

Polar code-based cryptosystem: comparative study and analysis of efficiency

Ritu Redhu, Ekta Narwal

Department of Mathematics, Maharshi Dayanand University, Rohtak, India

Article Info

Article history:

Received Jun 16, 2023

Revised Jul 9, 2023

Accepted Jul 28, 2023

Keywords:

Channel polarization

Code-based cryptography

Coding theory

Error-correcting codes

Polar codes

Public key cryptography

ABSTRACT

This review paper aims to examine the use of polar codes in public key cryptosystems, providing a comprehensive overview of the state-of-the-art in this field at present. This study thoroughly searches databases such as IEEE Xplore, Scopus, and the ACM digital library to locate relevant research articles. In this study, we demonstrate the use of polar codes in public key cryptography and provide valuable insights for researchers interested in this field of research. The paper identifies several areas for further research and development, such as improved security and reliability of polar code-based cryptosystems. An analysis of the review highlights the major challenges and open research questions in this area, including the need for efficient key generation algorithms and the trade-offs between security and performance. An analysis of various existing encryption techniques as well as their security proofs is provided in the tables.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ekta Narwal

Department of Mathematics, Maharshi Dayanand University

Rohtak, Haryana, India

Email: ektanarwal.math@mdurohtak.ac.in

1. INTRODUCTION

The rapid evolution of technologies and their security issues set the ground for cryptography [1], namely for public key cryptography. It provides confidentiality, integrity [2], non-repudiation, authentication [3], and availability to the users. It is generally believed that public key cryptography relies on the hardness of factoring large integers or computing discrete logarithms [4]. It was shown in 1994 by Peter Shor that quantum computers would be able to break the majority of classical cryptographic systems that are based on factoring of discrete logarithms [5]. The results showed that with the help of quantum computers, integers could be factorized in polynomial time. Thus, quantum computers can hack traditional algorithms and deploy public-key encryption schemes [6]. While several promising post quantum cryptography (PQC) [7] candidates have been identified, such as lattice-based [8], code-based [9], and hash-based cryptography [10], there are still open research questions and challenges that need to be addressed:

- Shor's quantum prime factorization algorithm poses a threat to existing cryptosystems based on discrete logarithmic problems and integer factorization. Thus, it is necessary to conduct research in order to comprehend and quantify the implications of replacing current cryptographic algorithms with PQC algorithms [11].
- The field of PQC is one of the most recent areas of research in cryptography. In order to determine its actual practical applicability, it is necessary to better understand its performance, security, and implementation.
- The large key size of public and private keys in a cryptosystem is the main weakness and the researchers are still trying to resolve this problem.

- Most cryptosystems take a longer time for the encoding process, which gives longer time to the hackers to retrieve keys and to design a way to know the keys whenever they are changed.

This paper is designed to address code-based cryptography [12], which refers to cryptosystems that rely on mathematical error-correction codes that are difficult to decode, also known as the syndrome decoding problem. McEliece [13] proposed the first code-based cryptosystem in 1978 based on Goppa codes. The main advantage of this cryptosystem is high encryption and decryption speed compared to Rivest, Shamir, Adleman (RSA). But, due to the large key size and low information rate, this cryptosystem has not been widely used. After this, many variants of the McEliece cryptosystem based on Reed-Solomon codes [14], reed-muller codes, low-density parity check (LDPC) codes [15], and convolution codes, have been designed. However, all these are broken by cryptanalysts and not secured against various structural attacks [16]. To enhance the security of the cryptosystems against these attacks, a new family of error-correcting codes named polar codes [17] are introduced by Arikan in 2008, these are the first family of error-correcting codes that have been proven to achieve the capacity of discrete memoryless channels with appropriate encoding and decoding algorithms [18]. These have a complexity of $O(N \log N)$ for encoding and decoding algorithms, making them suitable for better communication [19]. These have excellent decoding performance and a specific structure of generator matrix obtained using Kronecker product, enabling them to have a small key size [20].

