JISTecS: Journal of Information Systems, Technology and Security
ISSN 3125-1099 (online)
Vol. 1 Iss. 1 Pg. 20-45
https://ejournal.scmdigi.id/index.php/jistecs

A bibliometric analysis of rivest's cipher: trends and developments in modern cryptography

Decky Hendarsyah
Institut Syariah Negeri Junjungan Bengkalis, Riau, Indonesia
deckydb@gmail.com
DOI: https://doi.org/10.65881/jistecs.v1i1.48

ARTICLE INFO

History:
Received: 04-07-2026
Revised: 04-14-2026
Accepted: 04-15-2026
Published: 04-17-2026

Keywords:
rivest's cipher;
bibliometric;
modern cryptography;
stream chiper;
encryption algorithm.

ABSTRACT

Purpose: to systematically analyze the development of research on Rivest's Cipher in modern cryptography using a bibliometric approach.
Method: this study uses a quantitative bibliometric approach to examine research on Rivest's Cipher using Scopus data from 2010 to 2025. A total of 435 peer-reviewed journal articles were analyzed after applying selection criteria. The analysis was conducted using Scopus Analyzer and VOSviewer, covering publication trends, research contributions, keyword co-occurrence, and collaboration patterns. The results were visualized through network and density maps to provide an overview of the research landscape.
Findings: research on Rivest's Cipher generally increased from 2010 to 2025, peaking around 2021 before stabilizing. Contributions are mainly dominated by Asian countries, especially India and China. The main research themes focus on cryptography, encryption, and RC4, particularly in terms of security analysis. Collaboration patterns remain fragmented, and several gaps are identified, including limited studies on RC5 and RC6 and a lack of integration with modern technologies such as AI and blockchain, indicating opportunities for future research.
Implications: Rivest's Cipher remains influential in cryptography research and highlights key trends, contributors, and gaps. It suggests opportunities for collaboration and for exploring less-studied algorithms and emerging technologies, supporting the development of more secure and efficient cryptographic solutions.
Originality: lies in mapping Rivest's Cipher studies worldwide, highlighting trends, key authors, and research gaps for future exploration.

Introduction

The rapid development of information technology has increased the need for reliable data security systems, particularly in the context of digital communication and

the exchange of sensitive information (Shojaei et al., 2024). In modern cryptography, various encryption algorithms have been developed to ensure the confidentiality, integrity, and authenticity of data (Ramakrishna & Shaik, 2025). One significant contribution to this field is Ron Rivest's family of algorithms, known as Rivest's Cipher, including RC4, RC5, and RC6 (Farooq et al., 2024). These algorithms have been widely used across applications, from network protocols to software security systems, making them a relevant topic for in-depth study.

Along with the increasing use of Rivest's Cipher, various research topics have emerged, particularly regarding the performance, efficiency, and security of these algorithms. On the one hand, algorithms such as RC4 were once considered standards in communication protocols like SSL/TLS; on the other hand, numerous studies have revealed vulnerabilities that malicious parties can exploit (Almutairi & Sheldon, 2025; Mousavi et al., 2021b). This raises important questions about the extent to which Rivest's Cipher remains relevant and reliable in addressing the increasingly complex challenges of modern cryptography. Furthermore, the rapid development of new encryption algorithms underscores the need for a comprehensive evaluation of Rivest's Cipher's position and contribution within the current research landscape.

Based on the existing literature review, most previous studies have focused on technical analysis, performance evaluation, and security testing of individual Rivest's Cipher algorithms (Abidi et al., 2020; Al-Badrei & Alshawi, 2022; Al-Ta'i & Jumaa, 2019; Amin, 2010; Chalob et al., 2025; Dara & Manochehri, 2014; Elashry et al., 2012; Faisal & Abdul Ameer, 2020; Faragallah et al., 2022; Harish et al., 2016; L. Liu et al., 2011; Mahroos et al., 2024; Nagao et al., 2014; Rashmi et al., 2015; Shailaja & Krishnamurthy, 2019; Soboń et al., 2020; Suresh et al., 2015; Witwit et al., 2025; Wong et al., 2010; Zaki et al., 2025; Zhang et al., 2020). However, there is still limited research that systematically maps the development of scientific publications, research trends, author collaborations, and topic distributions related to Rivest's Cipher using a bibliometric approach. This gap indicates that, despite the abundance of technical studies, a comprehensive understanding of the direction of research development and the scientific dynamics in this field has not yet been fully explored. Therefore, this study offers novelty by adopting a bibliometric approach to analyze and map trends and developments in research on Rivest's Cipher in modern cryptography.

The objective of this study is to identify and analyze publication trends, collaboration patterns, and the evolution of research topics related to Rivest's Cipher. In addition, this study aims to reveal the distribution of scientific contributions by authors, institutions, and countries, and to identify research areas with potential for future development. Thus, this study is expected to provide a comprehensive overview of the research dynamics surrounding Rivest's Cipher within the context of modern cryptography. This research is of significant importance, as it offers strategic insights for researchers, academics, and practitioners to understand the direction of research development and identify opportunities for further exploration in cryptography. Through a systematic bibliometric analysis, this study is expected to serve as a valuable reference for research decision-making, the development of security technologies, and the formulation of information security policies. The main contribution of this study is to provide a comprehensive, structured scientific mapping of Rivest's Cipher, enriching the existing literature and opening avenues for more innovative and relevant future research.

In this study, five main research questions are formulated as the focus of analysis to understand the dynamics of research on Rivest's Cipher in modern cryptography:

RQ1: What are the publication trends for Rivest's Cipher in modern cryptography over a given period? RQ2: How is the distribution of scientific contributions on Rivest's Cipher based on authors, institutions, and countries? RQ3: What research topics or themes are most frequently discussed in relation to Rivest's Cipher? RQ4: What are the patterns of collaboration among researchers and institutions in Rivest's Cipher research? RQ5: What research gaps emerge from the existing literature, and what are the potential areas for further research?

Method

This study employs a quantitative bibliometric approach to analyze the development of the scientific literature on Rivest's Cipher in the context of modern cryptography. This approach is chosen because it provides a systematic and objective overview of publication trends, scientific contributions, and collaboration structures within a research field. Through this method, the study not only identifies the growth of the literature but also comprehensively maps the relationships among research topics and actors. The research data were obtained from the Scopus database, which offers broad coverage and high credibility in international scientific publications. The search was conducted in April 2026 using the following keywords: "Rivest Cipher" or "RC1" or "RC2" or "RC3" or "RC4" or "RC5" or "RC6" or "Ron Rivest" or "Ron Rivest encryption algorithm." The search was limited to titles, abstracts, and keywords, with a publication time range from 2010 to 2025 to ensure relevance to developments in modern cryptography. From the initial search results of 3,667 documents, a screening process was conducted using inclusion and exclusion criteria (Table 1), resulting in 435 documents deemed suitable for analysis.

Table 1 inclusion and exclusion criteria

Criteria	Inclusion (accepted)	Exclusion (rejected)
Time span	Publications between 2010 and 2025.	Publications before 2010 and after 2025.
Document type	Peer-reviewed journal articles.	Conference proceedings, books, book chapters, editorials, book reviews, and popular articles.
Language	Documents in English.	Documents other than English.
Subject area	Computer science and mathematics	Other
Availability	Full-text is available for analysis.	Only abstract or incomplete text is available.

The inclusion criteria for this study comprise peer-reviewed journal articles written in English, published in the fields of computer science and mathematics, and available in full text. Meanwhile, documents such as conference proceedings, books, editorials, and popular articles were excluded from the analysis. The selection process was conducted systematically to ensure the quality and relevance of the data used. Subsequently, the selected data were extracted and processed through a data-cleaning stage, which included normalising author names and affiliations and standardising keywords to avoid duplication and inconsistency. The bibliometric analysis was conducted using Scopus Analyzer and VOSviewer. The analytical techniques employed include publication trend analysis to examine annual article growth, scientific contribution analysis to identify dominant authors, institutions, and countries, and keyword co-occurrence analysis to map the main research themes.

In addition, this study applies co-authorship analysis to identify collaboration patterns among researchers and institutions, as well as co-citation and bibliographic coupling analyses to understand the intellectual relationships among publications. The analysis results are then visualised as a network and density maps to facilitate data interpretation. Through this approach, the study is expected to provide a comprehensive overview of trends, collaboration structures, and the direction of research on Rivest's Cipher, while also identifying research gaps that may present opportunities for future studies.

Results and discussion

Document by years

This section presents the distribution of research publications on Rivest's Cipher by year from 2010 to 2025, providing an overview of the development and dynamics of publication trends over time, as illustrated in Figure 1.

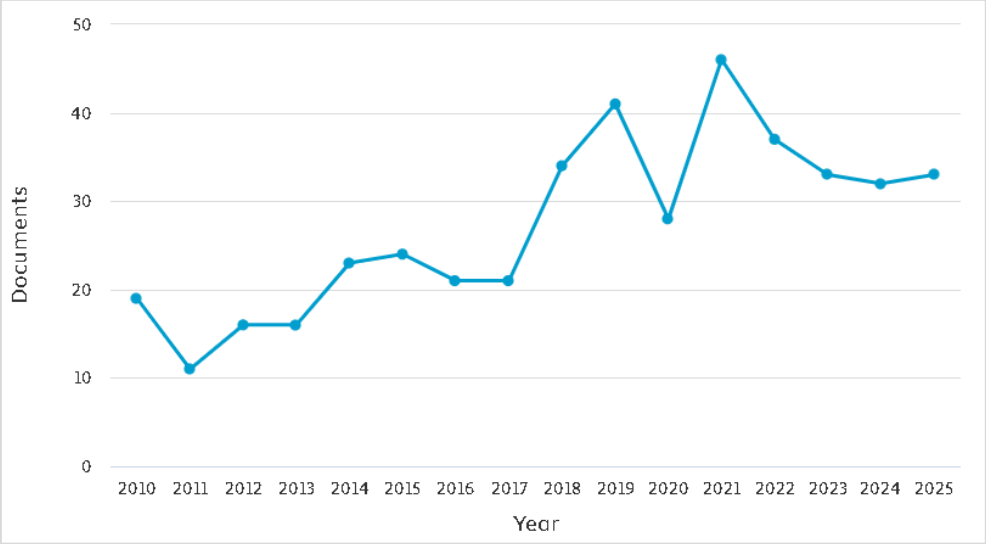

Figure 1 document by years
Source: Scopus, 2026

Based on the distribution of publications in Figure 1, it can be observed that the research trend related to Rivest's Cipher during the period from 2010 to 2025 experienced fluctuations, with a long-term tendency toward growth. At the beginning of the period, in 2010, the number of publications was 19, followed by a significant decrease to 11 in 2011. Subsequently, a gradual recovery occurred in 2012 and 2013, with publication numbers remaining relatively stable at 16 documents each year. During the period from 2014 to 2017, the publication trend showed a moderate increase but stagnated in certain years. The number of publications rose from 23 in 2014 to 24 in 2015, then decreased again and stabilised at 21 in 2016 and 2017. This indicates that, during this period, research interest in Rivest's Cipher remained present but had not yet experienced a significant surge.

