

Analysis of code-based digital signature schemes

Rupali Khurana, Ekta Narwal

Department of Mathematics, Faculty of Physical Sciences, Maharshi Dayanand University, Rohtak, India

Article Info

Article history:

Received Oct 17, 2022

Revised Jan 17, 2023

Accepted Feb 4, 2023

Keywords:

Code-based cryptography

Code-based digital signatures

Cryptography

Digital signatures

Error-correcting codes

Post-quantum cryptography

ABSTRACT

Digital signatures are in high demand because they allow authentication and non-repudiation. Existing digital signature systems, such as digital signature algorithm (DSA), elliptic curve digital signature algorithm (ECDSA), and others, are based on number theory problems such as discrete logarithmic problems and integer factorization problems. These recently used digital signatures are not secure with quantum computers. To protect against quantum computer attacks, many researchers propose digital signature schemes based on error-correcting codes such as linear, Goppa, polar, and so on. We studied 16 distinct papers based on various error-correcting codes and analyzed their various features such as signing and verification efficiency, signature size, public key size, and security against multiple attacks.

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, Faculty of Physical Sciences, Maharshi Dayanand University

Rohtak, India

Email: ektanarwal.math@mdurohtak.ac.in

1. INTRODUCTION

In modern times, we use the internet to transfer data from one point to another. For secure transmission of data, we use cryptography [1]. Cryptography is a technique of protecting useful information by converting it into an unreadable format [2]. Many cryptographic algorithms are present that provide secure transmission via the insecure network [3]. But it has been forecasted that quantum computers [4] can break many classical cryptographic algorithms. Now, to protect these classical cryptographic algorithms from quantum computers, several algorithms are made that are also secure in the quantum era and are named post-quantum cryptography (PQC) [5]. Post-quantum cryptography mainly includes hash-based cryptography [5], lattice-based cryptography [6], and code-based cryptography [7].

In this paper, we will discuss only code-based cryptography. It includes all the cryptosystems in which security depends upon the hardness of encoding and decoding of the error-correcting codes like Goppa codes [8], Bose-Chaudhuri-Hocquenghem (BCH) codes [9], and Reed-Solomon codes [10]. In 1978, McEliece introduced the first code-based public-key cryptosystem [11]. This cryptosystem is based on a random binary Goppa code. In 1986, Harald Niederreiter proposed a variation of the McEliece cryptosystem [11], which uses a parity check matrix in place of the generator matrix used by McEliece. After that Stern identification scheme [12], Courtois-Finiasz-Sendrier (CFS) signature scheme [13], and many more came into existence.

There is a high chance of data being forged or stolen by the theft during transmission. Due to this fact, various digital signatures [14] are used during transmission to ensure that the data or message comes from the authorized entity and remains unchanged [15]. Digital signature [16] is a type of electronic signature in which the integrity and authentication of a message are verified by using mathematical algorithms. Recently used digital signatures like digital signature algorithm (DSA) are not secure against

quantum attacks. So, post-quantum digital signatures are very much in demand. There are many signature schemes present like hash-based signatures [17], lattice-based signatures [18], and code-based signatures [19]. Here, we focus only on code-based digital signatures. Code-based digital signature [19] is a type of digital signature that depends on the hardness of decoding the error-correcting codes like Goppa codes [8], linear codes [20], polar codes [21], and cyclic codes [22]. The major problem in code-based digital signatures is the large size of the public key and slow signature generation speed. In this paper, we will discuss some code-based signatures and identification schemes and find the scheme that will resolve this problem.

Here, we will discuss some basic definitions and some present threats against the signature schemes in section 2. Section 3 will discuss a few existing code-based digital signature schemes. We will analyze various properties of code-based digital signature schemes like signing and verification efficiency, signature size, public key size, and security against multiple attacks in section 4. Section 5 will explain the future plan. Lastly, we will conclude in section 6.

2. PRELIMINARIES

In coding theory, error-correcting codes are used to detect and correct errors. They are also used in post-quantum primitives in order to resist attacks against quantum computers. Here are some basic definitions and problems related to coding theory.