As part of this study, the objective is to describe the state of the art of the PQC candidate, which has been provided by the National Institute of Standards and Technology (NIST), which is code-based cryptography, specifically for encryption and decryption schemes with a code-based approach. The present study examines polar code-based cryptographic systems in terms of security, efficiency, and practicality to evaluate these systems' efficacy, security, and efficiency. A brief overview of the principles, security analyses, information rate, key size, performance evaluation, and recent advancements is provided in this paper in order to contribute to a better understanding of polar code-based cryptographic schemes by contributing to a better understanding of their principles, security analyses, and performance evaluation. Code-based encryption schemes are a class of cryptographic algorithms that uses error-correcting codes to provide safe encryption and decryption process. These encryption schemes rely on hard mathematical problems, provide robust security properties, and resist attacks from classical and quantum computers [21]. Here, are some code-based encryption schemes:

- McEliece encryption scheme proposed by McEliece [13] a new public-key cryptosystem based on binary Goppa codes which resist quantum computers. The private key of the McEliece cryptosystem includes S (random $(k \times k)$ non-singular matrix called scrambling matrix), G (a $(k \times n)$ generator matrix of binary Goppa code with error-correcting probability of t vectors), and P (random $(n \times n)$ permutation matrix), and given by $P_{rk} = \{S, G, P\}$. The public key constitutes the set (G', t) , where $G' = SGP$, a $k \times n$ matrix and t is the error probability.
- Niederreiter encryption scheme given by Niederreiter [22] that is a variation of the McEliece cryptosystem in which he uses the same idea of binary Goppa codes on the parity check matrix. Thus, the private key includes (S, H, P) and the public key is given by $G' = SHP$. This scheme is ten times faster as compared to the encryption scheme of McEliece.
- Hybrid McEliece encryption scheme (HyMES) proposed by Biswas and Sendrier [23] which is a dual version of McEliece encryption scheme in which he uses a random monic irreducible polynomial $g(Z)$ as Goppa polynomial which can correct t errors. The public-key size of HyMES is $k \times n - k$ which is reduced as compared to the public-key size of McEliece. The encryption of message vector is given as: $c = mG' + e$ where $G' = \begin{pmatrix} I_k \\ Q \end{pmatrix} = SGP$ and the decryption is given as: $m' = mSGP$ and m is being computed from S_c decoding algorithm where $S_c = (HP)c^t$.
- Rank metric cryptography [24] uses error-correcting codes that are defined over matrix spaces. Unlike traditional code-based cryptosystem, rank metric codes work over matrices, and their security is based on the difficulty of matrix related problems. The encryption and decryption processes are performed using linear transformation and rank calculations. It involves cryptographic primitives such as encryption, signature schemes, and identification protocols.
- Digital signature schemes are cryptographic protocols that are used to authenticate and integrate documents and data. It is used to protect the forgery of documents during transmission. To create a digital signature, a key pair will be generated. A signature is generated by passing a message through a hash function. The same hash function is used to verify the signature [25].

The purpose of this paper is to present advances, challenges, and prospects related to cryptosystems based on polar codes. To achieve secure and efficient encryption, it is imperative that continuous research and innovation be undertaken to address the challenges and harness the full potential of polar codes. In this paper, we review the main ideas of the code-based cryptosystems initiated by NIST and discuss various aspects such as key size, information rate, known attacks, and error probability with various parameters of the code. An

overview of the various evolution phases of code-based cryptography is presented and reviewed in a table that compares and contrasts different encryption schemes.

2. METHOD

The method for this review includes a thorough search of academic databases and then identifying the key research questions about the current state-of-the-art techniques and research directions in this area. The narrative techniques have been commended for their impartiality and applicability, in which systematic reviews have outlined the procedures for conducting a comprehensive literature review. The steps which are used in the systematic review process are given in Figure 1.



