Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 959–972
DOI : 10.47974/JDMSC-2236

An exploratory analysis of the evolution and trends of code-based cryptography

Ritu Redhu *
Ekta Narwal †
Department of Mathematics
M. D. University
Rohtak 124001
Haryana
India

Abstract

Code-based cryptography has emerged as a promising paradigm in cryptographic research, offering robust security foundations against quantum computing threats. This bibliometric analysis provides a comprehensive overview of code-based cryptography scholarly contributions and trends using the Scopus's extensive database. The relevant publications, including articles and conference papers are extracted to understand the evolution of code-based cryptography research over time. To map the intellectual structure of this field, the bibliometric indicators such as the performance of a 45-year span of publication timelines, prominent journals, authors, research institutions, nations, and disciplines are used. This bibliometric analysis provides insight into pivotal advancement, key contributors, and emerging areas of code-based cryptography. In addition to contributing to the existing body of knowledge, this comprehensive bibliometric examination of code-based cryptography serves as an invaluable resource to researchers seeking understand the dynamics and trajectory of this crucial cryptographic field in contemporary research.

Subject Classification: *06F25.*

Keywords: *Bibliometric analysis, Code-based cryptography, Error-correcting codes, McEliece, Quantum computing.*

1. Introduction

Cryptographic [7], [18], [22] techniques have been a powerful force in tandem with information technology advancements. Code-based

* *E-mail:* `ritu.rs.maths@mdurohtak.ac.in (Corresponding Author)`
† *E-mail:* `ektanarwal.math@mdurohtak.ac.in`

cryptography, a paradigm rooted in the elegance of error-correcting codes, has emerged as a cornerstone in the search for robust and secure communication systems. Originating from McEliece's [19] groundbreaking work in the late 1970s, code-based cryptography has gained attention as researchers struggle to cope with the ever-growing challenges posed by emerging technologies and secure communication [26] channels. As a result of the inherent resistance of code-based cryptographic primitives to quantum attacks [20], this field has gained renewed interest in its theoretical foundations and practical applications. Thus, it is essential to gain a comprehensive understanding of the scholarly landscape within code-based cryptography [17]. To achieve this goal, it is critical to review the current literature and identify potential areas for further research. Bibliometric analysis can provide a comprehensive overview of the current literature, identify emerging trends, and inform future research directions. Furthermore, it can help researchers better understand the evolving landscape of code-based cryptography and their potential contributions to its progress. By mapping the network of connections, researchers can identify trends in the research community, identify the most influential authors, and gain insight into the current state of knowledge. By delving into the quantitative aspects of publications, citations, collaboration patterns, and thematic evolution, a bibliometric exploration aims to unearth not only the current state of code-based cryptography but also its historical roots and potential trajectories. This paper embarks on such a journey, employing bibliometric methods to shed light on the multifaceted dimensions of code-based cryptography research, thus contributing to the broader discourse on the evolution of cryptographic methodologies in our digitally interconnected world. The paper highlights the evolution of code-based cryptography research, exploring its major trends and developments, and examining its evolution over time. It also provides an in-depth analysis of the research landscape, highlighting the leading researchers in the field and the most active research topics. Finally, the paper offers insights into the future prospects of code-based cryptography research.

2. Literature Review

In cryptographic research, code-based cryptography has gained attention due to its ingenious application of error-correcting codes [21]. The purpose of this literature review is to provide a comprehensive overview of previous studies utilizing bibliometric analyses to shed light

on the evolving landscape, key contributors, and emerging trends within code-based cryptography. The existing body of literature emphasizes surveys in the domain, including topics like public key algorithms, digital signature schemes [12], and theoretical attacks associated with code-based cryptography. Although these surveys provide valuable insights into the theoretical foundations and vulnerabilities of code-based cryptographic methods, but a noticeable gap exists when it comes to the application of bibliometric analysis to this particular field in the literature. While extensive research has been conducted on related topics like cryptography, quantum technology [25], IoT devices [14], [23], and blockchain, the focused lens on code-based cryptography remains conspicuously absent in the existing body of bibliometric literature. As a result, the present study aims to fill this void by providing a pioneering examination of the quantitative dimensions, collaboration networks, and thematic trends inherent in code-based cryptography. As the cryptographic landscape evolves, this research will not only provide a foundational bibliometric analysis, but will also serve as a catalyst for further investigation into this crucial and resilient paradigm. It provides valuable insights into the growth, impact, and interconnectedness of research in this specialized field through this effort, thereby contributing to both the cryptographic community and academic discourse on secure communication methods as a whole. This research will provide a comprehensive overview of the state of this field and will provide a platform for further innovation and development.

