The ISC Int'l Journal of Information Security

ISeCure

November 2023, Volume 15, Number 3 (pp. 101–108)

http://www.isecure-journal.org

PRESENTED AT THE ISCISC'2023 IN TEHRAN, IRAN.

Post Quantum Digital Signature Based on the McEliece Cryptosystems with Dual Inverse Matrix **

Farshid Haidary Makoui [1], Thomas Aaron Gulliver [1], and Mohammad Dakhilalian [2,*]

[1] *Department of Electrical and Computer Engineering, University of Victoria, Victoria, B.C., Canada*

[2] *Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran*

ARTICLE INFO.

Keywords:
Cryptography, Code-Based Cryptosystem, Coding Theory, Digital Signature, Public Key Cryptography (PKC)

Type:
Research Article

doi: 10.22042/isecure.2023.419559.1026

ABSTRACT

Digital signatures are used to ensure legitimate access through identity authentication. They are also used in blockchains and to authenticate transactions. Code-based digital signatures are not widely used due to their complexity. This paper presents a new code-based signature algorithm with lower complexity than existing methods and a high success rate. The key generation algorithm constructs three-tuple public keys using a dual inverse matrix. The proposed signing scheme is based on the McEliece cryptosystem. It includes an integrity check to mitigate forgery before verification.

1 Introduction

Traditional cryptographic algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC) rely on mathematical problems that are difficult to solve with classical computers. However, quantum computers have the potential to solve mathematical problems such as factoring large numbers exponentially faster than classical computers. The goal of post-quantum cryptography [1] is to develop cryptographic algorithms that are secure even when attacked using quantum computers [2–4]. These algorithms are based on problems that are believed to be hard even for quantum computers to solve. Post-quantum cryptographic schemes have been developed based on error correcting codes, lattices, and multivariate polynomials.

The first code-based cryptosystem was introduced by McEliece [5]. To date, there is no attack that can break this cryptosystem in polynominal time [6]. However, code-based signatures are not widely used. One reason is that the ciphertexts do not cover the entire vector space [7, 8]. For example, on average it takes $t!$ executions of the Courtois-Finiasz-Sendrier (CFS) construction to obtain a valid signature [9]. In [10], a signature scheme based on the McEliece cryptosystem was proposed that covers the entire vector space. This results a higher success rate and thus a lower processing time for signature generation. A random parity check matrix inverse is employed which is difficult to determine by an adversary. In particular, the probability of constructing a specific inverse matrix is $2^{-k(n-k)}$ which is negligible if the parameters are chosen appropriately [10].

In this paper, a dual matrix A is employed which is both the inverse and transpose of the parity check matrix. This matrix is used to develop signing and verification schemes. In addition, a key generation algorithm is given to construct public and private

* Corresponding author.

**The ISCISC'2023 program committee effort is highly acknowledged for reviewing this paper.

Email addresses: makoui@uvic.ca, agullive@ece.uvic.ca, mdalian@iut.ac.ir

ISSN: 2008-2045

keys.

1.1 The McEliece Cryptosystem

A binary linear block code generates a codeword $c = (c_1, c_2, \ldots, c_n)$ for a message $m = (m_1, m_2, \ldots, m_k)$, so there are 2^k distinct codewords. The set of codewords is referred to as a $C(n, k)$ block code with length n and dimension k, $k \leq n$. A $C(n, k)$ linear code forms a k-dimensional subspace of the n-dimensional vector space. A set of k linearly independent codewords $g_1, g_2, \ldots, g_k$ forms a generator matrix G of the code. For any $C(n, k)$ block code, there is a dual code $C^{\perp}$ which is an $n - k$ dimensional vector subspace with generator matrix H. The matrix H is called a parity check matrix of $C(n, k)$ and is an $(n - k) \times n$ matrix such that $GH^T = 0$ where ^{T} denotes transpose.

The McEliece cryptosystem employs a code $C(n, k)$ with generator matrix $G_{k \times n}$, a scrambling matrix $S_{k \times k}$, and a permutation matrix $P_{n \times n}$. The public key is $pk = SGP$ while the private key is $pr = (S, G, P)$. In this cryptosystem, plaintext bits are scrambled and the corresponding codeword is permuted. Then up to t bits are flipped where t is the error correcting capability of the code.