2.1. Linear codes

A (n, k) linear code C' over a field with q elements is a linear subspace of dimension k and length n of the linear space F_q^n [20]. A matrix G of order $k \times n$ is a generator matrix for an (n, k) linear code C' if the rows of G form a basis of C' over the field F_q [23]. A matrix H of order $(n - k) \times n$ is said to be the parity-check matrix [23] for an (n, k) linear code C' over the field having q elements if the rows of H form a basis for the orthogonal complement of C' , and it satisfies $C' = \{y \in F_q^n ; Hy^T = 0\}$.

2.2. Difficult problems in coding theory

Here, we discuss syndrome decoding problem and Goppa code distinguishing problems. In syndrome decoding problem, we choose a matrix H of order $m \times n$, and p be a target vector such that $p \in F_q^m$ over a field F_q , and an integer $l > 0$. We find a vector $y \in F_q^n$ having weight $\leq l$ satisfying $Hy^T = p^T$ [24]. In Goppa code distinguishing problem, we choose a matrix H of order $(n - k) \times n$ randomly over a field F_q . Our goal is to decide whether H is a parity check matrix for a Goppa code (n, k) or a (n, k) random code parity check matrix [25].

2.3. Threats against code-based digital signatures

Digital signatures [26] are used very commonly in the digital world, and their main goal is to provide integrity and authentication [27]. But digital signatures are not secure and can be attacked by the attacker. Here are a few threats or attacks against digital signatures:

In a key recovery attack, the attacker attempts to recover the private/secret key with the help of the signer's public key. After recovering the private/secret key, he can easily forge the digital signature [28]. A forgery attack is an attack in which the attacker attempts to create a valid signature for a document without the knowledge of the signer's private key. If he creates a valid signature, he can forge the signature [28]. In chosen message attack, the attacker somehow makes the signer to sign one or more messages. Now, the attacker has some messages and signature pairs, and with the help of these pairs, the attacker analyzes the signature and tries to re-create it [29]. The attacker in a known-message attack has few messages and signature pairs. With the help of these signatures' pairs, the attacker analyzes the messages and signature pairs. After that, he can easily recover the signer's private key [30], and with the help of the private key, he can forge the signature. In a key substitution attack, the attacker has a public key and signature on a message $'d'$. Now, the attacker produces a different public key that validates the same signature on the same message $'d'$, which affects the authentication of a message [31].

Table 1 shows different attacks present on various code-based digital signature schemes. Key recovery attack against the rank quasi code-based signature. Forgery attack against CFS and identity-based signature. Chosen message attack against stern's identification and signature scheme. Known message attack against Kabastianskii-Krouk-Smeets (KKS) signature. Key substitution attack against CFS signature.

Table 1. Attacks on code-based digital signature schemes

Attacks\Code-based digital signature scheme	CFS	KKS	Stern's identification and signature	Identity-based signature	Rank quasi-cyclic code-based signature
Key recovery attack [28]					✓
Forgery attack [28]	✓			✓	
Chosen message attack [29]			✓		
Known message attack [30]		✓			
Key substitution attack [31]	✓				

3. CODE-BASED DIGITAL SIGNATURE SCHEMES

Firstly, Xinmei [32] proposed a digital signature scheme, which was proven to be insecure [33]. After that, many digital signature schemes are designed which depend upon various error-correcting codes. Some of them are discussed here.

Initially, Stern [12] proposed an identification scheme that depends on the syndrome decoding problem for the error-correcting codes. Here, the author describes a basic-zero knowledge protocol that enables any prover P to identify himself to any other verifier V . The probability of attacking the scheme is $(2/3)$. Using the Fiat-Shamir method, it is possible to convert Stern's identification scheme into a signature scheme [34].

Then, Kabatianskii *et al.* [35] proposed a digital signature scheme that depends on random linear error-correcting codes. The authors presented three different forms of the KKS scheme, and one modified form that helps to construct signatures from the codes containing low weight codewords. All the forms were based on different linear codes to enhance the scheme and resist some attacks. Also, the authors claimed that all the signature schemes were secure if the public parameters did not give any information. Cayrel *et al.* [36] proved that the attacker only needs a maximum of 20 signatures to break the KKS signature scheme. The authors gave new parameters to get a security of 40 signatures to resist this attack.