Figure 1. Research methodology process

To conduct this systematic review, we use several databases including IEEE Xplore, Scopus, and ACM digital library. To narrow the search, keywords such as public key cryptography or post-quantum cryptography, code-based cryptography, polar codes, or McEliece cryptosystem are used. These keywords are used to filter out irrelevant articles and to obtain relevant articles related to our topic. Following this, we establish inclusion and exclusion criteria to select the literature that will be included in the review paper [21]. The inclusion criteria include the relevance of the article to our research topic, and the McEliece cryptosystem and its variants based on polar codes. A number of exclusion criteria are specified, including a restriction on subject matter to the areas of computer science, mathematics, and engineering, a limitation on document type to the conference paper and article, and a restriction on language to English only. A total of 1,419 papers met this criterion out of 69,491 submissions. Then, we extract the data from the selected articles, analyze the data and identify the problems being addressed. Based on this data, the proposed cryptosystem, the method to hide the generator matrix, how to reduce the key size, the results obtained, and the conclusions are drawn. In last, we critically evaluate the strength and weaknesses of reviewed literature in terms of key size and security assessment of public key cryptosystems based on non-systematic polar codes. Here, Figure 2 provides a keywords cluster diagram that helps us to quickly identify the main areas to highlight in the review process and to navigate through the content more easily. The Figure 2 shows related keywords or phrases grouped according to their relevance and co-occurrence in the text. The minimum number of occurrences is set at 15, out of 7,271 keywords, only 183 met this requirement. In this study, there are 183 keywords divided into five clusters, each representing a specific theme or concept discussed in the paper. In Cluster 1 (red cluster), there are 56 items and 3,862 links related to public key cryptography and its primitives. Cluster 2 (green cluster) has 37 items with 3,058 total links that cover the topic of code-based cryptography and the McEliece cryptosystem. Cluster 3 (blue cluster) has 36 items with 2,910 total links that include post-quantum cryptography and its primitives. Cluster 4 (yellow cluster) has 34 items with 2,624 total links that cover error-correcting codes, decryption, and data security. Cluster 5 (purple cluster) has 20 items with 1,562 total links that include encryption schemes, and digital signature schemes.