The encryption algorithm is as follows.

1. For a plaintext m of length k bits, Alice employs Bob's public key to encode it as $c = mSGP$.
2. Alice generates a random error vector e of length n and Hamming weight no greater than t and adds it to c to obtain the ciphertext

$$c' = c + e = mSGP + e \qquad (1)$$

The decryption algorithm is as follows.

1. Multiply c' by the inverse of P

$$c'P^{-1} = (mSGP + e)P^{-1} = mSG + eP^{-1} \qquad (2)$$

2. As P is a permutation matrix, $P^{-1} = P^T$ is also a permutation matrix. Therefore, eP^{-1} is a vector with the same Hamming weight as e, so $c'P^{-1}$ can be decoded to obtain mS.
3. Multiply mS by S^{-1} to obtain the plaintext m.

2 Proposed Code-Based Digital Signature Scheme

The proposed code-based digital signature scheme is a probabilistic algorithm for key generation, signing, and verification. The dual matrix A described below is used in the key generation, signing, and verification algorithms.

2.1 Dual Matrix A

The proposed algorithm generates a three-tuple public key based on a matrix that functions as both H^T and H^{-1} so that $HA = I_{n-k}$ and $GA = 0$. Then

$$GA = 0 \text{ and } GH^T = 0$$

so $A = H^T P'$ and we have

$$HA = H(H^T P') = (HH^T)P' = I_{n-k}.$$

Thus, $P' = (HH^T)^{-1}$ so A can be constructed only if the $(n - k) \times (n - k)$ matrix HH^T is non-singular.

2.2 Key Generation

The key generation algorithm provides public and private keys using the generator matrix G of the code $C(n, k)$ and the dual matrix A which satisfy

$$GA = 0 \text{ and } HA = I_{n-k} \qquad (3)$$

The following matrices are used by the key generation algorithm:

1. A $k \times n$ generator matrix G
2. An $(n - k) \times n$ parity check matrix H
3. An $n \times (n - k)$ dual matrix A
4. A $k \times k$ scrambling matrix S
5. An $n \times n$ permutation matrix P
6. An $(n - k) \times (n - k)$ non-singular matrix L

Algorithm 1 Key Generation

1. Given a generator matrix G for $C(n, k)$ with non-singular HH^T and $A = H^T P'$.
2. Construct $P' = (HH^T)^{-1}$.
3. As in the McEliece cryptosystem, use the generator matrix G, the scrambling matrix S, and the permutation matrix P to mask G,

$$pk_1 = G' = SGP.$$

4. Use the non-singular matrix L and P to mask H

$$pk_2 = L^{-1}HP$$

5. Verification of a digital signature requires

$$pk_3 = P^{-1}AHP$$

6. Construct a parity check matrix H' corresponding to $G' = SGP$

$$Q = H'^T = ((AL)^T (P^{-1})^T)^T = P^{-1}AL$$

7. Public and private keys: $pk \leftarrow (pk_1, pk_2, pk_3)$ and $pr \leftarrow (S^{-1}, P^{-1}, G, Q)$

The generator matrix G and parity check matrix H are masked using a random non-singular scrambling matrix S and a random permutation matrix P, respectively, and the dual matrix A is masked using a random non-singular matrix L and P. The verification algorithm uses pk_3 to validate the digital signatures, and ensure their integrity and authenticity.

Theorem 1. *The public key $pk = (pk_1, pk_2, pk_3)$ satisfies the following*

(1) $pk_1 pk_3 = 0$
(2) $pk_2 pk_3 = pk_2$
(3) $pk_3 pk_3 = pk_3$

Proof. For the first item, we have

$$\begin{aligned} pk_1 pk_3 &= SGP(P^{-1}AHP) \\ &= S(GA)HP \\ &= 0. \end{aligned}$$

For the second item, we have

$$\begin{aligned} pk_2 pk_3 &= (L^{-1}HP)(P^{-1}AHP) \\ &= L^{-1}(HA)HP \\ &= L^{-1}HP \\ &= pk_2. \end{aligned}$$

For the third item, we have

$$\begin{aligned} pk_3 pk_3 &= (P^{-1}AHP)(P^{-1}AHP) \\ &= P^{-1}(AH)(AH)P \\ &= P^{-1}A(HA)HP \\ &= P^{-1}AHP \\ &= pk_3. \end{aligned}$$

□

The following theorem provides the relationship between the private and public keys.