A more pronounced increase was observed from 2018 to 2019, when the number of publications rose sharply from 34 in 2018 to 41 in 2019. Although there was a decline in 2020 to 28 documents, the trend surged again significantly in 2021, reaching the highest number of publications throughout the observation period, with 46 documents.

This surge indicates growing attention from the scientific community toward Rivest's Cipher, likely influenced by the increasing need to evaluate cryptographic algorithm security in an increasingly complex digital era. After peaking in 2021, the number of publications declined again but remained at a relatively high level compared to the early period. From 2022 to 2025, the annual number of publications was 37, 33, 32, and 33 documents, respectively. This pattern indicates a phase of stabilization, where research on Rivest's Cipher remains a relevant topic, albeit without experiencing the dramatic surges seen previously. This publication trend reflects that research on Rivest's Cipher continues to develop, driven by information security needs and the evolution of cryptographic technologies. Despite annual fluctuations, the overall upward trend demonstrates that this topic remains highly relevant and appealing in modern cryptography research.

Document per year by source

This section presents the distribution of research publications on Rivest's Cipher by journal source over a specific period, providing an overview of each journal's contributions to the literature and the dynamics of publication over time, as illustrated in Figure 2.

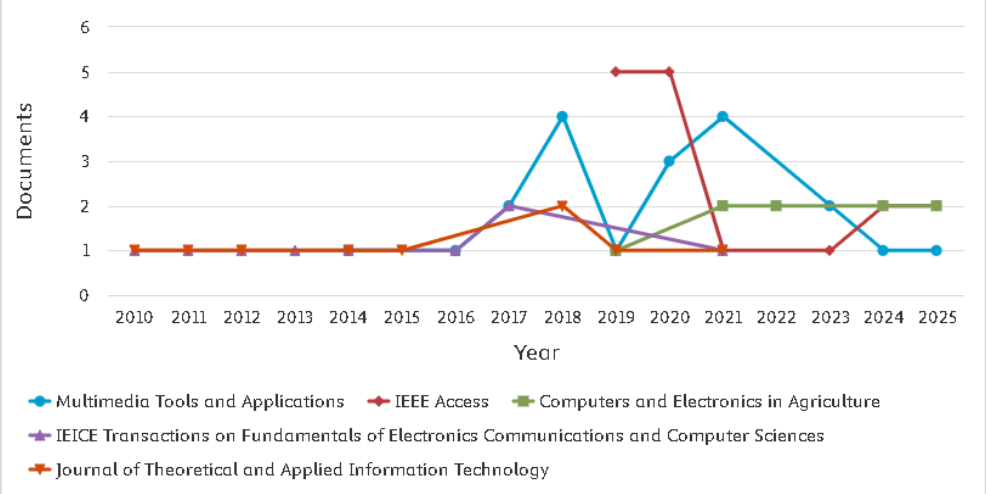

Figure 2 document per year by source
Source: Scopus, 2026

Based on Figure 2, the distribution of research publications on Rivest's Cipher by journal source shows that contributions come from several major journals with varying levels of productivity. Overall, the top five contributing journals are Multimedia Tools and Applications with a total of 20 documents, followed by IEEE Access with 16 documents, and three other journals, Computers and Electronics in Agriculture, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, and Journal of Theoretical and Applied Information Technology, each contributing 9 documents. Examining annual trends, Multimedia Tools and Applications demonstrates a relatively consistent contribution, with notable increases during certain periods, particularly between 2018 and 2021. During this period, the journal's publication output peaked, indicating growing attention to the application of Rivest's Cipher in multimedia and technology-based applications. Although there was a decline after 2021, this journal remained the largest contributor throughout the overall observation period.

Meanwhile, IEEE Access exhibits a rather interesting pattern, with a significant surge in publications in 2019 and 2020, reaching the highest number of documents compared to other years. This indicates that the journal served as an important platform for research publications on Rivest's Cipher, particularly during the period when this topic received increased global attention. However, following this period, the number of publications tended to decline before stabilizing at a lower level. The contributions from Computers and Electronics in Agriculture show a more limited but stable trend in recent years, particularly from 2021 to 2025. This suggests expanding Rivest's Cipher applications into interdisciplinary fields, including technology-based agriculture. On the other hand, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences and the Journal of Theoretical and Applied Information Technology show relatively consistent contributions, without significant surges, with publications distributed sporadically throughout the study period. The distribution of publications by journal source indicates that research on Rivest's Cipher is not concentrated in a single journal but is spread across multiple journals with diverse focuses. This reflects the multidisciplinary nature of cryptography research, in which Rivest's Cipher is discussed not only in theoretical contexts but also in practical applications across information technology and communication systems.

Document by author

This section presents the distribution of publications on Rivest's Cipher by individual author, illustrating the productivity levels and the significant role of key authors in the field's development, as shown in Figure 3.

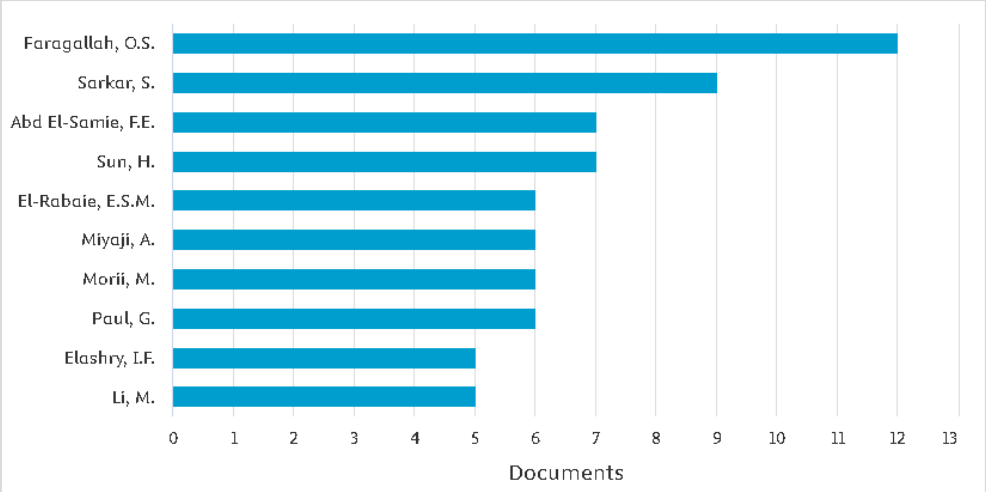

Figure 3 document by author
Source: Scopus, 2026

Figure 3 illustrates the distribution of research publications on Rivest's cipher across authors, highlighting variations in productivity among the main contributors. The author with the most publications is Faragallah, O.S., with 12 documents, making them the most dominant contributor in this field. The next position is held by Sarkar, S., with 9 documents, demonstrating a significant role in the development of literature on Rivest's Cipher. The group of moderately productive authors includes Abd El-Samie, F.E., and Sun, H., each of whom has produced 7 publications. Their contributions reflect active involvement in cryptography research, particularly in the development and analysis of Rivest's Cipher algorithms. Additionally, several authors have relatively balanced

publication counts, namely El-Rabaie, E.S.M., Miyaji, A., Morii, M., and Paul, G., each contributing 6 documents. The presence of this group indicates a fairly solid research community with consistent contributions.

On the other hand, Elashry, I.F. and Li, M. occupy the next positions, each with 5 publications. Although their numbers are lower than those of other authors on this list, their contributions remain significant in enriching studies of Rivest's Cipher. Overall, this distribution indicates that only one or two authors do not dominate research in this field, and that it involves a range of researchers with varying levels of productivity. These findings suggest that Rivest's Cipher research was developed through collaboration among multiple authors worldwide. The presence of several highly productive authors also reflects sustained interest and research focus in this area. Therefore, this author's contribution mapping provides an important overview of the key actors driving the advancement of knowledge about Rivest's Cipher.

Document by affiliation

This section presents the distribution of scientific publications by institutional affiliation that contributed to research on Rivest's Cipher, aiming to identify the most active institutions and to understand patterns of institutional contributions in the development of modern cryptography studies, as shown in Figure 4.