Later on, Courtois *et al.* [13] proposed the first practical code-based digital signature scheme depends on the McEliece cryptosystem. He made a signature using the Niederreiter cryptosystem. He used binary Goppa codes to develop the signature scheme. For any given integer m and t , Goppa codes are of length $n = 2^m$ and of dimension $k = n - mt$. These codes can correct a maximum of t errors. In this paper, the authors chose the parameters $m = 16$ and $t = 9$ and proposed a digital signature scheme of about 81 bits. This scheme depends upon a well-known syndrome decoding problem.

Zheng *et al.* [37] then presented the first code-based ring signature scheme by extending the CFS scheme. This practical ring signature was based on the syndrome decoding problem. Each signer uses t error-correcting Goppa codes having length $n = 2^m$ and dimension $k = n - mt$, for some integers m and t . In this paper, the authors chose the parameters $m = 16$ and $t = 9$, and made a ring signature of length about $144 + 126l$, where l is the number of ring members. The authors also showed that the probability of forging the signature was about $(1/2^n)$.

Following that, Melchor *et al.* [38] presented the first code-based threshold ring signature scheme. In this paper, the author generalizes stern's scheme into the t -out of N threshold ring signature scheme with the help of the Fiat-Shamir paradigm. The proposed signature did not depend on the number of signers, i.e., t and the signature size depends on the maximum number of signers, i.e., N in a ring. The signature length was N times of stern's identification scheme, i.e., $20k_0 * N$. Its security depends upon the syndrome decoding problem. The proposed signature has the cheating probability $(2/3)$.

Then, Dallot and Vergnaud [39] proposed the second code-based threshold ring signature scheme combining the technique of Bresson and the CFS scheme. The proposed scheme used an (n, k) t error correcting Goppa codes with $n = 2^m$ and dimension $k = n - mt$, for positive integer m and t . Cayrel *et al.* [40] then proposed an improved identity-based identification scheme based on error-correcting codes. To develop this scheme, the author combines the modified Courtois-Finiasz-Sendrier (mCFS) signature scheme with the stern's identification scheme, in which security depends on the syndrome decoding problem. The authors used Goppa codes of length $n = 2^m$, and of dimension $k = n - mt$. They choose parameters $(16, 9)$ and produces a signature length of about $2^m \times (\text{no. of rounds})$. For the first round, the signature length is approx. 1.1 MB.

Alamelou *et al.* [41] presented the first code-based group signature scheme. The proposed group signature was obtained from the stern's identification protocol using the Fiat-Shamir paradigm. The idea behind the signature scheme was building a collision of two syndromes which was associated with two different matrices, one is the random matrix, and another is the trapdoor matrix. The security of the proposed scheme was based on the relaxation of the Bellare-Shi-Zhang (BSZ) model. The signature provides several properties such as anonymity, traceability [42], and non-frameability [41].

After that, Ren *et al.* [43] proposed an efficient code-based digital signature algorithm with the help of code-based hash function using the mCFS scheme. Here, the authors used the code-based hash function in place of the random hash function to better the signature's efficiency. The signing process of the signature was improved by reducing the signing time by $t!$ which increases the signing speed. The authors used Goppa codes of length $n = 2^m$ and of dimension $k = n - mt$.

Later on, Liu *et al.* [44] proposed a secure signature scheme using the improved version of a McEliece public key cryptosystem (PKC). The proposed scheme depends on the idea of the CFS scheme. The authors used binary (n, k, d) Goppa codes whose length and dimension are $n = 2^m$ and $k = n - mt$, and distance $d = 2t + 1$. The authors gave the probability of signing a message was $(1/t!^2)$. Also, the authors claimed that a smaller t could be chosen in the presented signature, i.e., 1, 2, 3. With the help of this, the signer needs some attempts for signing a message which increases the speed of signing. The proposed scheme has properties like fast signing speed, high security, and strong practicability.