3. Bibliometric Analysis

Bibliometric analysis is a quantitative research method that examines publication patterns, citation, and collaboration in academic literature. This method allows researchers to identify trends in research, identify influential researchers, and measure research groups or individual researchers' productivity. This section provides a valuable lens through which we can explore the changing landscape of code-based cryptography research. Code-based cryptography has grown and developed significantly over time as a specialized area within cryptographic studies. This section examines quantitative aspects of code-based cryptography's scholarly output using various bibliometric methods. Through systematic data collection, analyses, and interpretation, the aim of this study is to unveil publication patterns, citation dynamics, collaboration networks, and the overall impact of research in this field. In addition to providing an

overview of the current state of code-based cryptography, this study sheds light on the historical trajectories, emerging trends, and collaborative endeavors that shape this critical area of research. In this section, 45-year span of publication timelines, important journals, authors, research institutions, and nations are compared. A thorough search of the Scopus database (upto October, 2023) has been conducted here to ensure the comprehensive coverage of the relevant literature. Thus, the objective of our exploration of bibliometric indicators is to provide valuable insights into the research ecosystem surrounding code-based cryptography, inform future directions, and facilitate informed decision-making for researchers, policymakers, and institutions concerned with cryptography. We performed bibliometric analysis using VOSviewer and R-Studio in this study. Using data from the Scopus database, we conducted an extensive citation analysis of 719 papers and reviews. This database allows users to find articles with specified key words, such as those in titles, abstracts, or key words. The initial sample size was 72,389 publications. We then filtered out irrelevant articles, leaving 802 papers for further analysis. The final sample for this investigation consists of 719 documents. We conducted an in-depth analysis of the 719 documents to understand the impact of our research.

3.1 *Leading Years*

The figure 1 below shows the trend in the field of code-based cryptography over the past years. In the early years, only two to four

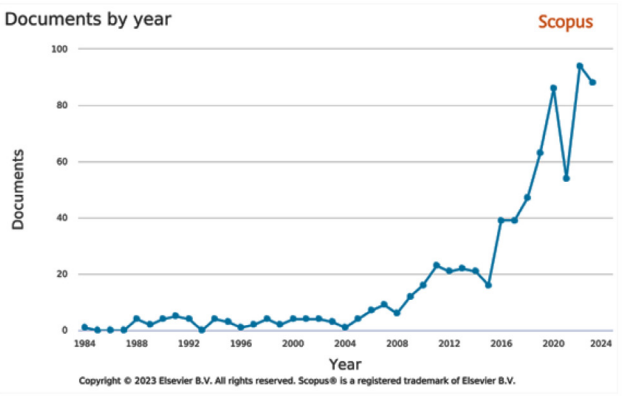

Figure 1

Number of Articles Published per Year

articles were published annually about code-based cryptography, but since the introduction of polar codes, this number has gradually increased. The figure 1 shows that the year 2022 has the most prominent number of publications compared to the other years. A total of 526 out of 719 articles were published during the year (2015-2023). This suggests that polar codes have become increasingly popular in the field of code-based cryptography in recent years. This trend will continue in the coming years, with more publications expected.

3.2 Most Prominent Countries

Out of 719 articles, 617 articles were published by the top ten countries, accounting for 85.81 % of total publications. It can be seen from the table 1 that France is the country that has the highest number of publications (118). In addition, around 100 articles were published in this research area by the United States, Germany, and China. Italy and India has 44 and 38 articles, respectively. The Netherlands has the lowest number of publications, 24. Table 1 and figure 2 below provide the number of articles published by several countries.

Table 1
Most Prominent Countries

Country	Documents
France	118
United States	105
Germany	100
China	92
Italy	44
India	38
Japan	37
Russian Federation	32
Singapore	27
Netherlands	24

