# A New Code Based Signature Scheme for Blockchain Technology

Adel Alahmadi, Selda Çalkavur, Patrick Solé, Abdul Nadim Khan, Arif Raza, Vaneet Aggarwal

MDPI

*Article*

# A New Code Based Signature Scheme for Blockchain Technology

**Adel Alahmadi [1,*], Selda Çalkavur [2], Patrick Solé [3], Abdul Nadim Khan [4], Mohd Arif Raza [4] and Vaneet Aggarwal [1]**

[1] Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science, King Abdulaziz University, 21589, Jeddah, Saudi Arabia; Saudi Arabia; vaneet@purdue.edu (V.A.)
[2] Department of Mathematics, Faculty of Arts and Science, Kocaeli University, 41380, Kocaeli, Turkey; selda.calkavur@kocaeli.edu.tr
[3] I2M, (Aix Marseille University, Centrale Marseille, CNRS), 163 Avenue de Luminy, 13009, Marseilles, France; patrick.sole@telecom-paris.fr
[4] Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science and Arts-Rabigh, King Abdulaziz University, 21589, Jeddah, Saudi Arabia; abdulnadimkhan@gmail.com (A.N.K.); arifraza03@gmail.com (M.A.R.)
* Correspondence: analahmadi@kau.edu.sa

**Abstract:** Blockchain is a method of recording information that makes it not feasible for the system to be replaced, attacked, or manipulated. A blockchain is equipped with a notebook that copies and processes the various procedures across the network of computers participating in the blockchain. Digital signature algorithm is one of the cryptographic protocols used by the blockchain. In this work, we introduce a new digital signature scheme based on error correcting codes. In the scheme constructed on a $[n, k, d]-$ code over $\mathbb{F}_q$, which is $d \geq 2t + 1$, and the size of the signature length is $n - k$. The signature verification is based on the bounded distance decoding of the code. Since the verification space is $(\mathbb{F}_q)^n$, the proposed scheme has an improved performance in terms of working in a wider space.

**Keywords:** blockchain; digital signature; public key cryptosystem; linear code

**MSC:** 94A60; 94B05; 94B35

**Citation:** Alahmadi, A.; Çalkavur, S.; Solé, P.; Khan, A.N.; Raza, M.A.; Aggarwal, V. A New Code Based Signature Scheme for Blockchain Technology. *Mathematics* **2023**, *1*, 0. https://doi.org/

Academic Editor: Jan Lansky and Jonathan Blackledge

Received: 31 January 2023
Revised: 21 February 2023
Accepted: 24 February 2023
Published:



## 1. Introduction

Public key cryptography is a procedure of encrypting or signing data with the public key and private key. The public key encrypts the data, and the private key decrypts the encrypted data. There is a mathematical relationship between these keys. Since the keys are connected, decoding it with the public key verifies that the suitable private key was used to sign the certificate, therefore verifying the signature's origin. Public key cryptography was proposed by Diffie and Hellman [1]. McEliece presented the first code-based public key encryption scheme based on the irreducible binary Goppa codes [2]. The encryption method is equivalent to adding an artificial error vector to the plaintext and the decryption method correspond to decoding in this scheme. Niederreiter's algorithm [3] is another public key encryption scheme based on error-correcting codes. The encryption and decryption methods are based on syndrome decoding. Çalkavur [4] introduced a new public key cryptosystem based on error correcting codes with bounded distance decoding. Digital signature algorithm, based on public key cryptography, is the electronic form, which uses a password method [2,5]. This algorithm is to use the user's private key to sign the message, and the user's public key is the sign [6]. One of the most common digital signatures is RSA [7], which is based on the factoring problem. ElGamal signature [8] is based on the difficulty of solving the discrete logarithm problem defined over finite fields. Dickson polynomial scheme [9,10], LUC [11,12], as well as the supersingular fulfilling of the elliptic curve digital signature algorithm (ECDSA) [13], have been proposed as digital signature

schemes. Elhabob et al. examined the mathematical NP hardness of digital signature schemes [14]. Nevertheless, one of the open problems in cryptography is to design a secure and effective digital signature scheme based on linear codes. In these systems, the plaintext and ciphertext areas do not overlap. The Courtois-Finiasz-Sendrier (CFS) scheme [15] is the first digital signature scheme based on error correcting codes. They use high rate Goppa codes. As it has some security defects, it is not practical. It is known that high-rate Goppa codes can be discriminated from random codes [16]. BBC$^+$ scheme [17] is based on low-density generator matrix (LDGM) codes, which have been cryptanalyzed in [18]. Persichetti proposed a one-time signature scheme in [19]. This scheme is based on quasi-cyclic (QC) codes. Kuznetsov et al. proposed a new electronic code-based digital signature scheme in [20,21]. Another digital signature scheme is suggested in [22]. Recently, multiple digital signature schemes have been proposed in [23–28].