Then, Sahu and Tripathi [45] proposed a signature scheme with the help of modified quasi-cyclic low density parity check (QC-LDPC) codes in place of Goppa codes used in the CFS scheme. Here, the authors used a belief propagation (BP) decoding scheme that increases the decoding speed. The security and efficiency of the CFS scheme were also improved by using the BP decoding scheme. The proposed scheme is fast, secure, and has small public key and signature size with high security. He chooses the parameters (16384, 12344) which reduces the key size to 6,140 bits.

Lee *et al.* [46] proposed a signature scheme that depends on modified reed-muller (RM) codes that reduce signing complexity. Here, the authors used $(U, U + V)$ codes with a high-dimensional hull in order to overcome the drawbacks of different code-based schemes. The presented signature scheme has a smaller key size and low signature time. This scheme also resists various known attacks like key substitution attacks. For classic security of 128 bits, the signature size is about 4096 bits, with a public key size less than 1 MB.

Forghani *et al.* [47] then proposed a digital signature scheme based on polar codes. This paper used polar codes [48] with the CFS scheme that reduces the public key size and signing time. The authors also proved that using polar codes in the CFS signature helps in improving security against forgery and key recovery attacks. The authors also showed that the proposed scheme is secure in random oracle model [49].

Hooshmand *et al.* [50] proposed two polar code-based identification schemes, Id-PC I, and Id-PC II, in which he replaces polar codes with random codes. The security of these schemes depends on the hardness of the syndrome decoding problem and the general decoding problem. As compared to the Stern and Veron scheme, the author reduces the size of public data by 90% and communication costs by 53%. The authors also showed in this paper that the proposed schemes Id-PC I and Id-PC II have a low cheating probability, i.e., $(2/3)^r$, where the protocol repeats ' r ' times, and are secure against information set decoding attacks.

Then, Cho *et al.* [51] proposed enhanced pqsigRM, a signature scheme based on modified reed-muller codes. Here, the author replaces the Goppa codes in the CFS scheme with modified reed-muller codes. This scheme has several advantages, including a small signature size and fast verification speed. The author also showed that the proposed scheme is resistant to a variety of attacks based on the Reed-Muller code-based cryptosystem. For the security of 128 bits, the size of the proposed signature is 512 bytes. To improve its performance, the author modifies the public code used in pqsigRM.

4. SUMMARY

This section will summarize the different code-based digital signature schemes and analyze their properties. Table 2 shows the survey of the different code-based digital signature schemes based on different error-correcting codes, signature size, security proof. We have also considered their properties like key size, signing time, and security against multiple attacks. From this table, we observe that the CFS scheme has the smallest signature size among various studied signature schemes.

Table 3 gives the public key sizes used in various digital signature schemes concerning their parameters and security. Among various schemes, we see that PolarSig has the smallest size of public key. This makes PolarSig a more practical and efficient digital signature scheme.

Figure 1 shows the size of a public key in Kilobytes for various code-based signature schemes. Dallot's signature scheme has the greatest public key size among all signature schemes, whereas PolarSig has the smallest public key size among all the signature schemes. This property makes the digital signature PolarSig more efficient.

Table 2. Different code-based digital signature schemes

Signature scheme	Security against model	Signature size	Codes	Properties	
Forghani <i>et al.</i> [47]	PolarSig	Random Oracle model	808 bits	Polar codes	Smaller key size, low signing time, secure against forgery and key recovery attacks
Liu <i>et al.</i> [44]	A secure and efficient signature scheme	Random Oracle model	81 bits	Goppa codes	Fast signing speed, high security, strong practicability, and authentication
Ren <i>et al.</i> [43]	An efficient code-based signature scheme	Random Oracle model	144 bits	Goppa codes	Fast signing speed, low signing time and more practicability
Alamélou <i>et al.</i> [41]	Group signature	Random Oracle model	$\sqrt{\log N} \sqrt{N}$	Linear codes	Anonymous, traceable, non-frameable, and authentication
Cayrel <i>et al.</i> [40]	Improved identity-based identification and signature scheme	Random Oracle model	1.1 MB	Goppa codes	Unforgeable and authentication
Melchor <i>et al.</i> [38]	Threshold ring signature scheme	Random Oracle model	$20k_0 * N$	Linear codes	Unforgeable, anonymous, and authentication
Zheng <i>et al.</i> [37]	Ring signature scheme	Random Oracle model	$144+126l$ (l : no. of ring members)	Goppa codes	Unforgeable, anonymous, practicability, and authentication
Courtois <i>et al.</i> [13]	CFS signature scheme	Random Oracle model	81 bits	Goppa codes	Practicability, short signature, fast verification, and authentication
Kabatianskii <i>et al.</i> [35]	KKS signature scheme	Random Oracle model	16,976 bits	Linear codes	Authentication
Stern [12]	Stern identification and signature scheme	Random Oracle model	120 Kbits	Linear codes	Unforgeable, simplicity
Fiat and Shamir [34]					