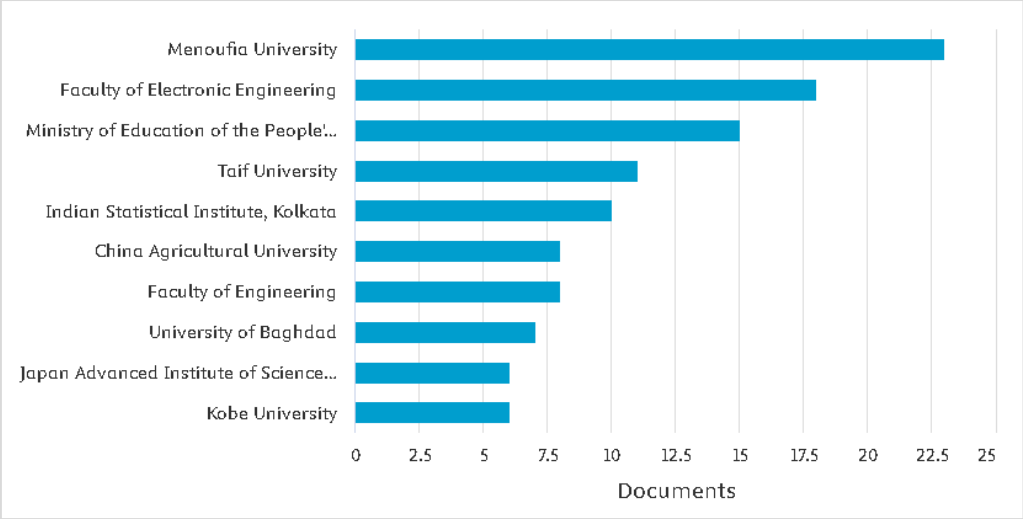

Figure 4 document by affiliation
Source: Scopus, 2026

Based on the data in Figure 4, it is evident that research contributions come from a variety of institutions across different countries, indicating that studies on this cryptographic algorithm have a global scope and involve diverse academic research centres and educational institutions. The institution with the highest number of publications is Menoufia University, with 23 publications, demonstrating a strong research focus on cryptography, particularly Rivest's Cipher. The second position is held by the Faculty of Electronic Engineering, with 18 publications, also reflecting a significant role in advancing technical research in this area. Following this the Ministry of Education of the People's Republic of China ranks third with 15 documents, indicating active involvement of a governmental institution in supporting cryptography research.

Further contributions come from Taif University (11 publications) and the Indian Statistical Institute, Kolkata (10 publications). Both institutions demonstrate

consistency in producing related research, thereby reinforcing their positions as active research centres in mathematics and computer science. Additionally, China Agricultural University and the Faculty of Engineering each contributed 8 publications, reflecting that cryptography research is also developing in institutions with broader focuses, including agriculture and general engineering. Meanwhile, the University of Baghdad contributed 7 documents, followed by the Japan Advanced Institute of Science and Technology and Kobe University, each producing 6 publications. Although these numbers are lower than those of other institutions, they still demonstrate ongoing involvement in Rivest's Cipher research. This distribution indicates that research on Rivest's Cipher is not concentrated in a single region but is spread across multiple international institutions. Nonetheless, there is a tendency for institutions with backgrounds in engineering and computer science to dominate publication contributions. This emphasises that Rivest's Cipher research remains closely linked to technical disciplines, while also highlighting opportunities for cross-institutional collaboration to expand the scope and impact of future studies.

Document by country

This section presents the distribution of scientific publications by authors' countries or regions, aiming to identify geographic contributions and understand patterns of dominance and dissemination of research on Rivest's Cipher at the global level, as shown in Figure 5.

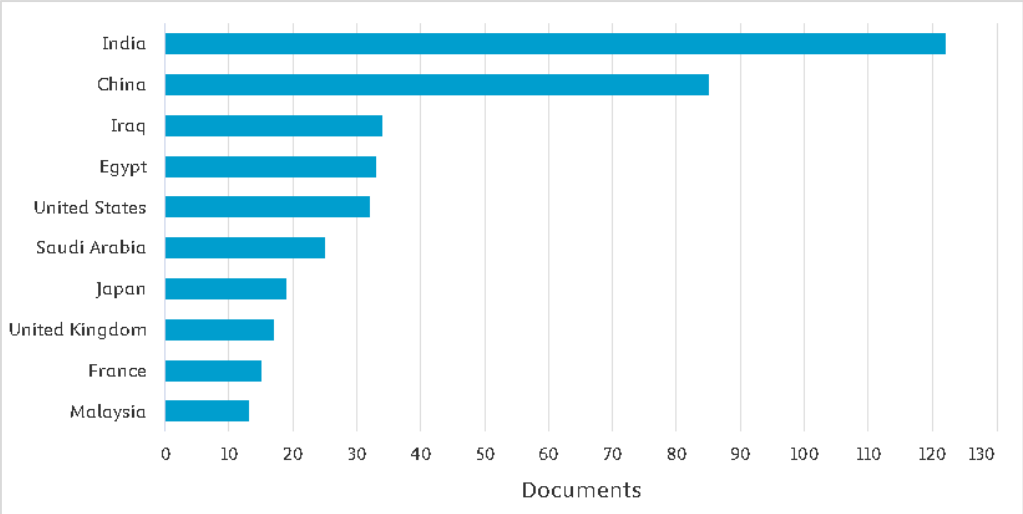

Figure 5 document by country
Source: Scopus, 2026

Based on the data in Figure 5, research contributions are distributed across various countries, reflecting the high global interest in the development and analysis of cryptographic algorithms in a modern context. The country with the most publications is India, with 122 documents. This dominance indicates that India has a highly intensive research program in cryptography, particularly in Rivest's Cipher. China ranks second with 85 publications, demonstrating a significant role in advancing research in information security. The significant contributions from these two countries suggest that the Asian region is a major hub for research on this topic. At the mid-level, several countries show relatively balanced contributions, including Iraq (34 documents), Egypt (33 documents), and the United States (32 documents). These countries demonstrate

active involvement in Rivest's Cipher research, although their publication numbers are lower than those of India and China. The presence of the United States in this group also underscores that countries with a strong research tradition continue to play a role in cryptography, even if their contributions in this dataset are not dominant.

Furthermore, Saudi Arabia contributed 25 publications, followed by Japan with 19, the United Kingdom with 17, France with 15, and Malaysia with 13. Although their publication numbers are lower, these countries still make important contributions by enriching the literature and broadening research perspectives on Rivest's Cipher. This distribution indicates that research on Rivest's Cipher is widely distributed, with strong dominance from Asian countries, particularly India and China. This suggests a shift in the global centre of research activity toward this region. Moreover, the diversity of countries involved offers opportunities for broader international collaboration, which can further drive innovation and development in modern cryptography.

Document by citations

This section presents a list of the most highly cited documents in research on Rivest's Cipher and modern cryptography (Table 2). Citation analysis identifies scientific works that have had a significant impact and serve as key references in the development of research in this field.

Table 2 document by citations

Nu	Document title	Authors (Year)	Source	Citations
1	Evaluating the performance of symmetric encryption algorithms	Elminaam et al. (2010)	International Journal of Network Security, 10(3), pp. 213–219	197
2	A review and comparative analysis of various encryption algorithms	Bhanot & Hans (2015)	International Journal of Security and Its Applications, 9(4), pp. 289–306	181
3	A resource-efficient encryption algorithm for multimedia big data	Aljawarneh et al. (2017)	Multimedia Tools and Applications, 76(21), pp. 22703–22724	165
4	A joint encryption/watermarking system for verifying the reliability of medical images	Bouslimi et al. (2012)	IEEE Transactions on Information Technology in Biomedicine, 16(5), pp. 891–899, 6236171	125
5	A multithreaded programming approach for multimedia big data: Encryption system	Aljawarneh et al. (2018)	Multimedia Tools and Applications, 77(9), pp. 10997–11016	111
6	Symmetric encryption algorithms: Review and evaluation study	Alenezi et al. (2020)	International Journal of Communication Networks and Information Security, 12(2), pp. 256–272	99
7	Efficient Security and Authentication for Edge-Based Internet of Medical Things	Parah et al. (2021)	IEEE Internet of Things Journal, 8(21), pp. 15652–15662	96
8	PRISEC: Comparison of symmetric key algorithms for IoT devices	Saraiva et al. (2019)	Sensors Switzerland, 19(19), 4312	85
9	A unified method for finding impossible differentials of block cipher structures	Luo et al. (2014)	Information Sciences, 263, pp. 211–220	80
10	Information hiding in edges: A high capacity information hiding	Parah et al. (2018)	Multimedia Tools and Applications, 77(1), pp.	79

Nu	Document title	Authors (Year)	Source	Citations
	technique using hybrid edge detection		185–207	
11	Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography	Atiewi et al. (2020)	IEEE Access, 8, pp. 113498–113511, 9118946	77
12	Quantum cryptanalysis on some generalized Feistel schemes	Dong et al. (2019)	Science China Information Sciences, 62(2), 22501	76
13	Triathlon of lightweight block ciphers for the Internet of things	Dinu et al. (2019)	Journal of Cryptographic Engineering, 9(3), pp. 283–302	75
14	Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications	Loan et al. (2017)	Journal of Biomedical Informatics, 73, pp. 125–136	73
15	Privacy Protection Based on Stream Cipher for Spatiotemporal Data in IoT	Liu et al. (2020)	IEEE Internet of Things Journal, 7(9), pp. 7928–7940, 9079473	69
16	A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images	Bouslimi, Coatrieux, & Roux (2012)	Computer Methods and Programs in Biomedicine, 106(1), pp. 47–54	68
17	HEVC Selective Encryption Using RC6 Block Cipher Technique	Sallam et al. (2018)	IEEE Transactions on Multimedia, 20(7), pp. 1636–1644 2	67
18	Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems	Mousavi et al. (2021a)	Journal of Ambient Intelligence and Humanized Computing, 12(2), pp. 2033–2051	65
19	Chlorophyll content estimation based on cascade spectral optimizations of interval and wavelength characteristics	Song et al. (2021)	Computers and Electronics in Agriculture, 189, 106413	61
20	Graspan: A single-machine disk-based graph system for interprocedural static analyses of large-scale systems code	Wang et al. (2017)	ACM SIGPLAN Notices, 52(4), pp. 389–404	60

Source: Scopus, 2026

Based on Table 2, it can be observed that highly cited publications generally focus on the evaluation, comparison, and application of encryption algorithms across contexts such as network security, multimedia, and the Internet of Things (IoT). The most highly cited document is the study by Elminaam et al. (2010), titled "Evaluating the Performance of Symmetric Encryption Algorithms", with a total of 197 citations. This study emphasizes the importance of evaluating the performance of various symmetric encryption algorithms, thereby providing a foundation for subsequent research. The second-highest cited work is by Bhanot & Hans (2015), with 181 citations, for the article "A Review and Comparative Analysis of Various Encryption Algorithms", reflecting strong interest in comparative studies to understand the strengths and weaknesses of different cryptographic algorithms. Following this, the study by Aljawarneh et al. (2017)

received 165 citations, highlighting the development of efficient encryption algorithms for multimedia big data. This is followed by Bouslimi et al. (2012), with 125 citations, which examined hybrid encryption and watermarking systems for verifying the reliability of medical images. The high citation counts of these studies indicate that integrating cryptography into practical applications, such as image processing and big data, is a significant focus in the literature.