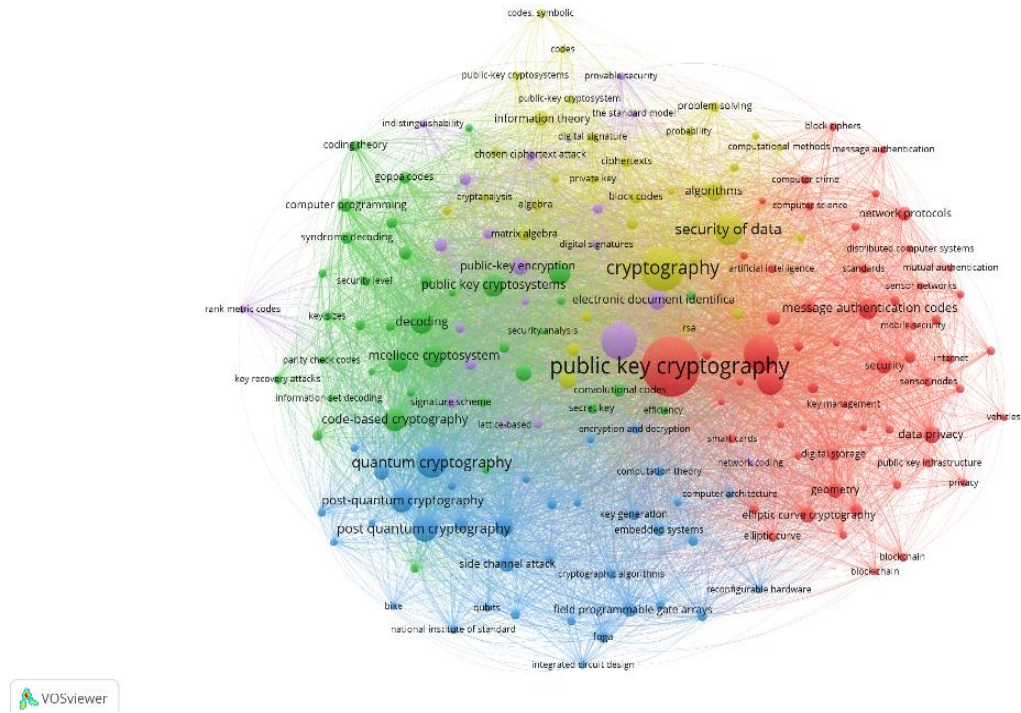


Figure 2. Keywords cluster diagram

3. RESULTS AND DISCUSSION

The weakness of the McEliece cryptosystem and its security against various well-known statistical attacks are analyzed in Table 1. Table 1 provides an overview of various attacks on three heuristic code-based encryption schemes and whether these schemes are resistant to these attacks or not. In this table, we will summarize the impact of the various attacks on code-based cryptosystems. The * in the table represents that the scheme is resistant to that attack. The researchers then started to work on security parameters for removal of these attacks [26] resulting in the development of the Rao and Nam (RN) cryptosystem [27], Major-Voting (MV), Struik and Triburg (ST) [28], and the Barbero and Ytrehus [29] scheme in which they focused on hamming code with small code length. The evolution of the scheme was proposed by Hooshmand and Aref [30]–[32] in which they proposed a cryptosystem based on polar codes [33]. With the special properties of polar codes [34], they tried to overcome the weakness of the McEliece cryptosystem and reduce the key length to a larger extent [35]. Also, they proposed a method to hide the generator matrix, preventing it from the adversary. Various researchers have proposed cryptosystems based on polar codes [36]–[40] and analyzed their security and compared their efficiency with the existing schemes. A comparison [41], [42] of various PQC algorithms based on different types of error-correcting codes [43]–[45] is provided in Table 2. The comparison has been done based on various parameters such as type of code, code length, key size, information rate, and attacks on that scheme.

Table 1. Various attacks on code-based cryptosystems

Attack	Broadcast	Known partial	Message resend	Related message	Batch chosen plain	Adaptive chosen plain	Chosen ciphertext	Reaction	Malleability
Scheme									
McEliece [13]	*	Yes	Yes	Yes	Yes	*	Yes	Yes	Yes
Niederreiter [22]	Yes	Yes	*	*	Yes	Yes	Yes	Yes	Yes
Biswas and Sendrier [23]	Yes	Yes	*	Yes	Yes	Yes	Yes	Yes	Yes

It is noted that with the use of the intrinsic property [46] of polar codes [47], the key length of existing algorithms is reduced to a larger extent and the increased information rate shows secured and reliable communication. Thus, we find that public key cryptosystems based on non-systematic polar codes [48] are more efficient than traditional public key cryptosystems in terms of key length and implementation timings. But, these traditional cryptosystems face challenges in quantum computers in terms of security and efficiency, so they need upgradation in both aspects for further practical applicability. The systematic polar codes [49] are proved to be more robust against error propagation than their non-systematic counterparts. Thus, the findings of this review provide a valuable resource for researchers and provide a research challenge to develop more secure and efficient public key cryptosystems [50] based on systematic polar codes.