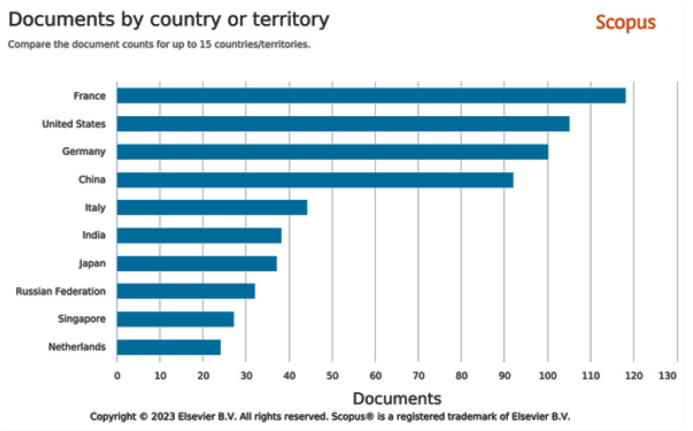

Figure 2

Number of Articles Published by Country

3.3 *Most relevant sources*

The figure 3 shows the ten most relevant sources based on code-based cryptography. In this research area, Lecture Notes in Computer Science is the most relevant source with 239 articles. From the figure 3, Lecture Notes in Computer Science has 239 documents, IEEE International Symposium on Information Theory Proceedings has 26 documents, Designs Codes and Cryptography has 21 documents, IEEE transactions on Information Theory has 19 documents, and IEEE Access has 12 documents respectively. Thus, the number of documents being produced annually by the different sources has also increased in the last five years.

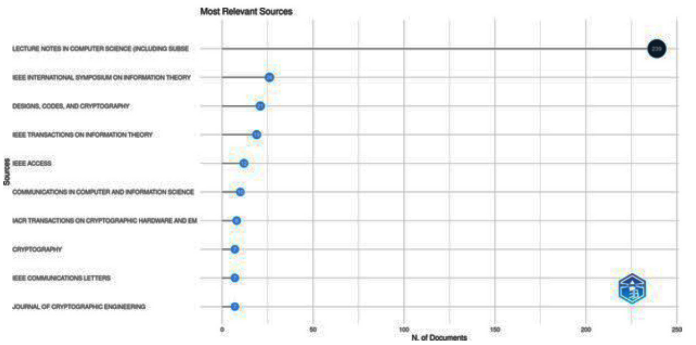

Figure 3

Most Relevant Sources

3.4 *Most Relevant Disciplines*

Figure 4 shows the documents by subject area. From the figure 4, we can see that computer science branch accounts 659 articles, which is about 46.3 % of total articles. Also, Mathematics and Engineering both includes 607 articles, which is about 29.3 % and 13.4 % respectively.

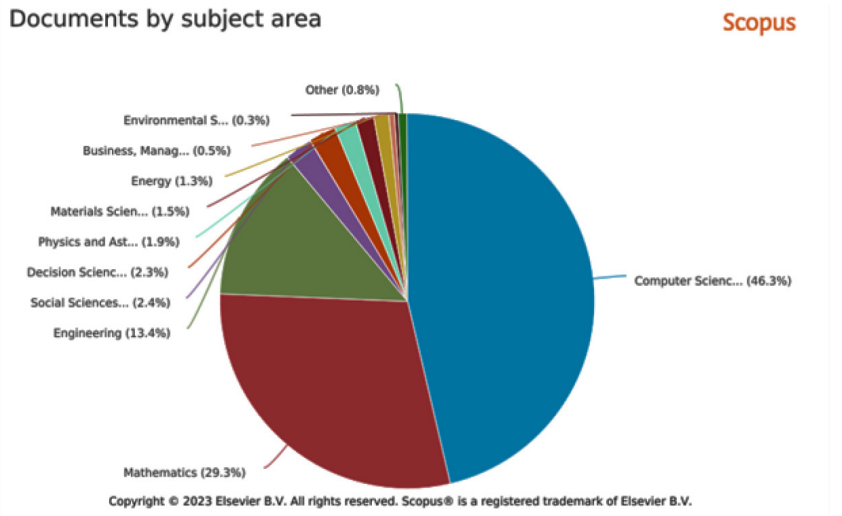

Figure 4

Number of Articles by Subject Area

3.5 *Most Relevant Authors*

The table 2 shows the top fifteen authors who contributed to the field of code-based cryptography in the past few years. The author Gaborit P. has the highest number of publications (34 articles) in the field of digital signature schemes based on error-correcting codes. From the table 2, we can see that the authors Cayrel P-L., Baldi M., Santine P., and Persichetti E. have the most number of publications (27, 19, 19, and 18 papers, respectively). The top fifteen authors contributed 243 articles accounting for around 33 % of total publications while Gabroit P. only accounts 4 % of total publications.