In the mid-citation group, several studies focus on IoT, medical data security, and lightweight cryptography. For example, the studies by Parah et al. (2021) and Saraiva et al. (2019) highlight the importance of efficiency and security in IoT devices. Additionally, the research by Dinu et al. (2019) on lightweight block cyphers reflects the growing demand for resource-efficient algorithms that maintain strong security. On the other hand, some studies contribute to the theoretical aspects of cryptography, such as Luo et al. (2014), which discusses differential cryptanalysis, and Dong et al. (2019), which examines quantum cryptanalysis. The presence of these topics indicates that, alongside practical applications, the development of foundational cryptographic theory remains a critical focus in research. This citation distribution suggests that review, comparative, and application-oriented studies tend to have a greater impact within the scientific community. Furthermore, research trends are increasingly oriented toward integrating cryptography with emerging technologies such as IoT, big data, and digital health systems. This indicates that the relevance of Rivest's Cipher and other cryptographic algorithms continues to evolve in line with security needs across various modern technological domains.

Author collaboration network

This section presents the author collaboration network in research related to Rivest's Cipher, as shown in Figure 6. The network visualization illustrates the collaborative relationships among researchers based on co-authored publications, with each node representing an author and the connecting lines indicating collaborations on scientific work. Different colors represent the groups or clusters of collaboration formed within the network.

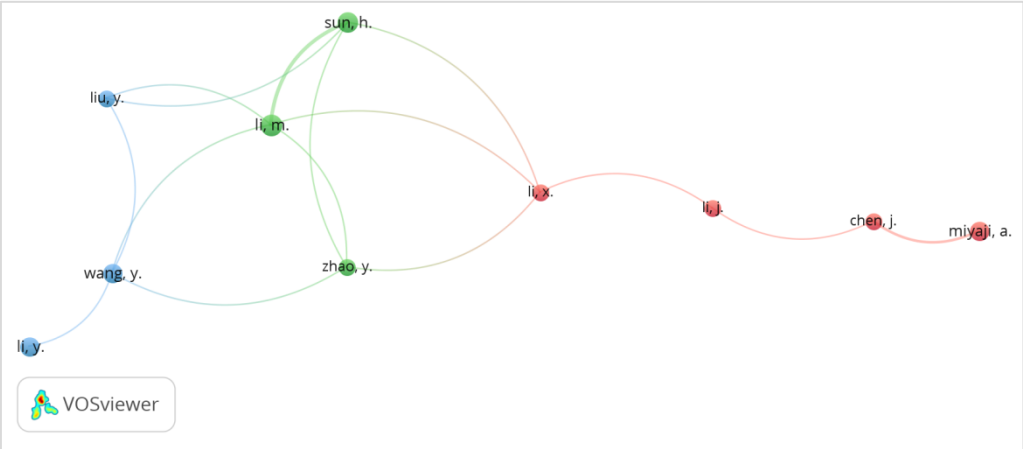

Figure 6 author collaboration network
Source: VOSviewer, 2026

Based on the visualization in Figure 6, the collaboration network appears to be divided into several small clusters with relatively limited interconnections between them. This indicates that research collaboration on Rivest's Cipher remains fragmented,

with most researchers working in small, separate groups. For instance, one cluster connects authors such as Wang Y. and Zhao Y., while another cluster links Li X., Li J., Chen J., and Miyaji A. The connectivity within these clusters demonstrates relatively intensive collaboration within each group. However, the connections between clusters appear weak, suggesting that cross-group or cross-institutional collaboration is still limited. Differences may influence this situation in research focus, geographic location, or institutional affiliation. As a result, the exchange of ideas and integration of knowledge among research groups has not yet occurred optimally.

Furthermore, there is no single author who dominantly serves as a central hub within the collaboration network. This indicates that the distribution of author contributions is relatively balanced, with no single figure connecting the majority of the network. Nevertheless, some authors appear to play a more active role within specific clusters, suggesting leadership within their respective research groups. This collaboration pattern suggests that research on Rivest's Cipher still has substantial potential to enhance broader, more integrated collaboration among researchers and across institutions and countries. Increasing cross-cluster collaboration is expected to enrich research perspectives, accelerate innovation, and yield more significant scientific contributions in modern cryptography.

Collaborative network between countries

This section presents the country-level collaboration network for research on Rivest's Cipher (Figure 7). Each node on the map represents a country, with the node size indicating the level of publication contribution. The connecting lines between nodes reflect collaborative relationships; thicker lines denote stronger collaboration between countries. Additionally, different colors represent clusters or groups of collaboration formed based on the closeness of research relationships.

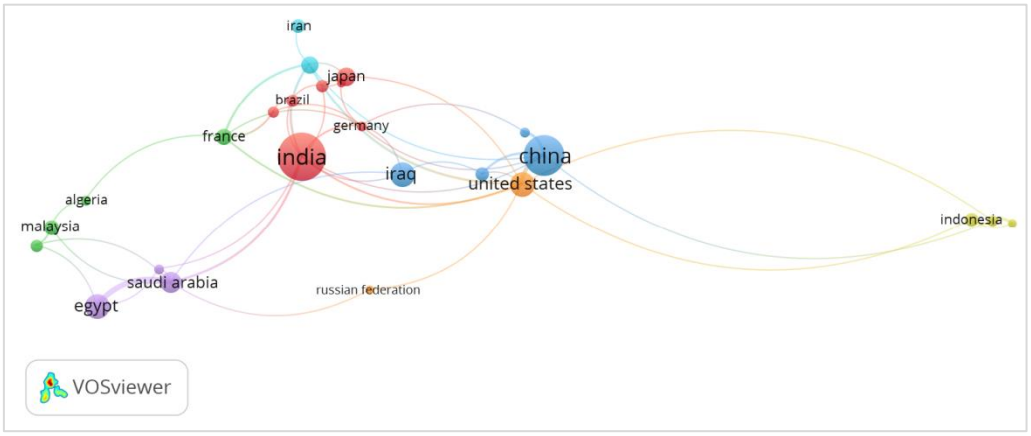

Figure 7 collaborative network between countries
Source: VOSviewer, 2026

Based on the visualization in Figure 7, India appears as one of the main hubs of collaboration, with a relatively large node size and extensive connections to various other countries. India maintains strong collaborative relationships with several countries, including China, the United States, Germany, Japan, and Brazil. This indicates that India plays a crucial role in the global research network on Rivest's Cipher, both as a major contributor and as a connector between countries in the exchange of scientific knowledge. China and the United States also emerge as dominant actors within this

network. Both have sizable nodes and occupy strategic positions connecting multiple countries, including Iraq and Indonesia. The connectivity between China and the United States demonstrates intensive collaboration in cryptography research, particularly concerning Rivest's algorithms. Additionally, China's connection with Indonesia indicates cross-regional cooperation that extends the reach of research into Southeast Asia.

On the other hand, there are several smaller yet significant regional clusters. For example, the cluster involving Egypt, Saudi Arabia, and Malaysia demonstrates relatively close collaboration within the Middle East and surrounding regions. Countries such as France and Algeria also appear connected within a more limited network, yet they contribute to enriching the diversity of global research. This map shows that research collaboration on Rivest's Cipher is global, with countries at varying levels of participation. Major countries like India, China, and the United States serve as central hubs, while other nations act as supporting or collaborative partners. This pattern indicates that advances in cryptography do not rely solely on a single region but result from broad international interaction and cooperation.

Research keyword network

This section presents the keyword network, illustrating the relationships among research topics in studies on Rivest's Cipher and modern cryptography (Figure 8). In this visualization, each node represents a keyword, with the node size indicating its frequency of occurrence in publications. The connecting lines between nodes reflect the co-occurrence or association of keywords, while different colors represent clusters of research topics that have formed.