Blockchain technology ensures integrity and validity that permits contributors in the blockchain to write, read, and confirm procedures booked in a system ledger. Nevertheless, it does not permit removal and innovation transactions on the procedures, nor does it permit other instructions stored on its ledger. The blockchain system is promoted and assured by cryptographic methods, e.g., digital signatures, hash functions, etc. These methods warrant that the procedures booked into the ledger are integrity preserved, authenticity ensured, and non-repudiated. Furthermore, blockchain assures autarchy, decentralization, stability, and affirmation for users in an unsafe circle [29,30]. Blockchain uses cryptography, especially public key cryptography, to generate digital signatures. The private key is saved in a digital wallet or in any program in the blockchain. A message is signed with the private key by an user. This message signing by the digital signature will be forwarded to the blockchain, and it is confirmed that the message is actually signed by the user. The user hashes the procedure output into a hash value determined by a one-way pseudo-random function, and then it signs on the hash value with the private key to produce the digital signature. Then, the user sends the digital signature, together with own procedure output, to the blockchain network. The receiver uses the user's public key to decrypt the taken digital signature to obtain hash value $A$, and he/she also hashes the procedure output to get another hash value, $B$. Finally, the receiver checks if the hash value $A$ equals the hash value $B$ or not. If they are equal, he/she allows the user's procedure. Chaum introduced a blockchain-like protocol in 1982 [31]. Haber et al. designated a safe blockchain in 1991 [32]. Bayer et al. introduced Merkle trees for blockchain in 1993 [33]. Nokamoto introduced Bitcoin in 2008 [34]. Ethereum was proposed by Buterin in 2013 [35]. Further, many blockchain studies were carried out [5]. In this paper, we construct a new digital signature scheme using the arguments of [4]. We describe the phases of signature generation and verification, and we analyze its security. In this context, we explain that our proposed scheme has integrity and non-repudiation, and it has no forgeability. Hence, we obtain some important security results, demonstrating that our new scheme is secure and effective.

The rest of the paper is organized as follows. The next section presents the background information about coding theory and cryptography. Section 3 explains the proposed digital signature scheme. Section 4 evaluates its security and efficiency. Furthermore, some possible attacks are also analyzed in this section. Section 5 compares the proposed approach with the other systems e.g., McEliece [2], Niederreiter [3], and Feneuil et al. [27]. Section 6 collects concluding remarks.

*Our Contributions*

Digital signature schemes can be used in many applications, including blockchain. We propose a new digital signature scheme based on error correcting codes and use the bounded distance decoding method. The proposed scheme has the properties of integrity, non-repudiation, and authenticity, which are required for blockchain. Furthermore, it is faster than the other code-based schemes. The proposed scheme is more reliable and preferable by means of security.

## 2. Preliminaries

In this section, we review some subjects [36,37] that provide a background for the manuscript.

### 2.1. Linear Codes

**Definition 1** (Linear Code). *A q-ary linear code C is a linear subspace of $(\mathbb{F}_q)^n$, $\mathbb{F}_q$ is the finite field, q is a prime power, and n is a positive integer. If C has dimension k, then C is called a $[n,k]$-code. The dual code $C^\perp$, which is a $[n, n-k]$-code, is orthogonal to every codeword of C.*

**Definition 2** (Hamming Weight). *The Hamming weight of a codeword $c \in C$ is the number of non-zero entries of c.*

**Definition 3** (Generator Matrix). *A generator matrix G for a linear code C is a $k \times n$ matrix for which the rows are a basis of C.*

**Definition 4** (Parity-Check Matrix). *The generator matrix of the dual code $C^\perp$ is called the parity-check matrix H of C, which is a $(n-k) \times n$ matrix.*

### 2.2. Coset Decoding

**Definition 5.** *Consider a $[n,k]$-code C over $\mathbb{F}_q$ and $v \in (\mathbb{F}_q)^n$. The coset of C is described as below.*

$$v + C = \{u + c | c \in C\}$$

**Theorem 1** (Lagrange [36]). *Suppose C is an $[n,k]$-code over $\mathbb{F}_q$. Then,*
*(i) every vector of $(\mathbb{F}_q)^n$ is in some coset of C,*
*(ii) every coset contains exactly $q^k$ vectors,*
*(iii) two cosets either are disjointed or coincided,*
*(iv) C contains exactly $q^{n-k}$ cosets.*