Table 2
Most Relevant Authors based on Number of Publications

Authors	Articles	Articles Fractionalized
GABORIT P [1]	34	9.06
CAYREL P-L [7], [8]	27	6.85
BALDI M [3]	19	4.80
SANTINI P [2]	19	4.82
PERSICHETTI E [5]	18	6.83
TILLICH J-P [9]	16	4.08
CHIARALUCE F	15	3.72
SENDRIER N [24]	14	6.31
JOHANSSON T [6]	12	4.07
LAU TSC [16]	12	5.01
OTMANI A [10]	12	3.22
TAN CH [15]	12	5.20
BARENGHI A [4]	11	3.12
GUNEYSU T	11	3.98
KUZNETSOV A	11	2.22

3.6 *Most Relevant Affiliation*

The table 3 shows the top fifteen most relevant affiliation in the research era of code-based cryptography. The Nanyang Technological University and Sun Yat-Sen University with 28 articles are the most relevant affiliation in this research field. Also, Universita Politecnica Delle Marche, Politecnico Di Milano, and National University of Singapore with 27, 27, and 23 articles respectively, contributed most in this research era. The top fifteen affiliations with 323 articles contributes about 45 % of total publication.

Table 3
Most Relevant Affiliation based on Number of Publications

Affiliation	Articles
NANYANG TECHNOLOGICAL UNIVERSITY	28
SUN YAT-SEN UNIVERSITY	28
UNIVERSITY OF LIMOGES	27

UNIVERSITA POLITECNICA DELLE MARCHE	27
POLITECNICO DI MILANO	23
NATIONAL UNIVERSITY OF SINGAPORE	22
TECHNISCHE UNIVERSITAT DARMSTADT	22
UNIVERSITE DE LIMOGES	22
UNIVERSITY OF WATERLOO	21
RUHR UNIVERSITY BOCHUM	20
TECHNICAL UNIVERSITY OF MUNICH	20
FLORIDA ATLANTIC UNIVERSITY	19
UNIVERSITE CHEIKH ANTA DIOP	16
EAST CHINA NORMAL UNIVERSITY	14
LUND UNIVERSITY	14

4. Emerging Trends and Future Directions

Based on our comprehensive bibliometric analysis, we have gained valuable insights into the landscape of cryptography research, revealing a rich tapestry of metrics that illuminate the field's trajectory. This bibliometric analysis found significant appearances for post quantum cryptography [13], code-based cryptography, and McEliece encryption scheme. A closer look at the 45-year span of publication timelines shows that there has been a significant upward trajectory in the number of articles published within code-based cryptography. For researchers working in this era, France is the best option as it has the highest number of publication. Among the top twenty sources identified in our bibliometric analysis, with 239 articles â€œLecture Notes in Computer Scienceâ€ is the most prominent and influential source in code-based cryptography research. As a result, this publication series serves as a crucial platform for disseminating cutting-edge research, innovative methodologies, and theoretical advancements in the field, highlighting the value of academic conferences. Additionally, an analysis of this bibliometric data reveals computer science to be the most relevant discipline in code-based cryptography research, accounting for 46.3 % of all articles. In addition to demonstrating the central nexus of code-based cryptography within computer science, its prevalence also emphasizes the interdisciplinary collaborations that often occur at the intersection of computer science, mathematics, information theory, and related fields. This interdisciplinary approach has enabled the development of new techniques, algorithms,

and protocols that are increasingly being used in real-world applications. Furthermore, it highlights the importance of collaboration between different research disciplines in order to effectively address the challenges of code-based cryptography. Using most relevant author analysis, Gaborit P. is one of the most prolific and influential authors, boasting the highest number of publications. His work has shaped the narrative and pushed the boundaries of research within this specialized cryptographic field as a leading figure in academia. The two standout affiliations, Nanyang Technological University and Sun Yat-sen University, emerge as the most relevant contributors to the scholarly landscape. The substantial number of publications affiliated with these institutions demonstrates their central role in shaping the scholarly landscape. Their prominence as affiliations signifies their role in advancing cryptographic technology and contributing to the academic discourse, strengthening their position as leading institutions in the field.

This analysis comprehensively delves into the expansive landscape of articles related to code-based cryptography, particularly emphasizing the use of various error-correcting codes [11]. Despite extensive research being conducted on public key algorithms incorporating error-correcting codes, very little work has been done in terms of exploring polar codes within the context of code-based cryptography. Despite being a potent family of error-correcting codes, polar codes have yet to receive the same degree of attention in this domain. A promising area of future research revolves around the integration of polar codes into code-based cryptographic schemes because of their capacity to achieve the Shannon limit. An exploration of polar codes and their potential applications and enhancements to code-based cryptography is an intriguing and valuable direction to pursue in order to advance the capabilities and security of cryptographic systems.