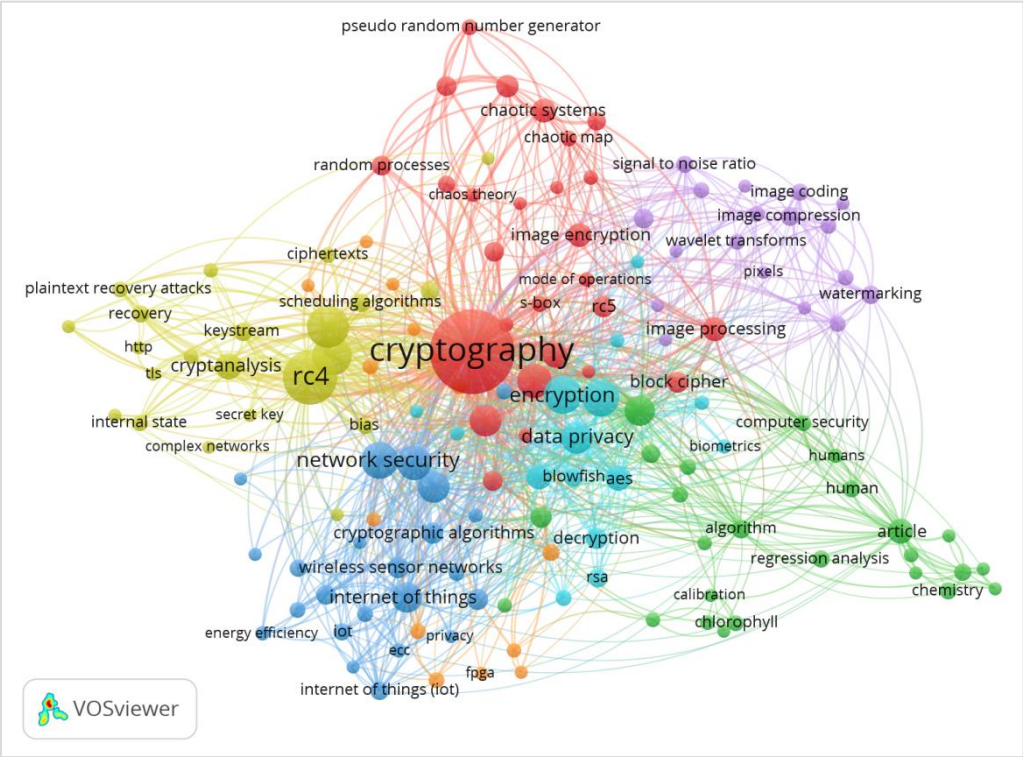

Figure 8 research keyword network
Source: VOSviewer, 2026

Based on Figure 8, the keyword cryptography appears as the central node, with the largest size and extensive connections. This indicates that cryptography serves as the core theme linking various other research topics. Surrounding this central node are important keywords such as encryption, data privacy, and network security, reflecting a research focus on data protection and information system security. The strong interconnections among these keywords demonstrate the integration of cryptographic theory with its implementation in various digital security systems. Furthermore, the keyword RC4 also emerges as a dominant topic, closely associated with terms such as cryptanalysis, keystream, bias, and plaintext recovery attacks. This indicates that research on RC4 not only focuses on its implementation but also on analyzing its vulnerabilities and potential attacks. The presence of keywords such as TLS and HTTP further reinforces the view that RC4 studies are often linked to its use in network communication protocols.

Another prominent cluster relates to the application of cryptography in image and signal processing, as indicated by keywords such as image encryption, image processing, image compression, wavelet transforms, and watermarking. This cluster illustrates the development of research integrating cryptographic techniques with the multimedia domain, particularly in securing visual data. Additionally, there is a cluster associated with mathematical approaches and dynamic systems, including chaotic systems, chaos theory, and pseudo-random number generators, reflecting the exploration of alternative methods in the development of encryption algorithms. Another cluster focuses on the application of cryptography in modern technologies such as the Internet of Things (IoT), wireless sensor networks, and energy efficiency, indicating a growing research emphasis on security challenges in resource-constrained environments. Meanwhile, the presence of keywords such as biometrics, algorithm, and even regression analysis highlights the expanding interdisciplinary nature of cryptography research. This keyword network demonstrates that studies on Rivest's Cipher have evolved in multiple directions, ranging from the security analysis of classical algorithms to integration with modern technologies and interdisciplinary approaches. The pattern suggests that cryptography is no longer an isolated field but has become a foundational component across diverse and rapidly evolving technological domains.

Research keyword network by color gradation

This section presents a research keyword network with a color gradient that depicts the temporal evolution of topics. Figure 9 shows that blue represents keywords that emerged earlier (around 2016), while green to yellow indicates more recent and evolving topics up to approximately 2022. Thus, this map not only illustrates the relationships among topics but also highlights the dynamic evolution of cryptography research, particularly in relation to Rivest's Cipher. The keyword cryptography remains the central node in the network; however, most surrounding nodes are dominated by green, indicating that research in this area has continued to develop actively in recent years. In the early phase (blue), research topics tended to focus on fundamental aspects such as cryptanalysis, keystreams, internal state, and analyses of algorithms such as RC4. This indicates that research during the initial period emphasized evaluating security and understanding the structure of classical cryptographic algorithms.

Over time, research has shifted toward more applied and integrated areas, as evidenced by the emergence of green-coloured keywords such as network security, encryption, data privacy, and wireless sensor networks. These topics reflect growing

attention to the implementation of cryptography within network systems and the protection of data in increasingly complex digital environments. Additionally, the appearance of the keyword "Internet of Things" (IoT) highlights the expanding use of cryptography in resource-constrained connected devices. In the more recent period (represented by yellow), more specific and interdisciplinary topics have emerged, including image compression, image coding, wavelet transforms, and regression analysis. This indicates that cryptography research has broadened into diverse fields, including image processing, data analysis, and other scientific domains such as chemistry.

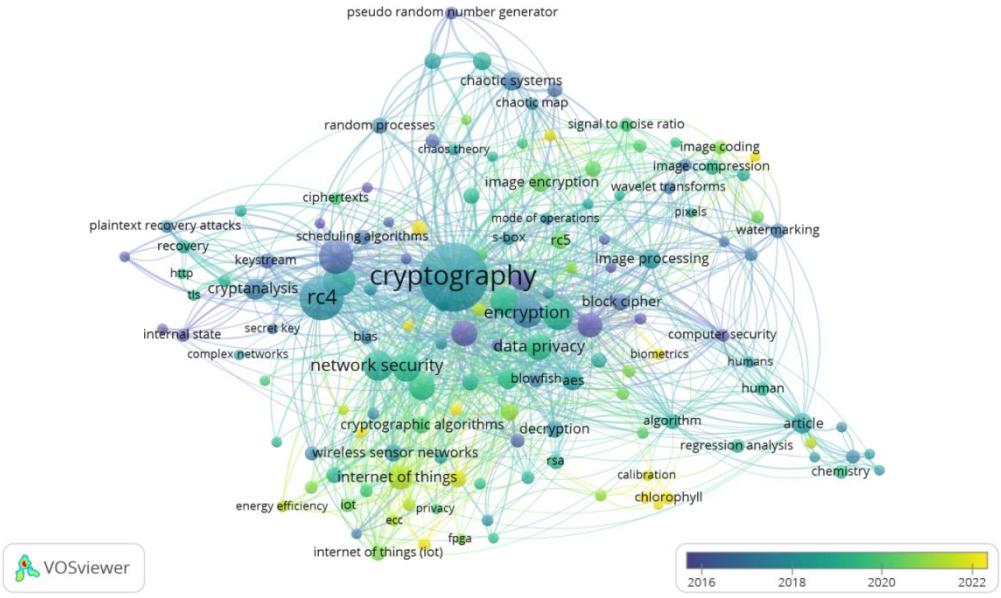

Figure 9 research keyword network by color gradation
Source: VOSviewer, 2026

Additionally, topics such as energy efficiency have emerged, reflecting growing attention to computational efficiency in the implementation of cryptographic algorithms, particularly on energy-constrained devices. This visualization demonstrates a shift in research trends from primarily theoretical approaches to broader, more contextually grounded applications. This evolution illustrates how cryptography, including Rivest's Cipher, continues to adapt to the demands of modern technology. Furthermore, the emergence of new interdisciplinary topics offers potential avenues for future research to address upcoming security challenges.

Research keyword density

This section presents a keyword density analysis to identify the primary research focus, the interconnections among topics, and the evolution of research themes in studies of Rivest's Cipher within modern cryptography. The keyword density visualization in Figure 10 shows the distribution of keyword occurrences in research on Rivest's Cypher during the observation period. Areas in bright yellow indicate keywords with high frequency and strong interconnections, whereas green to blue areas represent lower density. The keywords cryptography and encryption are located at the center of the map with the highest intensity, indicating that these two concepts constitute the core focus of the analyzed research. Additionally, the keyword RC4 also appears with high density

near the center, highlighting that this algorithm is a dominant focus in Rivest's Cipher studies compared to other variants. Surrounding the centre, several closely related keywords are observed, including network security, data privacy, and cryptanalysis. This indicates that research on Rivest's Cipher primarily focuses on network security, data protection, and the analysis of algorithmic vulnerabilities. The presence of terms like bias, keystream, and plaintext-recovery attacks further reinforces the idea that a significant portion of studies focus on security evaluation, particularly in identifying weaknesses in algorithms such as RC4.

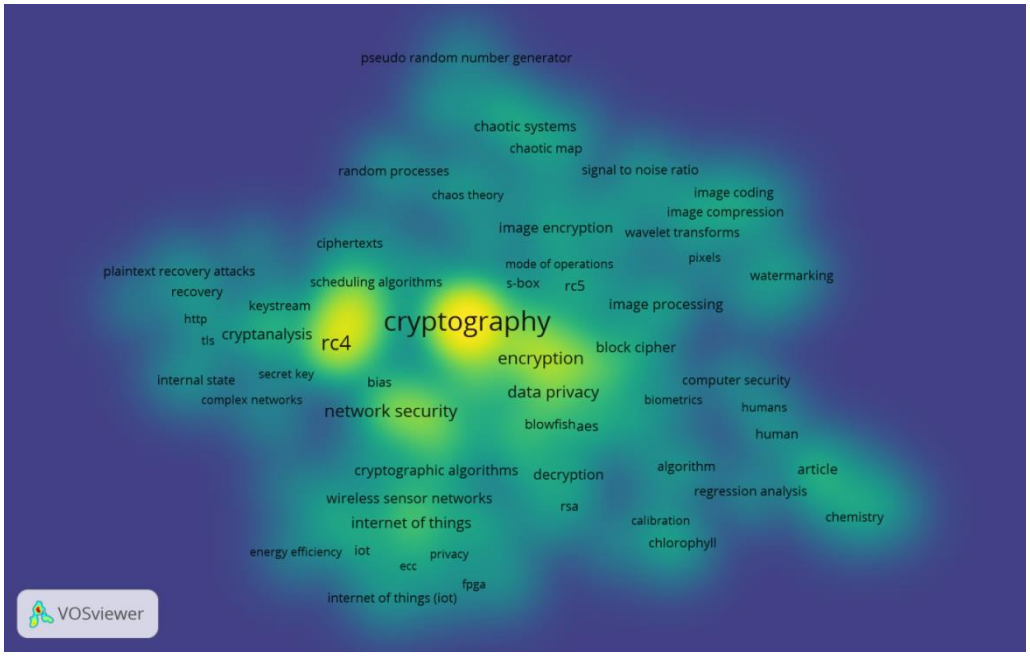

Figure 10 research keyword density
Source: VOSviewer, 2026

Furthermore, the map also highlights connections with broader application domains, such as image encryption, image processing, and watermarking. The presence of these keywords indicates that cryptographic algorithms are used not only for data communication but also for the processing and protection of digital media. Meanwhile, the emergence of topics such as the Internet of Things (IoT) and wireless sensor networks reflects a trend toward integrating Rivest's Cipher into modern network-based systems that demand both high efficiency and robust security. Interestingly, there are also keywords associated with alternative and interdisciplinary approaches, such as chaotic systems, chaos theory, and pseudo-random number generators. This suggests that research is beginning to focus on developing new encryption methods or enhancing existing algorithms by leveraging mathematical concepts and dynamic systems. Moreover, the appearance of terms like machine learning (although not dominant) and regression analysis indicates an exploration of analytical methods for evaluating cryptographic algorithm performance. These visualization results suggest that research on Rivest's Cipher remains centred on fundamental aspects of cryptography and security, but has expanded into diverse application domains and methodological approaches. The distribution of keyword density reflects a diversification of research topics while simultaneously opening opportunities for further exploration, particularly in integrating emerging technologies and enhancing algorithmic security.