Theorem 2. *The public key $pk = (pk_1, pk_2, pk_3)$ and private key Q are related as follows:*

(1) $pk_1 Q = 0$
(2) $pk_2 Q = I$
(3) $pk_3 Q = Q$

Proof. For the first item, we have

$$\begin{aligned} pk_1 Q &= (SGP)(P^{-1}AL) \\ &= S(GA)L \\ &= 0. \end{aligned}$$

For the second item, we have

$$\begin{aligned} pk_2 Q &= (L^{-1}HP)(P^{-1}AL) \\ &= L^{-1}(HA)L \\ &= I. \end{aligned}$$

For the third item, we have

$$\begin{aligned} pk_3 Q &= (P^{-1}AHP)(P^{-1}AL) \\ &= P^{-1}A(HA)L \\ &= P^{-1}AL \\ &= Q. \end{aligned}$$

□

Theorem 3. *The public key $L^{-1}HP$ has many inverses and the probability of constructing a particular inverse of $L^{-1}HP$ can be made negligible.*

Proof. The parity check matrix is a full rank matrix and is not unique [11]. The inverse of this matrix has $n-k$ columns, each of which can have 2^k different values, so the number of inverse matrices is $2^{k\times(n-k)}$ [11]. The public key $L^{-1}HP$ is a full rank matrix, so the probability of constructing a particular inverse of $L^{-1}HP$ is $\frac{1}{2^{k\times(n-k)}}$ which is negligible for appropriate values of n and k. □

2.3 Signing algorithm

The proposed signature scheme uses both keys to sign a document as follows.

Algorithm 2 Signing

1. Hash document *doc*, and hash the result to n bits
   $h(doc) \leftarrow$ hash document *doc*
   $h(h(doc)) \leftarrow$ hash $h(doc)$
2. Let s be the $n-k$ bit vector given by
   $s \leftarrow h(doc)(Q)$
3. Compute $sigSGP \leftarrow h(doc) + s(pk_2)$
4. Decode the codeword c to obtain sig
   $sigSG \leftarrow (sigSGP)(P^{-1})$
   $sigS \leftarrow$ decode $sigSG$
   $sig \leftarrow (sigS)(S^{-1})$
5. Construct the $n-k$ bit vector d
   $d \leftarrow h(h(doc))(Q) + s$
6. Output (sig, d) and document *doc*

Theorem 4. *$h(doc) + s(pk_2)$ is a valid codeword of the code $C(n,k)$ with generator matrix $G' = SGP$.*

Proof. Matrices S and P have full rank as they are non-singular. Therefore, the rank of SGP is k and the rank of $P^{-1}AL$ is $n-k$. Since the row vectors of SGP and column vectors of $P^{-1}AL$ are orthogonal, $P^{-1}AL$ generates the nullspace of the code generated by SGP. Hence, the transpose of $P^{-1}AL$ is a parity check matrix corresponding to SGP. □

For a codeword $c \in C(n,k)$ we have $c(H')^T = 0$. The corresponding generator matrix is $G' = SGP$ and $(H')^T = P^{-1}AL$ so

$$c = sigSGP = h(doc) + s(pk_2).$$

The vector s is equal to $h(doc)(Q)$

$$\begin{aligned} sigSGP &= h(doc) + h(doc)(Q)(pk_2), \\ sigSGP &= h(doc) + h(doc)(pk_3). \end{aligned}$$

Therefore

$$\begin{aligned} c(H')^T &= sigSGP(Q) \\ &= h(doc)(Q) + h(doc)(pk_3)(Q) \\ &= h(doc)(Q) + h(doc)(Q) \\ &= 0. \end{aligned}$$

2.4 Verification algorithm

The verification algorithm ensures the authenticity and integrity of the signature.