Conclusion

This research paper examines code-based cryptography from a bibliometric perspective to shed light on its multifaceted landscape. Using quantitative metrics, collaboration networks, and thematic evolution, we have attempted to gain valuable insight into the state and trajectory of this specialized field. Through this bibliometric analysis, we observed shifts in emphasis and emerging subdomains in code-based cryptography research over time. Our analysis not only quantified the prolific growth of publications but also identified key contributors, collaborative hubs, and

emerging trends that characterize the dynamic nature of code-based cryptography research. In this analysis, the focus on practical imple mentations indicates that code-based cryptography is maturing from theoretical proposals to practical applications. This analysis identified pivotal works that have influenced the field significantly, providing the foundation for future research. Our findings suggest that code-based cryptography is a vibrant and growing field with a diverse set of codes and an ever-evolving set of topics. Our findings can also provide useful insights into the strategies needed to stay ahead of the curve and develop innovative solutions.

References

[1] Nicolas Aragon, Philippe Gaborit, Ayoub Hauteville, Olivier Ruatta, and Gilles Zémor, "Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography," *IEEE Trans. Inf. Theory,* vol. 65, no. 12, pp. 7697–7717 (2019), doi: 10.1109/TIT.2019.2933535.

[2] Marco Baldi, Giacomo Cancellieri, Franco Chiaraluce, Edoardo Persichetti, and Paolo Santini, "Using Non-Binary LDPC and MDPC Codes in the McEliece Cryptosystem," in Proc. 2019 AEIT Int. Annu. Conf. (AEIT), Florence, Italy, pp. 1–6 (2019), doi: 10.23919/AEIT.2019.8893339.

[3] Marco Baldi, Franco Chiaraluce, Joachim Rosenthal, Paolo Santini, and Davide Schipani, "Security of generalised Reed–Solomon code-based cryptosystems," *IET Inf. Secur.,* vol. 13, no. 4, pp. 404–410 (2019), doi: 10.1049/iet-ifs.2018.5207.

[4] Alessandro Barenghi, Walter Fornaciari, Andrea Galimberti, Giuseppe Pelosi, and Davide Zoni, "Evaluating the Trade-offs in the Hardware Design of the LEDAcrypt Encryption Functions," in Proc. 2019 26th IEEE Int. Conf. Electron., Circuits Syst. (ICECS), Genoa, Italy, pp. 739–742 (2019), doi: 10.1109/ICECS46596.2019.8964882.

[5] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini, "LESS is More: Code Based Signatures Without Syndromes," in Lecture Notes in Computer Science, vol. 12174, Cham: Springer, pp. 45–65 (2020), doi: 10.1007/978-3-030-51938-4_3.

[6] Irina E. Bocharova, Thomas Johansson, and Boris D. Kudryashov, "Improved iterative decoding of QC-MDPC codes in the McEliece public

key cryptosystem," in Proc. 2019 IEEE Int. Symp. Inf. Theory (ISIT), Paris, France, pp. 1882–1886 (2019), doi: 10.1109/ISIT.2019.8849839.

[7] P.-L. Cayrel, S. M. El Yousfi Alaoui, G. Hoffmann, M. Meziani, and R. Niebuhr, "Recent progress in code-based cryptography," in Information Security and Assurance. ISA 2011, T. Kim, H. Adeli, R. J. Robles, and M. Balitanas, Eds., Communications in Computer and Information Science, vol. 200. Berlin, Germany: Springer, pp. 21–32 (2011). doi: 10.1007/978-3-642-23141-4_3.

[8] P.-L. Cayrel, G. Hoffmann, and E. Persichetti, "Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes," in Lecture Notes in Computer Science, vol. 7237, Berlin, Germany: Springer, pp. 138–155 (2012). doi: 10.1007/978-3-642-30057-8_10.

[9] A. Couvreur, M. Lequesne, and J.-P. Tillich, "Recovering short secret keys of RLCE in polynomial time," in Lecture Notes in Computer Science, vol. 11505, Berlin, Germany: Springer, pp. 133–152 (2019). doi: 10.1007/978-3-030-25510-7_7.