Publication trends

The publication trends of research on Rivest's Cipher during the period 2010–2025 exhibit a clear dynamic, characterized by an initial fluctuating phase, a phase of significant growth, and a stabilization phase. In the early period (2010–2013), the number of publications was relatively low and unstable, with a decline in 2011 followed by a gradual increase. This pattern can be associated with the context at the time, in which algorithms such as RC4 were still widely used in security protocols (e.g., SSL/TLS and WEP), leading research to focus primarily on basic implementations and evaluations. However, during this period, studies also began to identify fundamental weaknesses in RC4, such as biases in the keystream and potential cryptanalytic attacks.

Entering the period 2014–2017, the publication trend showed a moderate but relatively stagnant increase. This aligned with the growing attention to serious security issues with RC4, including the discovery of various practical attacks, such as the "Bar Mitzvah attack," and exploits targeting the TLS protocol. In 2014–2015, several major organizations began recommending discontinuing RC4 due to its vulnerabilities, and the Internet Engineering Task Force (IETF) officially prohibited its use in TLS in 2015. This situation spurred increased research on security analysis while shifting researchers' attention toward more secure algorithms.

A significant surge in publications occurred during 2018–2021, peaking in 2021. This increase was closely linked to the rapid development of digital technologies, such as the Internet of Things (IoT), big data, and cloud-based security systems, which demand efficient and lightweight cryptographic solutions. In this context, Rivest's Ciphers, particularly RC4, RC5, and RC6, remained important subjects of research, whether for reevaluation, modification, or comparison with modern algorithms. Moreover, the growing complexity of cybersecurity threats spurred further investigations into the weaknesses of classical algorithms as a basis for developing more secure systems. In other words, this surge was not due to increased direct use of RC4, but rather to the growing need to reassess legacy algorithms in light of new threats.

However, after reaching its peak, the publication trend during 2022–2025 entered a stabilization phase, with a slight decline. This indicates that, although the topic of Rivest's Ciphers remains relevant, research focus has gradually shifted toward modern cryptographic algorithms such as AES and newer protocols like TLS 1.3, which offer higher security and more robust designs. Additionally, many contemporary systems have abandoned RC4 due to its well-documented vulnerabilities, with major technology companies progressively removing support for it from their platforms. The fact that RC4 has been prohibited in numerous security standards underscores that its current use is primarily historical and analytical rather than practical. Overall, the publication trend suggests that research on Rivest's Ciphers has not declined entirely but has shifted in focus. Whereas early studies were oriented toward implementation and usage, current research emphasizes security analysis, algorithm comparison, and the development of variants or novel approaches. Thus, Rivest's Ciphers remain relevant in the scientific literature, particularly as a baseline or historical reference in cryptography, while their practical role is increasingly supplanted by modern, more secure, and efficient algorithms.

Distribution of scientific contributions

The distribution of scientific contributions in research on Rivest's Ciphers exhibits an interesting pattern across authors, institutions, and countries. From an individual perspective, several authors stand out as primary contributors. The most

prolific author in this dataset is Omar S. Faragallah, with 12 publications, followed by Subhamoy Sarkar with 9. Additionally, authors such as Fathi E. Abd El-Samie and Hua Sun have made significant contributions, each with 7 publications. Other author groups, including Eiichiro Miyaji and Goutam Paul, have also strengthened the research ecosystem through consistent contributions. This pattern indicates that although no single author dominates as the central hub of the global network, a core group of researchers plays a crucial role in sustaining research continuity in this field.

From an institutional perspective, scientific contributions are dominated by educational and research institutions with a strong focus on engineering and computer science. Menoufia University ranks first with 23 publications, followed by the Faculty of Electronic Engineering at Menoufia University with 18 publications. In addition, the Ministry of Education of the People's Republic of China has played a significant role with 15 publications, reflecting government support for cryptography research. Other institutions, such as Taif University and the Indian Statistical Institute, Kolkata, have also contributed consistently. The dominance of institutions from Asia and the Middle East indicates that cryptography research is no longer concentrated in Western countries but has spread to regions with growing research capacity.

At the country level, contributions are strongly dominated by developing countries, particularly in Asia. India emerges as the largest contributor, with 122 publications, followed by China with 85. Other countries, such as Iraq, Egypt, and the United States, show relatively balanced contributions at a moderate level. Meanwhile, developed countries like the United Kingdom and France continue to contribute, although they do not dominate in terms of publication numbers. This pattern indicates a shift in the center of global research activity from developed to developing countries, particularly in Asia.

The dominance of developing countries in this research can be interpreted through several factors. First, the increasing research capacity and the growing number of higher education institutions in countries such as India and China have significantly boosted scientific publication output. Second, the high demand for digital security, driven by the expansion of the digital economy and the large population of internet users in these countries, has further stimulated research in cryptography. Third, topics like Rivest's Ciphers are relatively accessible for academic research due to their open nature and long-standing study, making them a popular choice for researchers in developing countries seeking to publish. In contrast, developed countries tend to focus more on developing new cryptographic algorithms and cutting-edge industry standards, resulting in comparatively smaller contributions to more specific topics such as Rivest's Ciphers.

This distribution of scientific contributions indicates that research on Rivest's Ciphers is global and inclusive, with broad participation from various countries and institutions. However, the dominance of developing countries, particularly in Asia, is an important indicator that the cryptography research landscape is transforming, both geographically and in research focus. This shift opens opportunities for broader international collaboration and enriches perspectives in the future development of cryptographic science.

Main research topic or theme

Based on the keyword analysis, particularly through keyword density visualization, it can be identified that research themes related to Rivest's Ciphers are dominated by several core topics that are strongly interconnected. The keywords

cryptography and encryption appear as the central nodes with the highest density, indicating that the entire research landscape is rooted in the fundamental concept of information security. These two topics not only serve as a theoretical foundation but also act as connectors for various emerging subthemes. The high frequency of these keywords suggests that research remains strongly focused on the development, implementation, and evaluation of encryption techniques across diverse digital system contexts.

Furthermore, the RC4 algorithm appears to be one of the most dominant themes within Rivest's Cipher cluster. The high density of this keyword indicates that RC4 remains a primary subject of study compared to other variants such as RC5 or RC6. However, unlike the initial focus on implementation, current research on RC4 is increasingly focused on analysing its vulnerabilities. This is reflected in its association with subthemes such as cryptanalysis, keystream bias, and plaintext recovery attacks. The presence of these keywords underscores that most studies aim to identify security gaps and assess the algorithm's resilience against various attack types. Thus, RC4 is now more often used as a case study to understand the vulnerabilities of classical cryptographic algorithms.

Around these core themes, several important subthemes indicate the practical applications of cryptography research. Among the most prominent are network security and data privacy, suggesting that cryptography is widely used to protect digital communications and data. Associations with terms such as TLS, HTTP, and other network systems demonstrate that the research is not merely theoretical but also highly relevant to modern communication infrastructures. Furthermore, the emergence of keywords such as wireless sensor networks and the Internet of Things (IoT) indicates that research attention is increasingly shifting toward resource-constrained connected environments, which require algorithms that are both efficient and secure.

Another significant subtheme is the integration of cryptography with multimedia, as indicated by keywords such as image encryption, image processing, image compression, and watermarking. This cluster illustrates that research is not limited to text or numerical data but also encompasses the protection of visual data, such as digital images and videos. This focus is particularly relevant in applications like telemedicine, media security, and digital content distribution. The use of techniques such as wavelet transforms and image compression reflects a more complex technical approach that integrates cryptography with signal processing.

Interestingly, the analysis also reveals the emergence of new interdisciplinary topics, which serve as important indicators of future research directions. Keywords such as chaotic systems, chaos theory, and pseudo-random number generators suggest exploring alternative methods based on dynamic systems to enhance algorithm security. Moreover, the presence of terms such as machine learning and regression analysis indicates integration with data-driven approaches to evaluate the performance and security of cryptographic algorithms. Additionally, connections to fields such as energy efficiency reflect attention to computational efficiency, particularly in resource-constrained devices.

The results of the keyword analysis indicate that research on Rivest's Ciphers has evolved from an initial theoretical focus to a more applied, interdisciplinary approach. Core themes such as cryptography, encryption, and RC4 remain the foundational pillars, yet they are surrounded by various subthemes that reflect the demands of modern technology. The emergence of new topics suggests that the field continues to adapt to technological advancements while also opening avenues for more innovative research,

particularly in integrating cryptography with intelligent systems, the Internet of Things (IoT), and complex data processing.

Collaboration patterns

The collaboration patterns in research on Rivest's Ciphers, as revealed by co-authorship analysis, show a relatively fragmented, dispersed network. Network visualization of authors shows that most collaborations occur within small clusters, which are strongly interconnected within each cluster but weakly connected between clusters. This indicates that inter-author collaboration remains largely confined to specific contexts, such as the same research group or nearby institutions. No single author serves as a central hub, suggesting a decentralized collaboration structure. This pattern reflects that research on Rivest's Ciphers progresses through parallel contributions from multiple small groups rather than through an integrated global collaboration network.