Table 2. Comparing the various existing scheme based on various error-correcting codes

Scheme	Code	Code parameter (n, k)	Rate	Key length (Kbits)	Security
Rao and Nam [27]	Hamming	(72,64)	0.89	18	Insecure against chosen-plaintext attack
McEliece [13]	Goppa	(1024,524)	0.51	$P_b = 67.07$ $P_r = 102.5$	Secured against brute-force attack
Barbero and Ytrehus [29]	Hamming	(30,20)	0.66	4.9	Secured against chosen-plaintext attack
Rao [51]	LDPC	(1024,524)	0.51	2mbits	Secured against convolution attacks
Afshar <i>et al.</i> [50]	Quasi-Cyclic (QC) LDPC	(2044,1024)	0.5	2.5	Secured against brute-force, chosen-plaintext, RN attack
Secret key cryptosystem based on polar codes [31]	Polar	(1024,768)	0.75	9.34	Secured against brute-force, RN, ST attack
Efficient secure channel coding scheme [39]	Polar	(2084,1781)	0.87	1.6	Secured against brute-force, RN, ST attack
Shrestha [36]	Polar	(2048,1536)	0.75	384	Secured against brute-force, siedelnikov attack
PKC-PC [32]	Polar	(1024,768)	0.75	24	Secured against key search, key recovery, Information Set Decoding (ISD), adaptive chosen cipher-text attack
Reducing the key length of McEliece cryptosystem [35]	Polar	(2048,1750)	0.85	$P_b = 65.19$ $P_r = 2.75$	Secured against Stern, brute-force attack
Secret key cryptosystem based on non-systematic PC [30]	Polar	(1024,832)	0.8125	≤ 5	Secured against brute-force, RN, MV, ST attack
PolarRLCE [38]	Polar	(2048,500)	0.95	97.53	Secured against brute-force attack, square attack, key-recovery, message-decoding attack
Joint encryption-encoding scheme [43]	QC-LDPC	(1530,1275)	0.83	0.235	Secured against brute-force, ciphertext-only, message resend, statistical, chosen-plaintext attack

4. CONCLUSION

This review paper aims to explore potential solutions for systems that resist quantum computers. It presents a comprehensive examination of recent advancements in public key cryptosystems based on polar codes, starting from fundamental concepts and mathematical foundations to their application in constructing public key cryptosystems. By carefully considering various aspects of error-correcting code-based cryptosystems, including code length, dimension, information rate, key length, and susceptibility to structural attacks, we conducted a comparative analysis of different existing cryptosystems. To assess the efficiency and reliability of these schemes, we provide a comprehensive comparison table. Our findings indicate that the utilization of polar codes significantly reduces the required key length in existing algorithms. However, despite these encouraging results, several challenges remain, such as the development of more efficient decoding algorithms and the exploration of alternative constructions for systematic polar code-based public key cryptosystems.

ACKNOWLEDGEMENTS

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-public sectors.

REFERENCES





- [1] A. M. Qadir and N. Varol, "A review paper on cryptography," in *7th International Symposium on Digital Forensics and Security, ISDFS 2019, Institute of Electrical and Electronics Engineers Inc*, Jun. 2019, doi: 10.1109/ISDFS.2019.8757514.