**Definition 6** (Coset Leader). *The vector having a minimum weight in a coset is called the coset leader. If there is more than one vector with minimum weight in the coset, then one is randomly selected.*

**Definition 7** (Syndrome Decoding). *Let y be any vector of $(\mathbb{F}_q)^n$. The syndrome of y is computed as follows.*

$$S(y) = yH^T,$$

*where H is a parity-check matrix of a $[n,k]$-code C. It is clear that $S(y)$ is the $1 \times (n-k)$ row vector. Furthermore,*

$$S(y) = 0 \Longrightarrow y \in C.$$

### 2.3. Digital Signature Algorithm

Digital signature [2,5] is one of the most important methods in cryptography. Digital signature operates in the algorithm of public key cryptosystems, and it is rested on the algebraic approaches of modular exponentiation and the discrete logarithm problem, which are hard problems in complexity theory. The PKC uses a key pair (public key, private key). It is the private key that generates a digital signature for a message. The signer's corresponding public key confirms the signature. Digital signature is used to perform non-repudiation (the addresser cannot untruly argue that they have not signed the message), as well as authentication (the recipient can confirm the principle of the message). Digital signature also guarantees message integrity (the recipient can confirm that the message has not been replaced since it was signed).

### 2.4. McEliece and Niederreiter Signature

McEliece [2] public key cryptosystem is based on error-correcting codes. This system consists of fortuitously supplementing errors to a codeword and uses it as a cipher. The decryption is done by correcting inherent transmission errors. The security of the McEliece scheme depends on the difficulty of decoding a word without any knowledge of the structure of the code. Only the legitimate client can decode using the bait. Niederreiter uses a syndrome as ciphertext, and the message is an error pattern instead of a codeword [3]. The security of McEliece's and Niederreiter's systems is demonstrated to be equivalent from the viewpoint of complexity theory [38], and it is based on the following assumptions [15].

- It is difficult to sort out a type of the decoding problem.
- It is difficult to retrieve the essential construction of the code.

### 2.5. Cryptography for Blockchain

Information on the blockchain is stocked on the ledger using cryptography. Blockchain uses the public key cryptography, zero-knowledge proof, and hash functions. Especially, the blockchain technology is very important in the use of public key cryptography. It is used for digital signatures and encryption. The private key is saved in a digital wallet in blockchain. This wallet can be a hardware wallet, a physical apparatus to stock the private key, or any software wallet, e.g., a desktop wallet app or a mobile wallet app. An user attains its private key to sign a message with a digital signature that will be communicated to the blockchain, and then its public key is used to verify that the message indeed did come from the user. The user hashes its process output into hash value and then signs on the hash value with its private key to produce the digital signature. Then, the user transmits its digital signature with its process output to the blockchain networks. The receiver uses the user's public key to decrypt the received digital signature to reach the hash value $A$, and the receiver hashes the received process output to reach the other hash value $B$. Then, the receiver verifies if $A$ is equal to $B$ or not. If equal, the receiver confirms the user's process.

The corresponding digital signature guarantees the source of the process, since the private key is only saved by its owner. The algorithm ensures the digital signature on every process appertaining the person private key of each user. The public key and private key suit into blockchain as the spine of blockchain, and they are used to sign and verify processes that the user makes [39].

## 3. Proposed Digital Signature Scheme

In this section, we construct the digital signature scheme using $[n, k, 2t+1]$-code over $\mathbb{F}_q$. The phases of key generation, signature generation, and verification are given in the following.

### 3.1. Key Generation Phase

(1) Select a generator $k \times n$ matrix $G$ of a linear $[n, k, 2t+1]$-code $C$ over $\mathbb{F}_q$, where $t$ is the error correcting capability.
(2) Construct a parity-check $(n-k) \times n$ matrix $H$ from $G$ for the code $C$.
(3) Select any non-zero syndrome vector $h$, which has weight $t$ and dimension $(n-k)$.
(4) Select a random, non-singular $(n-k) \times (n-k)$ matrix $M$ over $\mathbb{F}_q$.
(5) Calculate $n \times (n-k)$ matrix $H' = H^T M$, where $H^T$ is denoted by the transpose of $H$.
(6) The public key is $(G, H, M^{-1})$.
(7) The private key is $(H', h)$.