At the institutional level, a similar pattern is observed. Collaborations tend to occur within internal networks or between institutions that are geographically or academically proximate. Institutions previously identified as highly productive do not necessarily maintain extensive connections with other institutions globally. This suggests that, although active research hubs exist, inter-institutional collaborative relationships remain suboptimal. Such limitations may result from differences in research focus, funding constraints on international collaboration, or a lack of initiatives to establish cross-country research networks. Consequently, the institutional collaboration structure tends to be local or regional rather than global.

At the country level, there is evidence of broader collaboration, although it remains uneven. Countries with substantial contributions, such as India, China, and the United States, serve as important nodes within the international collaboration network. These three countries maintain connections with various other nations, positioning them as key connectors in the global network. For example, India demonstrates relatively extensive collaborative links with countries across different regions, while China and the United States also act as bridges between developed and developing countries. Nevertheless, not all countries exhibit the same level of connectivity; some are involved only in limited collaborations or occupy peripheral positions within the network.

The collaboration patterns in Rivest's Cipher research can be described as semi-global. Although international collaborations exist, the majority of research activities are still dominated by local collaborations or small clusters. The dispersed network structure, lacking a dominant central hub, indicates that strong global collaboration integration has yet to be achieved. On the other hand, the presence of certain countries as key connectors offers significant potential to expand the collaboration network in the future. The implications of this pattern suggest considerable opportunities to enhance cross-country and cross-institution collaborations. By strengthening connections between clusters and promoting more intensive international collaboration, research in this field can become more innovative and comprehensive. Furthermore, increased collaboration can help integrate diverse perspectives and expertise, leading to more robust cryptographic solutions that can address the continuously evolving challenges of digital security.

Research gaps and future opportunities

The bibliometric analysis reveals several clear research gaps in studies on Rivest's Ciphers. One of the main gaps is the dominance of research on the RC4 algorithm, while other variants such as RC5 and RC6 have received relatively little attention. This is evident from keyword density and publication frequency, which are heavily focused on RC4, particularly in the context of vulnerability analysis and cryptanalytic attacks. As a result, a comprehensive understanding of the potential, strengths, and limitations of other algorithms within Rivest's Cipher family remains underdeveloped. Notably, RC5 and RC6 possess distinct design characteristics and can offer alternative solutions in certain contexts, especially for systems that require high flexibility and efficiency.

The second gap lies in the limited integration with modern and interdisciplinary technologies. Although some keywords, such as the Internet of Things (IoT) and wireless sensor network, have begun to emerge, the integration of Rivest's Ciphers with advanced technologies, such as Artificial Intelligence (AI), blockchain, and edge computing systems, remains very limited. In the context of current technological developments, demand for adaptive, intelligent security systems is growing. However, research combining classical cryptographic algorithms with AI-based approaches, for instance, for adaptive attack detection or encryption optimization, remains scarce. Similarly, the potential applications of Rivest's Ciphers in blockchain and other decentralized ecosystems have not been fully explored.

Furthermore, there is a strong tendency for research to focus on vulnerability analysis (cryptanalysis) rather than on developing new solutions. This is evident from the dominance of keywords such as bias, keystream, and various types of attacks against RC4. While such studies are crucial for understanding the algorithm's security limits, the lack of research focused on improvement, modification, or algorithmic innovation indicates an imbalance in research direction. In other words, many studies stop at problem identification without advancing to the development of practical, implementable solutions.

Based on these gaps, several future research opportunities can be identified. First, further exploration of algorithms beyond RC4, particularly RC5 and RC6, is needed, considering performance, security, and their potential for adaptation to modern systems. Research can focus on developing new variants or optimizing algorithm parameters to enhance efficiency and resilience against attacks. Second, integration with modern technologies represents a highly promising area. For instance, AI can be applied to improve encryption security through attack pattern detection, or blockchain can be used to create transparent and decentralized security systems based on classical cryptographic algorithms.

Furthermore, opportunities exist to develop hybrid algorithms that combine Rivest's Ciphers with other approaches, such as chaotic systems or lightweight cryptography, to address the needs of resource-constrained devices in IoT environments. In addition, research can focus on aspects of energy efficiency and computational optimization, given the increasing number of devices reliant on low-power encryption systems. Interdisciplinary approaches that integrate cryptography with machine learning, data science, or biomedical engineering also have the potential to generate innovations relevant to future needs. Although research on Rivest’s Ciphers has progressed substantially, there remains significant room for further exploration. Existing gaps create opportunities for more innovative research, not only to deepen understanding of classical algorithms but also to adapt them to the evolving ecosystem

of modern technologies. By directing research toward integration, innovation, and practical applications, Rivest's Ciphers can continue to expand and strengthen contributions to modern cryptography.

Overall, the results of the bibliometric analysis of research on Rivest's Ciphers indicate that this field exhibits complex, evolving dynamics, despite shifts in focus over time. Regarding publication trends (RQ1), research has fluctuated, with an overall tendency to increase, peaking during certain periods and then stabilizing. This reflects that, although algorithms such as RC4 are no longer dominant in practice, research interest remains high, particularly in the context of security evaluation and the historical relevance of these algorithms in modern cryptography.

From the perspective of scientific contribution distribution (RQ2), research is dominated by authors, institutions, and countries from Asia and developing regions, with India and China as the primary contributors. These findings indicate a shift in the global research activity centre, away from developed countries. Meanwhile, the analysis of research topics (RQ3) reveals that the main themes remain focused on cryptography, encryption, and RC4, with emerging subthemes in cryptanalysis, network security, and applications such as image encryption and IoT. This indicates a transition from a primarily theoretical approach to broader, more interdisciplinary applications.

In terms of collaboration patterns (RQ4), the research exhibits a fragmented network, with collaborations still largely confined to small clusters, although indications of international collaboration are present. The absence of dominant actors serving as central connectors suggests that the integration of the global research network can still be enhanced. On the other hand, the analysis of research gaps (RQ5) reveals several underexplored areas, including studies on algorithms other than RC4, integration with modern technologies (e.g., AI, blockchain), and the development of more innovative solutions.

By synthesizing all these findings, it can be concluded that research on Rivest's Ciphers is currently in a transitional phase, shifting from an initial focus on algorithm implementation toward security analysis, comparative evaluation, and integration with modern technologies. Although its practical relevance has waned compared to newer cryptographic algorithms, it continues to play an important role in research as a conceptual foundation and a topic of scientific inquiry. Therefore, the dynamics of this field do not indicate a decline but rather a transformation that opens the way for more innovative, collaborative, and adaptive exploration to address future digital security challenges.

Conclusions

This study demonstrates that research on Rivest's Ciphers has undergone dynamic development during the period 2010–2025, with publication trends fluctuating but generally increasing, reaching a peak in 2021, followed by a stabilization phase. Key findings indicate that although the practical use of algorithms such as RC4 has declined, research interest remains high, particularly in security analysis (cryptanalysis), performance evaluation, and comparisons with modern cryptographic algorithms. In terms of scientific contribution, the research is dominated by Asian countries, particularly India and China. It is supported by several productive authors and institutions, reflecting a shift in the global research center toward developing countries.

From a thematic perspective, research remains centered on the fundamental concepts of cryptography and encryption, with RC4 as the primary focus. However, a

significant shift has occurred from a theoretical approach toward practical and interdisciplinary applications, such as in the fields of the Internet of Things (IoT), network security, and digital image processing. The observed collaboration patterns tend to be fragmented within small clusters, with limited cross-institutional and cross-country collaboration, although the beginnings of a global collaborative network are emerging. This study's implications include providing a comprehensive mapping of the research landscape on Rivest's Ciphers, encompassing publication trends, key actors, and the evolution of research topics. These findings can serve as a strategic reference for researchers to identify research directions, explore collaboration opportunities, and develop topics more relevant to modern technological needs. Furthermore, the study confirms that Rivest's Ciphers continue to hold an important role as a conceptual foundation in the development and evaluation of cryptographic algorithms.

This study has several limitations. First, the research focus remains predominantly on RC4, providing a less balanced view of other algorithms in the Rivest's Cipher family, such as RC5 and RC6. Second, the bibliometric approach employed emphasizes quantitative analysis, which does not fully capture the qualitative aspects of the research content. Additionally, the visualization of collaboration networks is not yet sufficient to explain the underlying factors behind limited collaboration among researchers. Given these limitations, future research is recommended to conduct more in-depth studies of RC5 and RC6, both in terms of security and performance, to provide a more balanced perspective. Future investigations could also focus on integrating Rivest's Ciphers with modern technologies, such as Artificial Intelligence, blockchain, and edge computing, as well as developing hybrid algorithms that are more adaptive and efficient. Finally, enhancing cross-country and cross-institutional collaboration should be encouraged to foster more innovative and impactful research that addresses the evolving challenges of digital security.