- [2] E. Narwal, R. Ritu, N. Niram, and D. 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.
- [3] N. Ritu, E. Narwal, and S. Gill, "A novel cipher technique using substitution and transposition methods," in *Lecture Notes in Networks and Systems*, vol. 434, pp. 123–129, 2022.
- [4] E. Egorova, G. Kabatiansky, E. Krouk, and C. Tavernier, "A new code-based public-key cryptosystem resistant to quantum computer attacks," *Journal of Physics: Conference Series*, vol. 1163, no. 1, Feb. 2019, p. 12061, doi: 10.1088/1742-6596/1163/1/012061.
- [5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.
- [6] M. Kumar and P. Pattnaik, "Post quantum cryptography (PQC)-an overview: (invited paper)," *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, Sep. 2020, doi: 10.1109/HPEC43674.2020.9286147.
- [7] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: a review of techniques, challenges and standardizations," in *International Conference on Information Networking*, vol. 2023-Janua, Jan. 2023, pp. 146–151, doi: 10.1109/ICOIN56518.2023.10048976.
- [8] H. Bandara, Y. Herath, T. Weerasundara, and J. Alawaturgodu, "On advances of lattice-based cryptographic schemes and their implementations," *Cryptography*, vol. 6, no. 4, p. 56, Nov. 2022, doi: 10.3390/cryptography6040056.
- [9] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Code-based post-quantum cryptography," *The Multidisciplinary Preprint Platform*, Apr. 2021, doi: 10.20944/preprints202104.0734.v1.
- [10] L. Li, X. Lu, and K. Wang, "Hash-based signature revisited," *Cybersecurity*, vol. 5, no. 1, 2022, doi: 10.1186/s42400-022-00117-w.
- [11] M. Campagna, B. LaMacchia, and D. Ott, "Post quantum cryptography: readiness challenges and the approaching storm," *arXiv preprint arXiv:2101.01269*, 2021.
- [12] P. L. Cayrel, S. M. El Y. Alaoui, G. Hoffmann, M. Mezzani, and R. Niebuhr, "Recent progress in code-based cryptography," in *Communications in Computer and Information Science*, vol. 200 CCIS, Springer Berlin Heidelberg, 2011, pp. 21–32.
- [13] R. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, pp. 114–116, 1978.
- [14] V. Korrapati, V. D. Prasad, D. V. Reddy, and G. A. Tej, "A Study on performance evaluation of reed solomon codes through an AWGN channel model for an efficient communication system," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, pp. 1038–1041, 2013.
- [15] C. Yu, Z. H. Lin, T. W. Hsu, M. W. Chen, and Y. A. Chen, "Lower bit-error-rate polar-LDPC concatenated coding for wireless communication systems," in *2017 IEEE 6th Global Conference on Consumer Electronics, GCCE 2017*, vol. 2017-January, Oct. 2017, pp. 1–2, doi: 10.1109/GCCE.2017.8229237.
- [16] V. Drăgoi, T. Richmond, D. Bucerzan, and A. Legay, "Survey on cryptanalysis of code-based cryptography: From theoretical to physical attacks," in *2018 7th International Conference on Computers Communications and Control, ICCCC 2018 - Proceedings*, May 2018, pp. 214–223, doi: 10.1109/ICCC.2018.8390461.
- [17] A. Mohan and R. P. Sreedharan, "A review on the concept of polar codes," Mar. 2018, doi: 10.1109/WiSPNET.2018.8538538.
- [18] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009, doi: 10.1109/TIT.2009.2021379.
- [19] J. H. Bae, A. Abotabl, H. P. Lin, K. B. Song, and J. Lee, "An overview of channel coding for 5G NR cellular communications," *APSIPA Transactions on Signal and Information Processing*, vol. 8, no. 1, 2019, doi: 10.1017/ATSIP.2019.10.