### 3.2. Signature Generation Phase

(1) Randomly select message $m$, which is the vector dimension $n$ over $\mathbb{F}_q$ with weight $t$.
(2) Compute $c = mH' + h$, and $m$ is signed with the private key.
(3) Generate the signature $(m, c)$.
(4) Transmit to the blockchain the generating signature.

### 3.3. Verification Phase

The public key of blockchain is to confirm that the message did come from the user.
(1) Compute $c' = cM^{-1}$, where $M^{-1}$ is the inverse of $M$.
(2) Reach $m$ by syndrome decoding $c'$ in the code $C$. If it is the same, then the signature is valid, otherwise it is invalid. Verification is correct, since

$$w(hM^{-1}) = w(h), \tag{1}$$

and thus

$$c' = cM^{-1} = (mH' + h)M^{-1} = mH'M^{-1} + hM^{-1} \tag{2}$$

$$\Rightarrow cM^{-1} = mH^{T}MM^{-1} + hM^{-1} \tag{3}$$

$$\Rightarrow cM^{-1} = mH^{T} + hM^{-1} \tag{4}$$

$$\Rightarrow cM^{-1} - hM^{-1} = mH^{T}. \tag{5}$$

Thus, the method of syndrome decoding may be efficiently used.

**Example 1.** *Let $C$ be a $[5,2,3]$-code over $\mathbb{F}_2$ with generator matrix $G$ and parity-check matrix $H$, which are* $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$, $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$. $C = \{00000, 10110, 01011, 11101\}$.
*Select any non-singular matrix* $M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

The inverse of $M$ is $M^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. The syndromes and coset leaders of $C$ are the following table.

| Syndromes | Coset Leaders |
|---|---|
| (000) | (00000) |
| (110) | (10000) |
| (011) | (01000) |
| (100) | (00100) |
| (010) | (00010) |
| (001) | (00001) |
| (101) | (11000) |
| (111) | (10001) |

The number of different cosets of $C$ is

$$2^{5-2} = 2^3 = 8.$$

That is, there are eight syndrome vectors, which are $\{000, 110, 011, 100, 010, 001, 101, 111\}$.

Compute the matrix $H' = H^{T}M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

Select the syndrome vector $h$ is $(100)$. Since $d = 3$, $C$ can correct $t = 1$ error. Therefore, the public key is

$$(G, H, M^{-1}) = \left( \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right)$$

and the private key is

$$(H', h) = \left( \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, (110) \right).$$

**Signature:** Consider the message vector $m = (00100)$ and $h = (100)$. If the user wants to sign the message $m$, he/she will use the private key.

$$c = mH' + h = (00100). \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} + (100) =$$

$$(111) + (100) = (011).$$

The signed message $(m, c) = (00100, 011)$ is transmitted to the blockchain by an user. 181

**Signature verification:** The blockchain gets the signed message and computes

$$c' = cM^{-1} = (011). \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = (010)$$

using the public key. Since

$$c = mH' + h$$

and

$$H' = H^T M.$$

$c'$ is also equal to

$$c' = (mH' + h)M^{-1} = mH'M^{-1} + hM^{-1}$$
$$= mH^T MM^{-1} + hM^{-1}$$
$$\Rightarrow c' = mH^T + hM^{-1}.$$

Thus,

$$(010) = (m_1 m_2 m_3 m_4 m_5). \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$+(100). \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$(010) = (m_1 + m_3, m_1 + m_2 + m_4, m_2 + m_5) + (110)$$
$$(010) - (110) = (m_1 + m_3, m_1 + m_2 + m_4, m_2 + m_5)$$
$$(101) = (m_1 + m_3, m_1 + m_2 + m_4, m_2 + m_5).$$

The blockchain obtains the message $m = (00100)$ by solving the linear system. Hence, the signature is verified.

**Proposition 1.** *The size of the message is* $\log_q \binom{n}{t}(q-1)^t$.

**Proof.** The message is one of the $n$-$q$ tuple words of weight $t$. These are the integers between 1 and $\binom{n}{t}$ to the set of words of weight $t$ and length $n$. Thus, the size of the message is $\log_q \binom{n}{t}(q-1)^t$. □