Algorithm 3 Verification Algorithm

1. Use the hash function $h()$ to hash the received document to construct $h(doc)$ and $h(h(doc))$

$$a \leftarrow sigSGP$$

2. Use the public key and d to obtain $v_1 = s(pk_2)$ which is an n-bit vector

$$v_1 \leftarrow s(pk_2) = h(h(doc))(pk_3) + d(pk_2)$$
$$d = h(h(doc))(Q) + s$$
$$d(pk_2) = (h(h(doc))(Q) + s)(pk_2)$$
$$d(pk_2) = h(h(doc))(Q)(pk_2) + s(pk_2)$$

so

$$v_1 = s(pk_2) = h(h(doc))(pk_3) + d(pk_2) \quad (4)$$

3. Use the public key (pk_3) to obtain $v_2 = s(pk_2)$ which is an n-bit vector

$$v_2 \leftarrow s(pk_2) = h(doc)(pk_3)$$
$$sigSGP = h(doc) + s(pk_2)$$
$$s(pk_2) = sig(pk_1) + h(doc)$$
$$s(pk_2)(pk_3) = sig(pk_1)(pk_3) + h(doc)(pk_3)$$

so

$$v_2 = s(pk_2) = h(doc)(pk_3) \quad (5)$$

4. The integrity condition is satisfied if

$$v_1 = v_2$$

otherwise, verification fails.

5. Use $v_1 = s(pk_2)$ and $h(doc)$ to compute

$$c \leftarrow h(doc) + s(pk_2)$$

6. Verification is successful if $a = c$, otherwise it fails.

Changes made by an adversary should be detected by the verification algorithm. The integrity condition in step 4 checks the validity of the signature. Note that v_1 does not depend on the signature sig and v_2 does not depend on the private key, but the integrity condition is satisfied if $v_1 = v_2$.

2.5 An Example

Consider the following matrix with $n = 12$ and $k = 5$:

$$G = \begin{pmatrix} & | & 1\,0\,0\,1\,0\,1\,1 \\ & | & 0\,1\,0\,0\,1\,0\,0 \\ I_k & | & 0\,0\,1\,1\,1\,1\,1 \\ & | & 0\,1\,0\,1\,0\,1\,0 \\ & | & 1\,1\,0\,1\,0\,0\,1 \end{pmatrix}, H = \begin{pmatrix} 1\,0\,0\,0\,1 & | & \\ 0\,1\,0\,1\,1 & | & \\ 0\,0\,1\,0\,0 & | & \\ 1\,0\,1\,1\,1 & | & I_{n-k} \\ 0\,1\,1\,0\,0 & | & \\ 1\,0\,1\,1\,0 & | & \\ 1\,0\,1\,0\,1 & | & \end{pmatrix}$$

The dual inverse matrix A, non-singular matrix L, scrambling matrix S, and permutation matrix P are

$$A_{n\times(n-k)} = \begin{pmatrix} 0&1&1&0&1&0&1 \\ 0&1&0&1&0&1&0 \\ 0&0&0&1&0&0&0 \\ 1&1&1&0&0&0&0 \\ 1&1&1&0&1&1&0 \\ 0&0&0&0&0&1&1 \\ 0&0&0&1&1&0&0 \\ 0&0&1&1&0&0&0 \\ 0&1&1&0&0&1&1 \\ 0&1&0&0&1&1&0 \\ 1&0&0&1&1&1&1 \\ 1&0&0&1&0&1&0 \end{pmatrix},$$

$$L = \begin{pmatrix} 1&0&1&0&1&1&1 \\ 0&0&0&1&0&0&1 \\ 1&1&0&0&1&0&0 \\ 1&0&1&0&0&0&0 \\ 0&1&0&0&1&0&1 \\ 0&0&0&1&0&1&1 \\ 1&0&0&1&0&0&1 \end{pmatrix}, S = \begin{pmatrix} 0&1&0&0&0 \\ 1&0&1&1&0 \\ 0&1&1&1&0 \\ 0&0&1&0&1 \\ 1&1&0&0&1 \end{pmatrix},$$

$$P_{n\times n} = \begin{pmatrix} 0&0&0&0&0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0&0&0 \end{pmatrix}.$$

Alice generates the signature as follows.