References

Abidi, A., Guyeux, C., & Machhout, M. (2020). Evaluation of Chaotic Properties of CBC Mode of Encryption Embedded with RC5 Block Cipher Algorithm. *Discontinuity, Nonlinearity, and Complexity*, *9*(4), 607–618. https://doi.org/10.5890/DNC.2020.12.013

Al-Badrei, H. H., & Alshawi, I. S. (2022). Secure Routing Protocol for WSNs Using Bacterial Foraging Optimization and Improved RC4. *Informatica (Slovenia)*, *46*(8), 1–10. https://doi.org/10.31449/inf.v46i8.4277

Al-Ta'i, Z. T. M., & Jumaa, E. (2019). Improved RC6 algorithm using two types of chaos maps. *International Journal of Engineering and Advanced Technology*, *9*(1), 2856–2860. https://doi.org/10.35940/ijeat.A1075.109119

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091836194&partnerID=40&md5=b649313845256223e335d7288e331d0f

Aljawarneh, S., Yassein, M. B., & Talafha, W. A. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, *76*(21), 22703–22724. https://doi.org/10.1007/s11042-016-4333-y

Aljawarneh, S., Yassein, M. B., & Talafha, W. A. (2018). A multithreaded programming approach for multimedia big data: Encryption system. *Multimedia Tools and Applications*, *77*(9), 10997–11016. https://doi.org/10.1007/s11042-017-4873-9

Almutairi, M., & Sheldon, F. T. (2025). IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics*, *14*(7), 1394. https://doi.org/10.3390/electronics14071394

Amin, M. (2010). Efficient modified RC5 based on chaos adapted to image encryption. *Journal of Electronic Imaging*, *19*(1), 013012. https://doi.org/10.1117/1.3360179

Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y. (2020). Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography. *IEEE Access*, *8*, 113498–113511. https://doi.org/10.1109/ACCESS.2020.3002815

Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, *9*(4), 289–306. https://doi.org/10.14257/ijsia.2015.9.4.27

Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. (2012). A joint encryption/watermarking system for verifying the reliability of medical images. *IEEE Transactions on Information Technology in Biomedicine*, *16*(5), 891–899. https://doi.org/10.1109/TITB.2012.2207730

Bouslimi, D., Coatrieux, G., & Roux, C. (2012). A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images. *Computer Methods and Programs in Biomedicine*, *106*(1), 47–54. https://doi.org/10.1016/j.cmpb.2011.09.015

Chalob, D. F., Hasan, R. H., & Abbas, F. N. (2025). Image Encryption Based on Chaotic Blocks Shuffling and RC4. *Baghdad Science Journal*, *22*(5), 1692–1702. https://doi.org/10.21123/bsj.2024.9781

Dara, M., & Manochehri, K. (2014). Using RC4 and AES Key Schedule to Generate Dynamic S-Box in AES. *Information Security Journal*, *23*(1–2), 1–9. https://doi.org/10.1080/19393555.2013.877541

Dinu, D., Corre, Y. Le, Khovratovich, D., Perrin, L., Großschädl, J., & Biryukov, A. (2019). Triathlon of lightweight block ciphers for the Internet of things. *Journal of Cryptographic Engineering*, *9*(3), 283–302. https://doi.org/10.1007/s13389-018-0193-x

Dong, X., Li, Z., & Wang, X. (2019). Quantum cryptanalysis on some generalized Feistel schemes. *Science China Information Sciences*, *62*(2). https://doi.org/10.1007/s11432-017-9436-7

Elashry, I. F., Faragallah, O. S., Abbas, A. M., El-Rabaie, S., & Abd El-Samie, F. E. (2012). A new method for encrypting images with few details using Rijndael and RC6 block ciphers in the Electronic Code Book mode. *Information Security Journal*, *21*(4), 193–205. https://doi.org/10.1080/19393555.2011.654319

Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2010). Evaluating the performance of symmetric encryption algorithms. *International Journal of Network Security*, *10*(3), 213–219. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84875361430&partnerID=40&md5=ea1816658f37959a52934b390de16185

Faisal, Z., & Abdul Ameer, E. H. (2020). Encryption Image by Using RC6 and Hybrid Chaotic Map. *Webology*, *17*(2), 189–199. https://doi.org/10.14704/WEB/V17I2/WEB17024

Faragallah, O. S., Sallam, A. I., & El-Sayed, H. S. (2022). Visual protection using rc5 selective encryption in telemedicine. *Intelligent Automation and Soft Computing*, *31*(1), 177–190. https://doi.org/10.32604/IASC.2022.019348

Farooq, A., Tariq, S., Amin, A., Qureshi, M. A., & Memon, K. H. (2024). Towards the design of new cryptographic algorithm and performance evaluation measures.

Multimedia Tools and Applications, *83*(4), 9709–9759. https://doi.org/10.1007/s11042-023-15673-7

Harish, J., Madhuri, S. J., Yaswanth, V., & Jagannadha Naidu, K. (2016). Low power ASIC implementation of RC5 algorithm. *International Journal of Chemical Sciences*, *14*, 725–732. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85008515649&partnerID=40&md5=fd34fa8b9ff9ab03eff582f2483e487b

Liu, L., Hu, X., Zhang, T., Zhu, S., & Li, M. (2011). A real-time 3D collision detection encryption algorithm based on improved RC5. *Advanced Science Letters*, *4*(8–10), 2708–2712. https://doi.org/10.1166/asl.2011.1599

Liu, T., Wang, Y., Li, Y., Tong, X., Qi, L., & Jiang, N. (2020). Privacy Protection Based on Stream Cipher for Spatiotemporal Data in IoT. *IEEE Internet of Things Journal*, *7*(9), 7928–7940. https://doi.org/10.1109/JIOT.2020.2990428

Loan, N. A., Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Bhat, G. M. (2017). Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications. *Journal of Biomedical Informatics*, *73*, 125–136. https://doi.org/10.1016/j.jbi.2017.08.002

Luo, Y., Lai, X., Wu, Z., & Gong, G. (2014). A unified method for finding impossible differentials of block cipher structures. *Information Sciences*, *263*, 211–220. https://doi.org/10.1016/j.ins.2013.08.051

Mahroos, S., Hazim, R., Oliwe, A. K., Mohammed, N., Saad, Y., Makki, A., & El Emary, I. (2024). Discovering Unknown Non-Consecutive Double Byte Biases in RC4 Stream Cipher Algorithm. *Journal of Cybersecurity and Information Management*, *13*(2), 75–83. https://doi.org/10.54216/JCIM.130206

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021a). Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 2033–2051. https://doi.org/10.1007/s12652-020-02303-5

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021b). Security of Internet of Things using RC4 and ECC Algorithms (Case Study: Smart Irrigation Systems). *Wireless Personal Communications*, *116*(3), 1713–1742. https://doi.org/10.1007/s11277-020-07758-5

Nagao, A., Ohigashi, T., Isobe, T., & Morii, M. (2014). Expandingweak-key space of RC4. *Journal of Information Processing*, *22*(2), 357–365. https://doi.org/10.2197/ipsjjip.22.357

Parah, S. A., Kaw, J. A., Bellavista, P., Loan, N. A., Bhat, G. M., Muhammad, K., & De Albuquerque, V. H. C. (2021). Efficient Security and Authentication for Edge-Based Internet of Medical Things. *IEEE Internet of Things Journal*, *8*(21), 15652–15662. https://doi.org/10.1109/JIOT.2020.3038009

Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A., & Bhat, G. M. (2018). Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. *Multimedia Tools and Applications*, *77*(1), 185–207. https://doi.org/10.1007/s11042-016-4253-x

Ramakrishna, D., & Shaik, M. A. (2025). A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges. *IEEE Access*, *13*, 11576–11593. https://doi.org/10.1109/ACCESS.2024.3518533

Rashmi, Chawla, V., Sehgal, R., & Nagpal, R. (2015). The RC7 encryption algorithm. *International Journal of Security and Its Applications*, *9*(5), 55–60. https://doi.org/10.14257/ijsia.2015.9.5.05

Sallam, A. I., Faragallah, O. S., & El-Rabaie, E. S. M. (2018). HEVC Selective Encryption

Using RC6 Block Cipher Technique. *IEEE Transactions on Multimedia*, *20*(7), 1636–1644. https://doi.org/10.1109/TMM.2017.2777470

Saraiva, D. A. F., Leithardt, V. R. Q., de Paula, D., Mendes, A. S., González, G. V., & Crocker, P. (2019). PRISEC: Comparison of symmetric key algorithms for IoT devices. *Sensors (Switzerland)*, *19*(19). https://doi.org/10.3390/s19194312

Shailaja, A., & Krishnamurthy, G. N. (2019). FPGA implementation and analysis of RC7 algorithm using reversible logic gates. *International Journal of Engineering and Advanced Technology*, *8*(6), 769–776. https://doi.org/10.35940/ijeat.F7993.088619

Shojaei, P., Gjorgievska, E. V., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers*, *13*(2), 41. https://doi.org/10.3390/computers13020041

Soboń, A., Kurkowski, M., & Stachowiak, S. (2020). Complete sat based cryptanalysis of rc5 cipher. *Journal of Information and Organizational Sciences*, *44*(2), 365–382. https://doi.org/10.31341/jios.44.2.10

Song, D., Gao, D., Sun, H., Qiao, L., Zhao, R., Tang, W., & Li, M. (2021). Chlorophyll content estimation based on cascade spectral optimizations of interval and wavelength characteristics. *Computers and Electronics in Agriculture*, *189*. https://doi.org/10.1016/j.compag.2021.106413

Suresh, S., Varghese, M., & D, A. (2015). An efficient and optimized RC5 image encryption algorithm for secured image transmission. *International Journal of Imaging and Robotics*, *15*(3), 116–125. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84930808125&partnerID=40&md5=7afb5136a6899391062ef57d452b350c

Wang, K., Hussain, A., Zuo, Z., Xu, G., & Amiri Sani, A. (2017). Graspan: A single-machine disk-based graph system for interprocedural static analyses of large-scale systems code. *ACM SIGPLAN Notices*, *52*(4), 389–404. https://doi.org/10.1145/3037697.3037744

Witwit, A. J. H., Fanfakh, A., & Idrees, A. K. (2025). A New Lightweight Encryption Method Based on the DNA-RC4 Substitution for Resource-Constrained IoT Devices. *Iraqi Journal for Computer Science and Mathematics*, *6*(3), 327–348. https://doi.org/10.52866/2788-7421.1287

Wong, K. K. H., Carter, G., & Dawson, E. (2010). An analysis of the RC4 family of stream ciphers against algebraic attacks. *Conferences in Research and Practice in Information Technology Series*, *105*, 67–74. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84871246097&partnerID=40&md5=5046f36ab6e72f35e74f90c2bc6348ec

Zaki, R. M., Wahab, H. B. A., & Mahdi, Z. S. (2025). RC6 Key Generation Method using Permutation Last Layer Algorithm. *Iraqi Journal of Science*, *66*(11), 5168–5190. https://doi.org/10.24996/ijs.2025.66.11.38

Zhang, J., Liu, H., & Ni, L. (2020). A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR. *IEEE Access*, *8*, 38995–39012. https://doi.org/10.1109/ACCESS.2020.2975208