**Proposition 2.** *The size of the signed message is* $(n-k)$.

**Proof.** By construction, the signed message is a $(n-k)$- $q$ tuple word. □

**Proposition 3.** *The size of the verification message is* $(n-k)$.

**Proof.** Since the verificated sign is a $(n-k)$- $q$ tuple word, the result holds. □

**Corollary 1.** *The transmission rate of the proposed system is*

$$\frac{\log_q \binom{n}{t}(q-1)^t}{(n-k)}.$$

**Proof.** The transmission rate is equal to the proportion of the size of the message to the size of the signed message. So, the transmission rate is

$$\frac{\log_q \binom{n}{t}(q-1)^t}{(n-k)}.$$

□

**Example 2.** *Let $C$ be an $[4,2,3]-$ MDS (Maximum Distance Separable) code over $\mathbb{F}_4$, whose packing radius is one. It is clear that $q = 2$. Now, we explain the magnitudes of digital signature algorithm based on $C$. The size of the message is*

$$\log_2 \binom{4}{1} = \log_2 4 = 2.$$

*The size of the signed message is $4 - 2 = 2$. Since the message has small magnitude, its cost is not expensive and is preferable. The transmission rate is*

$$\frac{\log_2 \binom{4}{1}}{(4-2)} = 1,$$

*which is the maximum possible value. Thus, this scheme is referred to as ideal [40].*

## 4. Results and Discussion

Digital signature is a mathematical method in the world of network security over the message in order to ensure integrity and non-repudiation. However, it has no forgeability.

- Forgeability: Only an user can produce his own signature [41].
- Integrity: The message should not be changed during transmission [42].
- Non-repudiation: An user who signed some documents cannot at a later time disclaim having signed it [43].

In this context, the security analysis for the proposed digital signature scheme is as below.

- Forgeability: The security of proposed scheme depends on the matrix $H'$ and vector $h$. The error-correction capability of private key $H'$ is unknown, and the value $h$ is hidden. It is computationally impossible to determine $H'$ and $h$. Thus, the complexity and security of the algorithm relies on decoding in the code $H'$.
- Integrity: The signature is valid only when the computed $c'$ and $c'$ sent along with the signature is the same. So, if any change is made on the signature that is transmitted, it cannot produce the same hash function of the message $H(m)$ and, thus, the signature is incorrect.
- Non-repudiation: The values $H'$ and $h$ ensure that only a signer can generate the valid signature. It summarizes the security analysis of proposed digital signature scheme in Table 1.

**Table 1.** Security Analysis of Proposed Digital Signature Scheme.

| | |
|---|---|
| Forgeability | No |
| Integrity | Yes |
| Non-repudiation | Yes |

The proposed digital signature scheme protects the integrity and is secure against forgeability. Only the signer has generated the signature regarding the use of the hash function value. This means it covers non-repudiation.

### *4.1. Cryptanalysis of the Proposed Scheme*

We analyze the security of proposed system in this section. We construct the digital signature scheme to use in blockchain technology, taking $[n, k, 2t + 1]$-code over $\mathbb{F}_q$. The verification of the signature is done by the bounded distance decoding method. The following terms should be performed to obtain a secure digital signature scheme.

- The signature length should be quite small. This magnitude is $k$, which is fairly small for our system.
- The phases of key generation, signature generation, and verification should be influential. It is computationally easy to construct the public key and private key. In the approached systems, these phases are very effective.
- It should be unfeasible to access the message by an attacker.
- The system should be durable for all possible attacks. We explain these arguments for the proposed systems.

#### 4.1.1. Algebraic Attack

In a digital signature scheme, since the message is signed with the private key, the security depends on the private key. Thus, the first attack will be to try to reach it. When computing $c$ in the signature process, the proposed scheme uses the procedure of installing the information signature into a matrix $H'$ on the code. The signer calculates the codeword $c = mH' + h$ using the private key. Then, he/she computes $c' = cM^{-1}$ and checks the message $m$ using the method of syndrome decoding. The security of equation $c' = cM^{-1}$ is guaranteed by syndrome decoding. This means the proposed scheme is secure.

#### 4.1.2. Generic Attack

The second attack is to access $m$ from $c$ without using the private key. Since the message is a $n$- $q$ tuple word of weight $t$, we need a practical method that maps the integers between 1 and $\binom{n}{t}$ to the set of words of weight $t$ and length $n$, as well as conversely. In this situation, an enemy cryptanalyst will try to choose $n$ bits from $(n - k)$- bit signed message randomly and estimate $m$ based on the $n$ chosen bits, which is unfeasible. Furthermore, the attacker cannot obtain the $H'$ and $h$ through the equation $c = mH' + h$, cannot obtain the signature $m$ through replacing the $h$ and $h'$, and thus it is impossible that the attacker

attempts to forge the signature by replacing the message. Hence, the proposed scheme can avoid forgery.