Table 3. Public key sizes of different code-based digital signature schemes

Digital Signature Scheme	Public Key Size	Security (in bits)
CFS (m, t) (16, 9) [13]	9,437,184 bits	83
KKS $(N, K, n, k, t_1, t_2, t, l)$ (9800, 4510, 1900, 259, 844, 1056, 1046, 8) [52]	6.8 MB	128
Stern $(2n, n)$ (694, 347) [53]	347 bits	83
PolarSig (N', k') (788, 246) [47]	50.2 KB	128
Ring signature (m, t) (15, 12) [37]	0.7 MB	80
Modified pqsigRM (r, m) (6, 12) [46]	0.773 MB	128
Parallel CFS (m, t) (16, 10) [28]	1.2 MB	80
mCFS (m, t) (19, 11) [54]	13.7 MB	80
Threshold ring signature		
(a) ACG (n, N) (634, 100) [38]	2.41 MB	80
(b) DV (m, t, N) (15, 12, 100) [39]	70 MB	80
Improved identity-based identification scheme (m, t) (15, 12) [40]	0.7 MB	80
Enhanced pqsigRM (r, m) (6, 12) [51]	474,445 Bytes	128
Id-PC identification scheme		
Id-PC I $(2k, k)$ (512, 256) [50]	256 bits	64
Id-PC II $(2k, k)$ (512, 256) [50]	512 bits	64

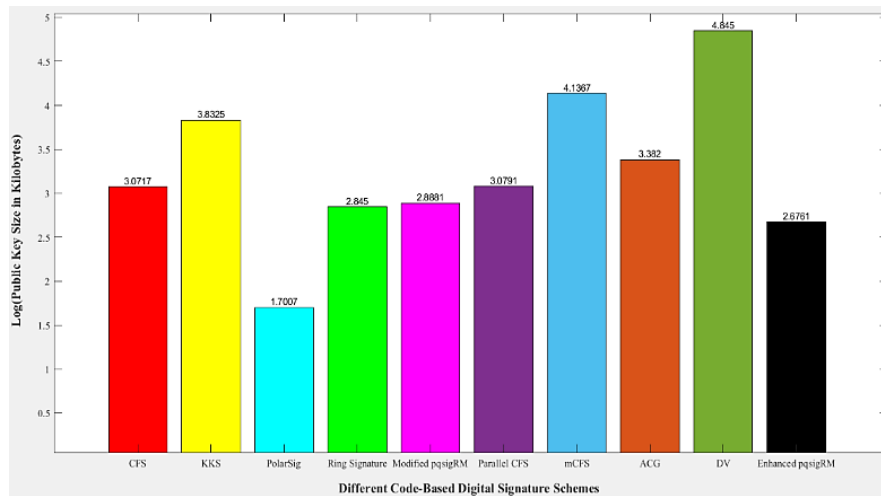


Figure 1. Comparison of public key sizes of various schemes

5. FUTURE PLAN

Polar codes have recently been used in 5G communications, making them a better choice among several error-correcting codes. Using polar codes in both the signature PolarSig and the identification scheme Id-PC gives them several advantages, such as reduced signature and key size, faster signing speed, and resistance to various attacks. These qualities make them the best of all schemes studied. In the future, we will create a digital signature scheme based on polar codes.

