10.1080/19393555.2020.1800150.

[89] M. S. Lydia, M. Andri Budiman, and D. Rachmawati, 'FACTORIZATION OF SMALL RPRIME RSA MODULUS USING FERMAT'S DIFFERENCE OF SQUARES AND KRAITCHIK'S ALGORITHMS IN PYTHON', *J Theor Appl Inf Technol*, vol. 15, no. 11, 2021, [Online]. Available: www.jatit.org

[90] W. Susilo, J. Tonien, and G. Yang, 'Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA', *Comput Stand Interfaces*, vol. 74, Feb. 2021, doi: 10.1016/j.csi.2020.103470.

[91] L. Jyotsna and L. Praveen Kumar, 'CRYPTANALYSIS OF RSA-LIKE CRYPTOSYSTEM WITH MODULUS N = pq AND ed ≡ 1(mod (p2 + p + 1)(q2 + q + 1))', *South East Asian J. of Mathematics and Mathematical Sciences*, vol. 17, no. 3, pp. 01–16, 2021.

[92] N. N. H. Adenan, M. R. K. Ariffin, F. Yunos, S. H. Sapar, and M. A. Asbullah, 'Analytical cryptanalysis upon N = p2q utilizing Jochemsz-May strategy', *PLoS One*, vol. 16, no. 3 March, Mar. 2021, doi: 10.1371/journal.pone.0248888.

[93] W. N. A. Ruzai, A. H. Abd Ghafar, N. R. Salim, and M. R. K. Ariffin, 'On (Unknowingly) Using Near-Square RSA Primes', *Symmetry (Basel)*, vol. 14, no. 9, Sep. 2022, doi: 10.3390/sym14091898.

[94] B. Wang, X. Yang, and D. Zhang, 'Research on Quantum Annealing Integer Factorization Based on Different Columns', *Front Phys*, vol. 10, Jun. 2022, doi: 10.3389/fphy.2022.914578.

[95] A. Nitaj, M. R. B. K. Ariffin, N. N. H. Adenan, T. S. C. Lau, and J. Chen, 'Security Issues of Novel RSA Variant', *IEEE Access*, vol. 10, pp. 53788–53796, 2022, doi: 10.1109/ACCESS.2022.3175519.

[96] D. Savić, P. Milić, B. Mažinjanin, and P. Spalević, 'Cryptanalytic attacks on RSA algorithm and its variants', *Przeglad Elektrotechniczny*, vol. 98, no. 2, pp. 14–20, 2022, doi: 10.15199/48.2022.02.04.

[97] Z. Mahad, M. R. K. Ariffin, A. H. A. Ghafar, and N. R. Salim, 'Cryptanalysis of RSA-Variant Cryptosystem Generated by Potential Rogue CA Methodology', *Symmetry (Basel)*, vol. 14, no. 8, Aug. 2022, doi: 10.3390/sym14081498.

[98] M. Zheng, 'Revisiting the Polynomial-Time Equivalence of Computing the CRT-RSA Secret Key and Factoring', *Mathematics*, vol. 10, no. 13, Jul. 2022, doi: 10.3390/math10132238.

[99] A. Nitaj, M. R. K. Ariffin, N. N. H. Adenan, D. S. Merenda, and A. Ahmadian, 'Exponential increment of RSA attack range via lattice based cryptanalysis', *Multimed Tools Appl*, vol. 81, no. 25, pp. 36607–36622, Oct. 2022, doi: 10.1007/s11042-021-11335-8.

[100] N. Nek Abd Rahman, 'Successful cryptanalysis on RSA type modulus N=p2q', *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, Jun. 2024, doi: 10.1016/j.prime.2024.100466.

[101] Y. Lu, L. Peng, and S. Sarkar, 'Cryptanalysis of an RSA variant with moduli N=prql', *Journal of Mathematical Cryptology*, vol. 11, no. 2, pp. 117–130, Jun. 2017, doi: 10.1515/jmc-2016-0025.

[102] H. Kim *et al.*, 'Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited', *Entropy*, vol. 25, no. 7, 2023, doi: 10.3390/e25070986.

[103] H. Kimura, K. Emura, T. Isobe, R. Ito, K. Ogawa, and T. Ohigashi, 'A Deeper Look into Deep Learning-based Output Prediction Attacks Using Weak SPN Block Ciphers', *Journal of Information Processing*, vol. 31, pp. 550–561, 2023, doi: 10.2197/IPSJJIP.31.550.

[104] D. Kwon, H. Kim, and S. Hong, 'Non-Profiled Deep Learning-Based Side-Channel Preprocessing with Autoencoders', *IEEE Access*, vol. 9, pp. 57692–57703, 2021, doi: 10.1109/ACCESS.2021.3072653.

[105] S. Park, H. Kim, and I. Moon, 'Automated Classical Cipher Emulation Attacks via Unified Unsupervised Generative Adversarial Networks', *Cryptography*, vol. 7, no. 3, 2023, doi: 10.3390/cryptography7030035.

[106] Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, 'Lightweight Cryptography for Internet of Things: A Review', *EAI Endorsed Transactions on Internet of Things*, vol. 10, Mar. 2024, doi: 10.4108/eetiot.5565.

[107] F. Hazzaa, M. M. Hasan, A. Qashou, and S. Yousef, 'A New Lightweight Cryptosystem for IoT in Smart City Environments', *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp. 46–58, Sep. 2024, doi: 10.58496/MJCS/2024/015.

[108] F. Hazzaa *et al.*, 'Performance Analysis of Advanced Encryption Standards for Voice Cryptography with Multiple Patterns', *International Journal of Safety and Security Engineering*, vol. 14, no. 5, pp. 1439–1446, Oct. 2024, doi: 10.18280/ijsse.140511.

[109] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, 'Lightweight cryptography system for IoT devices using DNA', *Computers and Electrical Engineering*, vol. 95, p. 107418, Oct. 2021, doi: 10.1016/j.compeleceng.2021.107418.

[110] M. Rana, Q. Mamun, and R. Islam, 'Lightweight cryptography in IoT networks: A survey', *Future Generation Computer Systems*, vol. 129, pp. 77–89, Apr. 2022, doi: 10.1016/j.future.2021.11.011.

[111] A. K. Nanda *et al.*, 'Evaluating Lightweight Asymmetric Cryptography for Secure Communication in Internet of Drones', in *2025 Fourth International Conference on Power, Control and Computing Technologies (ICPC2T)*, IEEE, Jan. 2025, pp. 875–879. doi: 10.1109/ICPC2T63847.2025.10958641.

[112] Y. Desai, 'A Comprehensive Survey on Lightweight Cryptographic Algorithms for IoT Security: Challenges and Future Directions', *Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596*, vol. 10, no. si4, 2025, [Online]. Available: http://j.vidhyayanaejournal.org/index.php/journal/article/view/2173