## 5. Comparison with Other Digital Signature Schemes

We compare our scheme with the other code-based digital signature schemes in this section. Consider a $[n, k, d]$-code $C$ over $\mathbb{F}_q$ with $d \geq 2t + 1$. As it is seen in Table 2, in the proposed scheme, solving an instance of the decoding problem is more difficult from McEliece's and Niederreiter's systems, since we are working in a wider space. Having short signatures ensures the resistance to the attacks. Thus, our approach provides the potential for an enhanced security, relative to existing schemes, and, subject to known attack scenarios that are currently and practically realizable.

**Table 2.** Comparison with the other schemes.

| Algorithm | Mathematical NP-Hard Problem | Signature Length | Verification Space |
|---|---|---|---|
| McEliece Scheme [2] | decoding of general codes | k | $(\mathbb{F}_2)^n$ |
| Niederreiter Scheme [3] | syndrome decoding problem | n-k | $(\mathbb{F}_2)^{n-k}$ |
| Feneuil et al. Scheme [27] | syndrome decoding problem | n | $(\mathbb{F}_2)^n$ |
| This paper | bounded distance decoding method | n-k | $(\mathbb{F}_q)^{n-k}$ |

In Table 2, we explain the complexity cost of signature generation and verification phase with regard to similar schemes. It is seen that the signature length and verification cost will always be enormously small. The McEliece scheme is based on error correcting codes. It operates by inserting errors to a codeword at random, and this is also a cipher. Since McEliece's and Feneuil's schemes have large key size, the efficiency of these schemes will be slower than the others. Both Niederreiter's schemes and the proposed schemes have small key size. Thus, these schemes are faster than McEliece's and Feneuil's schemes. However, the transmission rate of McEliece's is $\frac{\log_2 \binom{n}{t}}{k}$, Niederreiter's is $\frac{\log_2 \binom{n}{t}}{(n-k)}$, Feneuil's is $\frac{\log_2 \binom{n}{t}}{n}$, but, in the proposed scheme, this rate, as it is seen in Corollary 1, is $\frac{\log_q \binom{n}{t}(q-1)^t}{(n-k)}$, which is exponentially larger. The signing is faster than the other systems, as the transmission rate is bigger in the proposed system. Thus, the signature length and verification cost remain low. Moreover, Feneuil et al. [27] use zero-knowledge protocol to construct their schemes, but we are inspired by the McEliece approach.

One of the first digital signature schemes based on the algebraic properties of modular exponentiation is the ElGamal signature scheme. The ElGamal signature scheme, which requires a hash function $h : \{0, 1\}^* \to \mathbb{Z}_p$, where $p$ is a large prime, is based on the difficulty of solving of discrete logarithm problem defined over finite fields. The security of the system depends on maintaining on confidentiality of private key in ElGamal's scheme. The mathematical NP-hard problem of RSA is based on the integer factorization. When we compare to some known signature schemes as RSA [7] and ElGamal [8], the proposed scheme is more effective than the others.

RSA and ElGamal schemes do not well satisfy the request for high security, since they have a large public key. These schemes are also slower than the others. The RSA problem is the process of finding $e$-th roots modulo $N$, which is a hard problem. McEliece's disjunction problem is the problem of decoding an error correcting code. There is no effective systemic attack that might discriminate between an altered Goppa code used by McEliece and a random code. However, the RSA and McEliece schemes have resisted for more than 40 years against cryptanalysis attacks. RSA is preferable to McEliece's scheme of security.

Another important scheme is the elliptic curve digital signature algorithm [44]. The security of elliptic curve cryptosystems relies on the assumed hardness of the discrete logarithm problem in the group of points on the curve. Elliptic curve cryptography requires a comparatively brief encryption key—a value that must be nurtured into the encryption algorithm to decode an encrypted message. This short key is quicker to compute and necessitates smaller computational burden than other first-generation encryption public key algorithms. A 160-bit elliptic curve cryptography encryption key provides the same security as a 1024-bit RSA encryption key, and it is 15 times quicker, relying on the place on which it is performed. The advantages of elliptic curve cryptography over RSA are especially significant in wireless appliances, where computational power and memory are restricted. However, this raises the size of the encrypted message significantly more than RSA encryption. This is one of the fundamental disadvantages of elliptic curve cryptography. Moreover, the elliptic curve cryptography is more computationally complex to apply than RSA, which raises the possibility of application errors, thus decreasing the security of the algorithm. The proposed digital signature scheme based on the error correcting codes increases the security of the digital signature.