6. CONCLUSION





We presented various code-based digital signature schemes based on different error-correcting codes. We examined properties such as signature and public key size, signing and verification efficiency, and their resistance to various attacks. Digital signature PolarSig and the identification scheme Id-PC schemes based on polar codes are the best among the various studied digital signature and identification schemes because they have properties such as smaller key size and low signing time. These schemes are also resistant to a variety of attacks like key recovery attacks and forgery attacks.

REFERENCES





- [1] S. M. Naser, "Cryptography: from the ancient history to now, it's applications and a new complete numerical model," *International Journal of Mathematics and Statistics Studies*, vol. 9, no. 3, pp. 11–30, 2021.
- [2] A. M. Qadir and N. Varol, "A review paper on cryptography," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–6, doi: 10.1109/ISDFS.2019.8757514.
- [3] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security," *Journal of Physics: Conference Series*, vol. 1641, no. 1, Nov. 2020, doi: 10.1088/1742-6596/1641/1/012042.
- [4] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J.-M. Leimeister, "Quantum computing," *Electronic Markets*, vol. 32, no. 4, pp. 2525–2536, Dec. 2022, doi: 10.1007/s12525-022-00570-y.
- [5] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Post-quantum and code-based cryptography—some prospective research directions," *Cryptography*, vol. 5, no. 4, Dec. 2021, doi: 10.3390/cryptography5040038.
- [6] P. K. Pradhan, S. Rakshit, and S. Datta, "Lattice based cryptography: its applications, areas of interest and future scope," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Mar. 2019, pp. 988–993, doi: 10.1109/ICCMC.2019.8819706.
- [7] K. Sekhar Roy and H. Kumar Kalita, "A survey on post-quantum cryptography for constrained devices," *International Journal of Applied Engineering Research*, vol. 14, no. 11, pp. 2608–2615, 2019.
- [8] J. L. Carrasquillo-López, A. O. Gómez-Flores, C. Soto, and F. Piñero, "Introducing three best known Goppa codes," arxiv.org/abs/2010.07278, Oct. 2020.
- [9] M. Bossert, R. Schulz, and S. Bitzer, "On hard and soft decision decoding of BCH codes," *IEEE Transactions on Information Theory*, vol. 68, no. 11, pp. 7107–7124, Nov. 2022, doi: 10.1109/TIT.2022.3184168.
- [10] G. D. Priyadarshini and G. Suchitra, "Performance analysis of Reed-Solomon codes in digital communication system using labview," *ICTACT Journal on Communication Technology*, 2020.
- [11] A. Vambol, V. Kharchenko, O. Potii, and N. Bardis, "McEliece and Niederreiter cryptosystems analysis in the context of post-quantum network security," in *2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, Aug. 2017, pp. 134–137, doi: 10.1109/MCSI.2017.31.
- [12] J. Stern, "A new identification scheme based on syndrome decoding," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 773, Springer Berlin Heidelberg, 1994, pp. 13–21.
- [13] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2248, Springer Berlin Heidelberg, 2001, pp. 157–174.
- [14] S. Aggarwal and N. Kumar, "Digital signatures," in *Advances in Computers*, Elsevier, vol. 121, pp. 95–107, 2021.
- [15] E. Narwal and S. Gill, "Simulating manual signature using Elman back propagation model to create pseudo digital signature," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 2, pp. 4548–4551, Dec. 2019, doi: 10.35940/ijitee.B6452.129219.
- [16] U. Patel, A. Patel, and F. Suthar, "The study of digital signature authentication process," *Journal of Information, Knowledge and Research in Computer Science and Application*, 2019.
- [17] L. Li, X. Lu, and K. Wang, "Hash-based signature revisited," *Cybersecurity*, vol. 5, no. 1, Dec. 2022, doi: 10.1186/s42400-022-00117-w.
- [18] X. Lu, W. Yin, and P. Zhang, "Lattice-based verifiably encrypted signature scheme without gaussian sampling for privacy protection in blockchain," *Sustainability*, vol. 14, no. 21, Oct. 2022, doi: 10.3390/su142114225.
- [19] S. Gueron, E. Persichetti, and P. Santini, "Designing a practical code-based signature scheme from zero-knowledge proofs with trusted setup," *Cryptography*, vol. 6, no. 1, Jan. 2022, doi: 10.3390/cryptography6010005.
- [20] S. Y. Korabelshchikova, B. F. Melnikov, S. V. Pivneva, and L. V. Zyablitsseva, "Linear codes and some their applications," *Journal of Physics: Conference Series*, vol. 1096, no. 1, Dec. 2018, doi: 10.1088/1742-6596/1096/1/012174.
- [21] I. El Kaime, A. A. Madi, and H. Erguig, "A survey of polar codes," in *2019 7th Mediterranean Congress of Telecommunications (CMT)*, Oct. 2019, pp. 1–7, doi: 10.1109/CMT.2019.8931392.
- [22] B. Radičić, "Cyclic codes," in *Proceedings of the International Scientific Conference - Sinteza 2019*, Jan. 2019, pp. 465–471, doi: 10.15308/Sinteza-2019-465-471.
- [23] R. Hooshmand, M. Koochak Shoostari, and M. Reza 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.
- [24] P. S. Roy, K. Morozov, and K. Fukushima, "Evaluation of code-based signature schemes," *Cryptology ePrint Archive*, 2019.