1. Use the hash function $h()$ with the document doc to obtain
$$\begin{aligned} h(doc) &= 100110010001, \\ h(h(doc)) &= 110001110111. \end{aligned}$$
2. Construct the $(n-k)$-bit vector $s = h(doc)Q$
$$s = 0101111.$$
3. Construct a codeword $h(doc) + s(pk_2)$ of the code $C(n, k)$
$$\begin{aligned} c &= sigSGP = h(doc) + s(pk_2) \\ &= 100110010001 + (0101111)(pk_2) \\ &= 100110010001 + 000110110010 \\ &= 100000100011. \end{aligned}$$
4. Decode the codeword to obtain
$$sig = 01010.$$
5. Use Q and s to obtain
$$\begin{aligned} d &= h(h(doc))Q + s \\ &= (110001110111)(P^{-1}AL) + 0010111 \\ &= 1000110 + 0010111 \\ &= 1101001. \end{aligned}$$
6. Output (sig, d) along with the document doc.

Bob verifies the signature as follows.

1. Use the hash function $h()$ and the received document to obtain
$$\begin{aligned} h(doc) &= 100110010001, \\ h(h(doc)) &= 110001110111, \end{aligned}$$
$$a = sigSGP = (0000110)(SGP) = 100000100011.$$
2. Use Alice's public key and d to compute
$$\begin{aligned} v_1 &= h(h(doc))(pk_3) + d(pk_2) \\ &= 110001110111(pk_3) + 1101001(pk_2) \\ &= 110111000110 + 110001110100 \\ &= 000110110010. \end{aligned}$$
3. Use Alice's public key to compute $v_2 = s(L^{-1}HP)$
$$\begin{aligned} v_2 &= h(doc)(pk_3) \\ &= 100110010001(pk_3) \\ &= 000110110010. \end{aligned}$$
4. Check the integrity condition $v_1 = v_2$. If it is met, continue, otherwise verification is failed.
5. Use $v_1 = s(pk_2)$ and $h(doc)$ to compute
$$\begin{aligned} c &= h(doc) + s(pk_2) \\ &= 100110010001 + 000110110010 \\ &= 10000010011. \end{aligned}$$
6. Verification is successful as $a = c$.

3 Performance and Security Analysis

The size of the public and private keys in the McEliece cryptosystem is $(n+k)^2$ [11]. The size of pk_1, pk_2, and the private keys in the proposed cryptosystem is $3n^2 + k^2$ [12]. Including pk_3 gives the total key size $4n^2 + k^2$. Table 1 shows that for $n = 1024$ and $k = 524$, the total key size for the McEliece cryptosystem is 292.5 kB, and with $n = 256$ and $k = 128$ [12] the total key size for the proposed cryptosystem is 34.0 kB.

The size of the signature and the speed of the signing process are the main factors that influence the choice of a digital signature algorithm. Speed is important for applications such as online banking, e-commerce, and blockchains (Bitcoin, Ethereum). On average, the CFS code-based signature schemes require $t!$ executions to obtain a valid signature [13], so the speed is proportional to the error correcting capability of the code. Table 2 compares the success rate and signature size of the proposed and lattice-based schemes. This shows that the proposed scheme has the smallest signature size and the highest success rate.

Adversaries use attacks on algorithms to gain access to documents and steal information [17]. To prevent attacks, the proposed algorithm masks the generator matrix using the permutation and scrambling matrices. Verification of a forged document signed by an adversary should fail [18] and the probability

Table 1. Key size comparison (kB)

Scheme	McEliece	Proposed
Public Key	65.5	16.0
Private Key	227.0	18.0
Public and Private Keys	292.5	34.0

Table 2. Signature size comparison

Scheme	Security (bits)	Success rate	Signature size (kB)
Bliss-IV [14]	192	0.19	6656
qTeslaIII [15][16]	256	1	2848
proposed $n = 256$	128	1	32
proposed $n = 512$	256	1	64

of constructing the private key from the public key should be negligible.

Consider a structural attack to construct the private key from the public key. The challenger provides an adversary with access to input any selected document and obtain a valid signature. Then the adversary uses their private key Q_{adv} to sign a document and produce (sig, d) to be verified by the challenger. The challenger uses the verification algorithm and at step 4 checks the integrity condition $v_1 = v_2$. The algorithm steps give

$$d = h(h(doc))(Q) + s,$$
$$d(pk_2) = (h(h(doc))(Q) + s)(pk_2),$$
$$d(pk_2) = h(h(doc))(Q)(pk_2) + s(pk_2).$$