## 6. Conclusions

This paper proposed a new digital signature scheme based on error correcting codes that are suitable for blockchain technology. The signature verification is done by the bounded distance decoding method. The respective sizes of the message, of the signed message, and of the transmission rate, have been computed. The security has been analyzed, and some attacks have been considered. The comparison with other digital signature schemes in the literature shows the benefits of proposed approach.

In the proposed system, since the signature length is small, it is more practical in industry. Another advantage of this system is high transmission rate. In this way, the signature length and verification cost remain low. Moreover, the proposed digital signature ensures that transactions in the public sector, such as health, education, and taxation, are carried out quickly and reliably on the internet.

**Author Contributions:** Investigation: A.A., A.N.K., M.A.R., V.A., and P.S., supervision: S.Ç. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research work was funded by Institutional Fund Projects under grant number (IFPRC-105-130-2020). Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *IT-22*, 644–654.
2. McEliece, R.J. *A Public-Key Cryptosystem Based on Algebraic Coding Theory*; DSN Progress Report; Jet Propulsion Labaratory: Pasadena, CA, USA, 1978; pp. 42–44.
3. Niederreiter, H. Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control. Inf. Theory* **1986**, *15*, 159–166.
4. Çalkavur, S. Public-key cryptosystems and bounded distance decoding of linear codes. *Entropy* **2022**, *22*, 498–508.
5. Groetsema, A.; Sahdev, N.; Salami, N.; Schwentker, R.; Cionca, F. *Blockchain for Business: An Introduction to Hyperledger Technologies, The Linux Foundation: 2019, California, the United States of America.*
6. Digital Signature Algorithm Analysis and Hash Signature. 2005. Available online: http://www.upsdn.net/html (accessed on 1 January 2005).
7. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *26*, 96–99.
8. El Gamal, T.E. A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472.
9. Lidl, R.; Mullen, G.L.; Turnwald, G. *Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics 65*; Willey: New York, NY, USA, 1993.
10. Nöbauer, W. Cryptanalysis of a public-key cryptosystem based on Dickson polynomials. *Math. Slovaca* **1989**, *38*, 309–323.