- [25] R. Mora and J.-P. Tillich, "On the dimension and structure of the square of the dual of a Goppa code," *Designs, Codes and Cryptography*, vol. 91, no. 4, pp. 1351–1372, Apr. 2023, doi: 10.1007/s10623-022-01153-w.
- [26] Y. Bayane, F. Amounas, and L. El Bermi, "A novel digital signature based on error correcting codes," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 7, no. 3, pp. 25–28, Mar. 2019, doi: 10.17762/ijritcc.v7i3.5253.
- [27] J. Chandrashekhara, A. V B, P. H, and R. B R, "A comprehensive study on digital signature," *International Journal of Innovative Research in Computer Science and Technology*, vol. 9, no. 3, May 2021, doi: 10.21276/ijrcst.2021.9.3.7.
- [28] M. Finiasz, "Parallel-CFS strengthening the CFS McEliece-based signature scheme," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6544, Springer Berlin Heidelberg, 2011, pp. 159–170.
- [29] V. Shoup, "On the security of a practical identification scheme," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1070, Springer Berlin Heidelberg, 1996, pp. 344–353.
- [30] A. Otmani and J.-P. Tillich, "An efficient attack on all concrete KKS proposals," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7071, Springer Berlin Heidelberg, 2011, pp. 98–116.
- [31] K. Morozov, P. S. Roy, R. Steinwandt, and R. Xu, "On the security of the Courtois-Finiasz-Sendrier signature," *Open Mathematics*, vol. 16, no. 1, pp. 161–167, Mar. 2018, doi: 10.1515/math-2018-0011.
- [32] W. Xinmei, "Digital signature scheme based on error-correcting codes," *Electronics Letters*, vol. 26, no. 13, 1990, doi: 10.1049/el:19900586.
- [33] L. Ham and D.-C. Wang, "Cryptanalysis and modification of digital signature scheme based on error-correcting code," *Electronics Letters*, vol. 28, no. 2, 1992, doi: 10.1049/el:19920098.
- [34] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Advances in Cryptology*, vol. 263, Berlin, Heidelberg: Springer Berlin Heidelberg, 1987, pp. 186–194.
- [35] G. Kabatianskii, E. Krouk, and B. Smeets, "A digital signature scheme based on random error-correcting codes," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1355, Springer Berlin Heidelberg, 1997, pp. 161–167.
- [36] P. L. Cayrel, A. Otmani, and D. Vergnaud, "On Kabatianskii-Krouk-Smeets signatures," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4547, Springer Berlin Heidelberg, 2007, pp. 237–251.
- [37] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *International Journal of Network Security*, vol. 5, no. 2, pp. 154–157, 2007.
- [38] C. Aguilar Melchor, P.-L. Cayrel, and P. Gaborit, "A new efficient threshold ring signature scheme based on coding theory," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5299, Springer Berlin Heidelberg, 2008, pp. 1–16.
- [39] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5921, Springer Berlin Heidelberg, 2009, pp. 222–235.
- [40] P. L. Cayrel, P. Gaborit, D. Galindo, and M. Girault, "Improved identity-based identification using correcting codes," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 762–770, 2009.
- [41] Q. Alamélou, O. Blazy, S. Cauchie, and P. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, pp. 469–493, Jan. 2017, doi: 10.1007/s10623-016-0276-6.