[10] P. Gaborit, A. Otmani, and H. T. Kalachi, "Polynomial-time key recovery attack on the Faure-Loidreau scheme based on Gabidulin codes," *Designs, Codes and Cryptography,* vol. 86, no. 7, pp. 1391–1403 (Jul. 2018). doi: 10.1007/s10623-017-0402-0.

[11] K. Khathuria, J. Rosenthal, and V. Weger, "Encryption scheme based on expanded Reed-Solomon codes," *Advances in Mathematics of Communications,* vol. 15, no. 2, pp. 207–218 (May 2021). doi: 10.3934/amc.2020053.

[12] R. Khurana and E. Narwal, "Analysis of code-based digital signature schemes," *International Journal of Electrical and Computer Engineering* (IJECE), vol. 13, no. 5, pp. 5534–5541 (Oct. 2023). doi: 10.11591/ijece.v13i5.pp5534-5541.

[13] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array,* vol. 15, p. 100242 (Dec. 2022). doi: 10.1016/j.array.2022.100242.

[14] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," *Computer Networks,* vol. 217, p. 109327 (Apr. 2022). doi: 10.1016/j.comnet.2022.109327.

[15] T. S. C. Lau and C. H. Tan, "A new encryption scheme based on rank metric codes," in *Lecture Notes in Computer Science*, vol. 10946, pp. 750–758 (2018). doi: 10.1007/978-3-319-93638-3_43.

[16] T. S. C. Lau and C. H. Tan, "A new Gabidulin-like code and its application in cryptography," in *Lecture Notes in Computer Science*, vol. 11445, pp. 269–287 (2019). doi: 10.1007/978-3-030-16458-4_16.

[17] A. Leevik, V. Beliaev, B. Stasenko, V. Davydov, and S. Bezzateev, "Review and analysis of the classical and post-quantum ring signature algorithms," in Proc. 2020 12th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 105–112 (2020). doi: 10.1109/ICUMT51630.2020.9222244.

[18] E. Narwal, Ritu, Niram, and Deepika, "ERN cryptosystem for the security of textual data based on modified classical encryption techniques," *Indian Journal of Science and Technology,* vol. 16, no. 4, pp. 292–298 (Jan. 2023). doi: 10.17485/IJST/v16i4.2009.

[19] P. Perez-Pacheco and P. Caballero-Gil, "McEliece cryptosystem: reducing the key size with QC-LDPC codes," in Proc. 2023 19th Int. Conf. on the Design of Reliable Communication Networks (DRCN), pp. 1–6 (2023). doi: 10.1109/DRCN57075.2023.10108339.

[20] I. Putu Agus Eka Pratama and I. Gusti Ngurah Agung Krisna Adhitya, "Post quantum cryptography: comparison between RSA and McEliece," in Proc. 2022 Int. Conf. on ICT for Smart Society (ICISS), pp. 1–5 (2022). doi: 10.1109/ICISS55894.2022.9915232.

[21] R. Redhu and E. Narwal, "Polar code-based cryptosystem: comparative study and analysis of efficiency," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 804–810 (May 2023). doi: 10.11591/ijeecs.v32.i2.pp804-810.

[22] Niram Ritu, E. Narwal, and S. Gill, "A novel cipher technique using substitution and transposition methods," in Rising Threats in Expert Applications and Solutions, Lecture Notes in Networks and Systems, vol. 434, pp. 123–129 (2022). doi: 10.1007/978-981-19-1122-4_14.

[23] M. Schöffel, J. Feldmann, and N. Wehn, "Code-based cryptography in IoT: A HW/SW co-design of HQC," in Proc. 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), pp. 1–7 (2022). doi: 10.1109/WF-IoT54382.2022.10152031.

[24] N. Sendrier, "Code-based cryptography: State of the art and perspectives," *IEEE Security & Privacy,* vol. 15, no. 4, pp. 44–50 (2017). doi: 10.1109/MSP.2017.3151345.

[25] S. Sharma, K. R. Ramkumar, A. Kaur, T. Hasija, S. Mittal, and B. Singh, "Post-quantum cryptography: A solution to the challenges of classical encryption algorithms," in *Lecture Notes in Electrical Engineering*, vol. 948, pp. 23–38 (2023). doi: 10.1007/978-981-19-6383-4_3.

[26] M. K. Shathir, G. E. Arif, and R. K. K. Ajeena, "More secure on the symmetric encryption schemes based on triple vertex path graph," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 4, pp. 1175–1182 (2023). doi: 10.47974/JDMSC-1564.

Received March, 2024