11. Smith, P. LUC public-key encryption. *Dr. Jobb's J.* Vol. 18, No. 1, pp. 44-49. **1993**.
12. Smith, P.; Skinner, C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. In Proceedings of the Advances in Cryptology—ASIACRYPT'94: 4th International Conferences on the Theory and Applications of Cryptology, Wollongong, Australia, 28 November–1 December 1994; pp. 298–306.
13. Koblitz, N. An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm. In *Conference Paper, Part of the Lecture Notes in Computer Science Book Series (LNCS, Volume 1462), Proceedings of the Annual Inernational Cryptology Conference CRYPTO 1998: Advances in Cryptology-CRYPTO'98, Santa Barbara, CA, USA, 23–27 August 1998*; Springer: Berlin/Heidelberg, Germany; pp. 327–338.
14. Elhabob, R.; Adel, A.; Omer, M.; Eshaush, H. Survey on NP-Hard Problems of Digital Signature Schemas. *Int. J. Eng. Res. Technol. (IJERT)* **2014**, *3*, pp. 722-727, DOI: 10.17577/IJERTV3IS110591, ISSN: 2278-0181.
15. Courtois, N.T.; Finiasz, M.; Sendrier, N. How to Achieve a McEliece-Based Digital Signature Scheme. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2001: Advances in Cryptology, Gold Coast, Australia, 9–13 December 2001; pp. 157–174.
16. Faugére, J.C.; Otmani, A.; Perret, L.; Tillich, J.-P. A distinguisher for high rate McEliece cryptosystems. In Proceedings of the IEEE Information Theory Workshop (ITW), Paraty, Brazil, 16–20 October 2011; pp. 282–286.
17. Baldi, M.; Bianchi, M.; Chiaraluce, F.; Rosenthal, J.; Schipani, D. Using LDGM codes and sparse syndromes to achieve digital signatures. In *Post-Quantum Cryptography*; Gaborit, P., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1–15.
18. Phesso, A.; Tillich, J.-P. An efficient attack on a code-based signature scheme. In *Post-Quantum Cryptography*; Takagi, T., Ed.; Springer International Publishing: Cham, Switzerland, 2016; pp. 86–103.
19. Persichetti, E. Efficient one-time signatures from quasi-cyclic codes: A full treatment. *Cryptography* **2018**, *2*, 4.
20. Kuznetsov, A.; Pushkar'ov, A.; Kiyon, N.; Kuznetsova, T. Code-based electronic digital signature. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems Services and Technlogies (DESSERT), Ukraine, Kyiv, 24–27 May 2018; pp. 331–336.
21. Kuznetsov, A.; Kiian, A.; Pushkar'ov, A.; Mialkovskyi, D.; Smirnov, O.; Kuznetsova, T. Code-Based Schemes for Post-Quantum Digital Signatures. In Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 18–21 September 2019; Volume 2, pp. 707–712.
22. Kuznetsov, A.; Kiian, A.; Babenko, V.; Perevozova, I.; Chepurko, I.; Smirnov, O. New Approach to the Implementation of Post-Quantum Digital Signature Scheme. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; pp. 166–171.
23. Gueron, S.; Persichetti, E.; Santini, P. Designing a Practical Code-Based Signature Scheme from Zero-Knowledge, Proofs with Trusted Setup. *Cryptography* **2022**, *6*, 5.
24. Biasse, J.F.; Micheli, G.; Persichetti, E.; Santini, P. LESS is More: Code-Based Signatures without Syndromes. In *AFRICACRYPT*; Nitaj, A., Youssef, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 21–51.
25. Barenghi, A.; Biasse, J.F.; Persichetti, E.; Santini, P. *LESS-FM: Fine-Tuning Signatures from a Code-Based Cryptographic Group Action, Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings*. pp. 23–43.
26. Baldi, M.; Battaglioni, M.; Chiaraluce, F.; Horlemann-Trautmann, A.L.; Persichetti, E.; Santini, P.; Weger, V. A new path to code-based signatures via identification schemes with restricted errors. *arXiv* **2020**, arXiv:2008.06403.
27. Feneuil, T.; Joux, A.; Rivain, M. Shared Permutation for Syndrome Decoding: New-Zero Knowledge Protocol and Code-Based Signature, Cryptology ePrint Archive: Report 2021/1576. Available online: https://eprint.iacr.org/2021/1576 (accessed on 9 December 2021).
28. Wang, Y.; Xie, H.; Wang, R. Digital Signature Scheme to Match Generalized Reed-Solomon Code over $GF(q)$. In Proceedings of the Cyberspace Safety and Security: 14th International Symposium, CSS 2022, Xi'an, China, 16–18 October 2022; pp. 32–47.
29. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717.
30. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375.
31. Chaum, D. Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups. Ph.D. Thesis, University of California, Berkeley, CA, USA, 1982.
32. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111.
33. Bayer, D.; Haber, S.; Stornetta, W.S. Improving the efficiency and reliability of digital time-stamping. In *Sequences II*; Capocelli, R., Santis, A.D., Vaccaro, U., Eds.; Springer: New York, NY, USA, 1993.
34. Nokamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. October 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 1 March 2009).
35. Buterin, V. Ethereum Whitepaper. 2013. Available online: https://ethereum.org/en/whitepaper/ (accessed on 1 January 2013).
36. Hill, R. *A First Course in Codig Theory*; Oxford University: Oxford, UK, 1986.
37. Lint, J.H.V. *Introduction to Coding Theory*; Springer: Berlin/Heidelberg, Germany, 1992. https://doi.org/10.1007/978-3-662-00174-5.

38. Li, Y.X.; Deng, R.H.; Wang, X.M. On the equivalence of McEliece's and Niederreiter's public-key cyptosystems. *IEEE Trans. Inf. Theory* **1994**, *40*, 271–273.
39. Guo, H.; Yu, X. A Survey on blockchain technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067.
40. Yılmaz, R. Some Ideal Secret Sharing Schemes. Mater's Thesis, Bilkent University, Ankara, Turkey, 2010.
41. Tianhuang, C.; Xiaoguang, X. Digital Signature In The Application Of E-Commerce Security. In Proceedings of the 2010 IEEE International Conference on E-Health Networking, Digital Ecosystems and Technologies, Shenzhen, China, 17–18 April 2010.
42. Eliza, P. *What Is Digital Signature—How It Works, Benefits, Objectives, Concept*; EMP Trust HR: Gaithersburg, MD, USA, 12 September 2017.
43. Dawn, T. Major Standards and Compliance of Digital Signatures—A World-Wide Consideration, Cryptomathic, online resource, https://www.cryptomathic.com/news-events/blog/major-standards-and-compliance-of-digital-signatures-a-world-wide-consideration, 7 January 2016.
44. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63.