- [20] K. D. Rao, "Performance analysis of polar codes for 5G short message transmissions," in *2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 2018, doi: 10.1109/UPCON.2018.8596901.
- [21] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A review of the present cryptographic arsenal to deal with post-quantum threats," *Procedia Computer Science*, vol. 215, pp. 834–845, 2022, doi: 10.1016/j.procs.2022.12.086.
- [22] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Problems of Control and Information Theory*, vol. 15, no. 2, pp. 157–166, 1986.
- [23] B. Biswas and N. Sendrier, "McEliece cryptosystem implementation: Theory and practice," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5299 LNCS, Springer Berlin Heidelberg, pp. 47–62, 2008.
- [24] T. S. C. Lau and C. H. Tan, "A new technique in rank metric code-based encryption," *Cryptography*, vol. 2, no. 4, pp. 1–16, Oct. 2018, doi: 10.3390/cryptography2040032.
- [25] R. Khurana and E. Narwal, "Analysis of code-based digital signature schemes," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 5, p. 5534, Oct. 2023, doi: 10.11591/ijece.v13i5.pp5534-5541.
- [26] R. Devi, E. Narwal, and S. Gill, "Securing unauthorized access to cloud data storage," in *Lecture Notes in Networks and Systems*, vol. 434, Springer Nature Singapore, pp. 205–213, 2022.
- [27] T. R. N. Rao and K. H. Nam, "Private-key algebraic-code encryptions," *IEEE Transactions on Information Theory*, vol. 35, no. 4, pp. 829–833, Jul. 1989, doi: 10.1109/18.32159.
- [28] R. Struik and J. van Tilburg, "The rao-nam scheme is insecure against a chosen-plaintext attack," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 293 LNCS, Springer Berlin Heidelberg, 1988, pp. 445–457.
- [29] Á. I. Barbero and Ø. Ytrehus, "Modifications of the rao-nam cryptosystem," in *Coding Theory, Cryptography and Related Areas*, Springer Berlin Heidelberg, pp. 1–12, 2000.
- [30] R. Hooshmand, M. R. Aref, and T. Eghlidos, "Secret key cryptosystem based on non-systematic polar codes," *Wireless Personal Communications*, vol. 84, no. 2, pp. 1345–1373, May 2015, doi: 10.1007/s11277-015-2691-9.
- [31] R. Hooshmand, M. K. Shooshtari, and M. R. Aref, "Secret key cryptosystem based on polar codes over binary erasure channel," in *International ISC Conference on Information Security and Cryptology (ISCISC)*, Aug. 2013, doi: 10.1109/ISCISC.2013.6767351.
- [32] R. Hooshmand, M. K. Shooshtari, and M. R. Aref, "PKC-PC: A variant of the McEliece public-key cryptosystem based on polar codes," *IET Communications*, vol. 14, no. 12, pp. 1883–1893, Jul. 2020, doi: 10.1049/iet-com.2019.0689.
- [33] K. H. Moussa, S. Shaaban, and A. H. El-Sakka, "Secured polar code derived from random hopped frozen-bits," *Wireless Networks*, vol. 29, no. 1, pp. 423–435, Sep. 2023, doi: 10.1007/s11276-022-03127-1.
- [34] T. Zhang, S. Li, and B. Yu, "A channel coding scheme based on multi-kernel polar codes for transmitting data over compressed voice channels," in *2020 IEEE 6th International Conference on Computer and Communications, ICC 2020*, Dec. 2020, pp. 674–679, doi: 10.1109/ICCC51575.2020.9345272.
- [35] R. Hooshmand, M. K. Shooshtari, T. Eghlidos, and M. R. Aref, "Reducing the key length of mceliece cryptosystem using polar codes," in *2014 11th International ISC Conference on Information Security and Cryptology, ISCISC 2014*, Sep. 2014, pp. 104–108, doi: 10.1109/ISCISC.2014.6994031.