Therefore, $(Q)(pk_2) = (pk_3)$ so

$$v_1 \leftarrow s(pk_2) = h(h(doc))(pk_3) + d(pk_2) \tag{6}$$

and hence $v_1 = s(pk)$ does not depend on the signature sig. Further

$$sigSGP = h(doc) + s(pk_2),$$
$$s(pk_2) = sig(pk_1) + h(doc),$$
$$s(pk_2)(pk_3) = sig(pk_1)(pk_3) + h(doc)(pk_3).$$

From Theorem 1, $(pk_1)(pk_3) = 0$ and $(pk_2)(pk_3) = pk_2$, so

$$v_2 \leftarrow s(pk_2) = h(doc)(pk_3). \tag{7}$$

Thus, $v_2 = s(pk_2)$ does not depend on the adversary private key Q_{adv}. The condition $v_1 = v_2$ gives

$$h(doc)(pk_3) = h(h(doc))(pk_3) + d(pk_2). \tag{8}$$

The left side can be expressed as $(h(doc)(P^{-1}AHP))$ and is independent of Q_{adv}, while d on the right side is constructed using Q_{adv} during the signing process.

We have

$$d = h(h(doc))Q_{adv} + h(doc)Q_{adv},$$
$$d(pk_2) = h(h(doc))(Q_{adv})(pk_2) + h(doc)(Q_{adv})(pk_2),$$
$$d(pk_2) = (h(h(doc)) + h(doc))(Q_{adv})(pk_2), \tag{9}$$

and (8) and (9) give

$$pk_3 = Q_{adv}pk_2,$$
$$P^{-1}AHP = Q_{adv}(L^{-1}HP).$$

Based on Theorem 2, this is satisfied if and only if $Q_{adv} = Q$.

Consider that an adversary selects $(L^{-1}H''P)^{-1}$ as their private key. Then

$$\begin{aligned}(Q_{adv})(pk_2) &= (L^{-1}H''P)^{-1}(L^{-1}HP)\\ &= (H''P)^{-1}(L)(L^{-1})(HP)\\ &= P^{-1}(H'')^{-1}HP\end{aligned}$$

so if $(H'')^{-1} = A$, $Q_{adv}pk_2$ is equal to $pk_3 = P^{-1}AHP$ and the signed document can be verified successfully, i.e. the adversary has succeeded in forging a signature.

An algorithm is considered secure if the probability of a successful attack is negligible [19, 20]. The parity check matrix H has full rank and dimensions $(n-k)\times n$, so H'' is also full rank with the same dimensions. From Theorem 3, the probability of $(L^{-1}HP)^{-1} = (L^{-1}H''P)^{-1}$ is $2^{-k\times(n-k)}$. Therefore, the probability of constructing the private key from the public key is negligible for appropriate values of n and k. Hence, the proposed digital signature algorithm is secure against structural attacks.

4 Conclusion

The CFS digital signature scheme has drawbacks which limit its use in practical applications. For example, the ciphertexts only cover part of the vector space so on average $t!$ executions are required to obtain a valid signature. A code-based digital signature scheme was proposed which overcomes this problem. Further, it includes a verification process to ensure the integrity and authenticity of the signatures. The proposed signature algorithm is safe against structural attacks as the probability of constructing the private key from the public key is negligible. Moreover, it is faster than existing code-based signature algorithms and has a small key size.

References

[1] Marco Baldi. Post-quantum cryptographic schemes based on codes. In *2017 International Conference on High Performance Computing & Simulation (HPCS)*, pages 908–910. IEEE, 2017.

[2] Kil-Hyun Nam. Private-key algebraic-coded cryptosystems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 35–48. Springer, 1986.

[3] Reza Hooshmand and Mohammad Reza Aref. Efficient secure channel coding scheme based on low-density lattice codes. *IET Communications*, 10(11):1365–1373, 2016.

[4] TRN Rao. Joint encryption and error correction schemes. *ACM SIGARCH Computer Architecture News*, 12(3):240–241, 1984.

[5] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[6] Nicolas Sendrier. Code-based cryptography: State of the art and perspectives. *IEEE Security & Privacy*, 15(4):44–50, 2017.

[7] Pierre-Louis Cayrel and Mohammed Meziani. Post-quantum cryptography: Code-based signatures. In *International Conference on Advanced Computer Science and Information Technology*, pages 82–99. Springer, 2010.