- [42] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "A survey on group signatures and ring signatures: traceability vs. Anonymity," *Cryptography*, vol. 6, no. 1, Jan. 2022, doi: 10.3390/cryptography6010003.
- [43] D. Z. F. Ren and W. J. Wang, "An efficient code-based digital signature algorithm," *International Journal of Network Security*, vol. 19, no. 6, pp. 1072–1079, 2017.
- [44] X. Liu, X. Yang, Y. Han, and X. A. Wang, "A secure and efficient code-based signature scheme," *International Journal of Foundations of Computer Science*, vol. 30, no. 4, pp. 635–645, Jun. 2019, doi: 10.1142/S0129054119400173.
- [45] R. Sahu and B. P. Tripathi, "A code-based digital signature scheme using modified quasi-cyclic low-density parity-check codes (QC-LDPC)," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 2759–2763, Aug. 2019, doi: 10.35940/ijeat.F8822.088619.
- [46] Y. Lee, W. Lee, Y. S. Kim, and J.-S. No, "Modified PQSIGRM: RM code-based signature scheme," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3026989.
- [47] P. Forghani, M. Koochak Shooshtari, and M. R. Aref, "PolarSig: an efficient digital signature based on polar codes," *IET Communications*, vol. 14, no. 17, pp. 2889–2897, Oct. 2020, doi: 10.1049/iet-com.2019.0578.
- [48] A. Mohan and R. P. Sreedharan, "A review on the concept of polar codes," in *2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2018, pp. 1–5, doi: 10.1109/WiSPNET.2018.8538538.
- [49] J. Blocki, S. Lee, and S. Zhou, "On the security of proofs of sequential work in a post-quantum world," in *Leibniz International Proceedings in Informatics, LIPIcs*, vol. 199, Jul. 2021, doi: 10.4230/LIPIcs.ITC.2021.22.
- [50] R. Hooshmand, A. Jafari, and G. Karamali, "Id-PC: an identification scheme based on polar codes," *Information Security Journal: A Global Perspective*, pp. 1–14, Jan. 2022, doi: 10.1080/19393555.2021.2023239.
- [51] J. Cho, J.-S. No, Y. Lee, Z. Koo, and Y.-S. Kim, "Enhanced pqsigRM: code-based digital signature scheme with short signature and fast verification for post-quantum cryptography," *IEEE Access*, vol. 11, pp. 73413–73441, 2022.
- [52] O. Blazy, P. Gaborit, D. T. Mac, A. Otmani, and J.-P. Tillich, "A code-based signature scheme in the standard model," *Journal of Cryptology*, vol. 2, no. 4, pp. 451–474, 2002.
- [53] P. Gaborit and M. Girault, "Lightweight code-based identification and signature," in *2007 IEEE International Symposium on Information Theory*, Jun. 2007, pp. 191–195, doi: 10.1109/ISIT.2007.4557225.
- [54] L. Dallot, "Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4945, Springer Berlin Heidelberg, 2008, pp. 65–77.

BIOGRAPHIES OF AUTHORS

Rupali Khurana     did her M.Sc. (5-year Integrated M.Sc. Hons. Mathematics) from the Department of Mathematics, Maharshi Dayanand University, Rohtak. She is currently pursuing a Ph.D. Degree in Mathematics from the Department of Mathematics, Maharshi Dayanand University, Rohtak. Her area of research is coding theory and cryptography. She can be contacted at email: rupali.rs.maths@mdurohtak.ac.in.



Ekta Narwal     did her 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 8 years and teaching experience of nearly 11 years. She has published 11 research papers. She can be contacted at email: ektanarwal.math@mdurohtak.ac.in.