- [36] S. R. Shrestha, "Design of new public key encryption scheme based on the polar coding," in *Proceeding 2013 the 23rd Joint Conference Communication and Information (JCCI'13)*, 2013.
- [37] Y. S. Kim, J. H. Kim, and S. H. Kim, "A secure information transmission scheme with a secret key based on polar coding," *IEEE Communications Letters*, vol. 18, no. 6, pp. 937–940, Jun. 2014, doi: 10.1109/LCOMM.2014.2318306.
- [38] J. Liu, Y. Wang, Z. Yi, and Z. Lin, "polarRLCE: a new code-based cryptosystem using polar codes," *Security and Communication Networks*, vol. 2019, pp. 1–10, Dec. 2019, doi: 10.1155/2019/3086975.
- [39] B. Mafakheri, T. Eghlidos, and H. Pilaram, "An efficient secure channel coding scheme based on polar codes," *The ISC Int'l Journal of Information Security*, vol. 9, no. 2, pp. 111–118, 2017.
- [40] C. Sun, Z. Fei, D. Jia, C. Cao, and X. Wang, "Secure transmission scheme for parallel relay channels based on polar coding," *Tsinghua Science and Technology*, vol. 23, no. 3, pp. 357–365, Jun. 2018, doi: 10.26599/TST.2018.9010081.
- [41] N. Sharma, D. Jain, K. Bhatt, and M. T. Themalil, "Performance comparison of various digital modulation schemes based on bit error rate under AWGN channel," in *Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021*, Apr. 2021, pp. 619–623, doi: 10.1109/ICCMC51019.2021.9418396.
- [42] P. Pathak and R. Bhatia, "Performance analysis of polar codes for next generation 5G technology," in *2022 3rd International Conference for Emerging Technology (INCET)*, IEEE, May 2022, doi: 10.1109/INCET54531.2022.9824746.
- [43] H. Khayami, T. Eghlidos, and M. R. Aref, "A joint encryption-encoding scheme using QC-LDPC codes based on finite geometry," *Scientia Iranica*, Aug. 2022, doi: 10.24200/sci.2022.58300.5658.
- [44] A. M. Cuc, C. Grava, F. L. Morgos, and T. A. Burca, "Performances comparison between low density parity check codes and polar codes," in *International Conference on Systems, Signals, and Image Processing*, Jun. 2022, vol. 2022-June, doi: 10.1109/IWSSIP55020.2022.9854483.
- [45] X. Wang *et al.*, "An optimized encoding algorithm for systematic polar codes," *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Aug. 2019, doi: 10.1186/s13638-019-1491-4.
- [46] M. Zhang, Z. Li, and L. Xing, "An enhanced belief propagation decoder for polar codes," *IEEE Communications Letters*, vol. 25, no. 10, pp. 3161–3165, Oct. 2021, doi: 10.1109/LCOMM.2021.3104152.
- [47] K. D. Rao and T. A. Babu, "Performance analysis of QC-LDPC and polar codes for eMBB in 5G systems," in *Proceedings - 2019 International Conference on Electrical, Electronics and Computer Engineering, UPCON 2019*, Nov. 2019, doi: 10.1109/UPCON47278.2019.8980142.
- [48] K. Niu and Y. Li, "Polar codes for fast fading channel: design based on polar spectrum," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10103–10114, Sep. 2020, doi: 10.1109/TVT.2020.3005914.
- [49] I. E. Kaime, A. A. Madi, and H. Erguig, "Systematic polar codes in 5G NR," Mar. 2022, doi: 10.1109/IRASET52964.2022.9738221.
- [50] A. A. S. Afshar, T. Eghlidos, and M. R. Aref, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes," *IET Communications*, vol. 3, no. 2, pp. 279–292, 2009, doi: 10.1049/iet-com:20080050.
- [51] T. R. N. Rao, "Joint encryption and error correction schemes," *ACM SIGARCH Computer Architecture News*, vol. 12, no. 3, pp. 240–241, Jan. 1984, doi: 10.1145/773453.808188.

BIOGRAPHIES OF AUTHORS



Ritu Redhu     received the M.Sc. from the Department of Mathematics, Kurukshetra University, Kurukshetra. She had passed B.Sc. from Govt. P.G. College, Jind. She is currently pursuing Ph.D. Degree in Mathematics from the Department of Mathematics, Maharshi Dayanand University, Rohtak. Her area of research is coding theory and cryptography. She has published 2 research papers. She may be contacted at email: ritu.rs.maths@mdurohtak.ac.in.



Dr. Ekta Narwal     B.Sc. (Computer Science, Mathematics, Physics), M.C.A., Ph.D. in Computer Science and Applications. She is working as an Assistant Professor in the Department of Mathematics, at Maharshi Dayanand University, Rohtak (Haryana) India since 2012. She worked as Guest Lecturer, in Computer Science in the Department of Mathematics, M. D. University Rohtak from January 2011 to March 1, 2012. Her major research areas are coding theory, cryptography, network security, and artificial neural networks. She has research experience of 7 years and teaching experience of nearly 12 years. She has published 13 research papers. She may be contacted at email: ektanarwal.math@mdurohtak.ac.in.