[8] Wang Xinmei. Digital signature scheme based on error-correcting codes. *Electronics Letters*, 26(13):898–899, 1990.

[9] Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a mceliece-based digital signature scheme. In *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, pages 157–174. Springer, 2001.

[10] Farshid Haidary Makoui, Thomas Aaron Gulliver, and Mohammad Dakhilalian. A new code-based digital signature based on the mceliece cryptosystem. *IET Communications*, pages 1199–1207, 2023.

[11] Mostafa Esmaeili. *Application of linear block codes in cryptography*. PhD thesis, 2019.

[12] Farshid Haidary Makoui, T Aaron Gulliver, and Mohammad Dakhilalian. Post quantum code-based cryptosystems with dual inverse matrix. In *2023 13th International Conference on Information Technology in Asia (CITA)*, pages 43–47. IEEE, 2023.

[13] Matthieu Finiasz. Parallel-cfs: Strengthening the cfs mceliece-based signature scheme. In *Selected Areas in Cryptography: 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers 17*, pages 159–170. Springer, 2011.

[14] Thomas Pöppelmann, Léo Ducas, and Tim Güneysu. Enhanced lattice-based signatures on reconfigurable hardware. In *Cryptographic Hardware and Embedded Systems–CHES 2014: 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings 16*, pages 353–370. Springer, 2014.

[15] James Howe, Thomas Pöppelmann, Máire O'neill, Elizabeth O'sullivan, and Tim Güneysu. Practical lattice-based digital signature schemes. *ACM Transactions on Embedded Computing Systems (TECS)*, 14(3):1–24, 2015.

[16] Dipayan Das, Jeffrey Hoffstein, Jill Pipher, William Whyte, and Zhenfei Zhang. Modular lattice signatures, revisited. *Designs, Codes and Cryptography*, 88:505–532, 2020.

[17] Thammavarapu RN Rao and Kil-Hyun Nam. Private-key algebraic-coded cryptosystems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 35–48. Springer, 1986.

[18] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing*, 17(2):281–308, 1988.

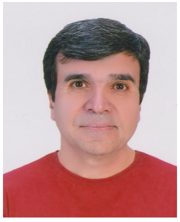
[19] Denis Diemert, Kai Gellert, Tibor Jager, and Lin Lyu. More efficient digital signatures with tight multi-user security. In *IACR International Conference on Public-Key Cryptography*, pages 1–31. Springer, 2021.

[20] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1):1–61, 2009.

Farshid Haidary Makoui received his B.Sc. degree in Electrical and Computer Engineering from Tehran Azad University in 1997. Currently, he is pursuing a Ph.D. at the University of Victoria, focusing on research in the field of post-quantum cryptography. Since 2019, he has been teaching Network Security at Toronto Metropolitan University as part of the computer network graduate program within the Faculty of Engineering and Architectural Science (FEAS). In 2003, he achieved his first CCIE certification. Currently, he holds the Penta CCIE certification with a worldwide designation number of 11365, encompassing Routing and Switching, Voice over IP, Service Provider MPLS, Security, and Data Center. With approximately two decades of executive experience as a Lead Network Architect in the IT field at IBM and Cisco, he has leveraged his skills to benefit various industry sectors. Currently, his research focus encompasses network communication, cryptography, and security.

T. Aaron Gulliver received the Ph.D. degree in electrical engineering from the University of Victoria, Victoria, BC, Canada, in 1989. From 1989 to 1991, he was a Defence Scientist with Defence Research Establishment Ottawa, Ottawa, ON, Canada.

He has held academic appointments with Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999, where he is a Professor with the Department of Electrical and Computer Engineering. In 2002, he became a fellow of the Engineering Institute of Canada. In 2012, he was elected as a fellow of the Canadian Academy of Engineering. His research interests include information theory and communication theory, algebraic coding theory, discrete mathematics, intelligent networks, cryptography, and security.



Mohammad Dakhilalian received the B.Sc. and Ph.D. degrees in Electrical Engineering from Isfahan University of Technology (IUT) in 1989 and 1998, respectively and M.Sc. degree in Electrical Engineering from Tarbiat Modarres University in 1993. He joined IUT in 2001 and at present time is an Associate Professor in Electrical and Computer Engineering Department. His current research interests are Cryptography and, Data Security.