Generalized Inverse Binary Matrix Construction with PKC Application

Farshid, Haidary Makoui[1] and Thomas Aaron, Gulliver[1]

[1] *Department of Electrical and Computer Engineering, University of Victoria, Victoria, B.C., Canada. email: makoui@uvic.ca and agullive@ece.uvic.ca*

Abstract

The generalized inverses of systematic non-square binary matrices have applications in mathematics, channel coding and decoding, navigation signals, machine learning, data storage, and cryptography, such as the McEliece and Niederreiter public-key cryptosystems. A systematic non-square $(n-k) \times n$ matrix H, $n > k$, has $2^{k\times(n-k)}$ different generalized inverse matrices. This paper presents an algorithm for generating these matrices and compares it with two well-known methods, i.e. Gauss-Jordan elimination and Moore-Penrose. A random generalized inverse matrix construction method is given, which has a lower execution time than the Gauss-Jordan elimination and Moore-Penrose approaches. This paper also expands the novel idea to non-systematic non-square binary matrices and provides an application in public-key cryptosystems.

Keywords: Code-Based Cryptography, Generalized Inverse Binary Matrix, Error-Correcting Applications, Blockchains, Post Quantum, Public Key Cryptosystem (PKC)

1 Introduction

The generalized inverse of a systematic binary matrix is used for decoding in all applications of error-correcting codes including digital communication [1], navigation signals [2], data storage systems [3] and coding theory [4] in cryptography. Generalized inverse matrices can be obtained using Gauss-Jordan elimination [5] and Moore-Penrose pseudoinverse (MPP) techniques [6] [7].

A matrix is invertible if it has full rank. A non-square matrix A with m rows and n columns where $n > m$ is full rank if it is a full row rank matrix, where the rows are linearly independent.

Gauss-Jordan elimination is used to solve linear systems $Ax = b$ by employing row reduction operations to transform augmented matrices $[A|b]$ to row-echelon form (REF). This technique also provides a reduced row-echelon form (RREF) where the leading coefficient in each row is the only non-zero element entry in its column. Gauss-Jordan elimination uses an augmented matrix to construct the nullspace of the matrix A [8] and its associated vectors that lead to the generalized inverse of full rank matrices.

The Moore-Penrose technique provides a single pseudoinverse matrix, where the multiplication of the matrix and its pseudoinverse approximately equal the identity matrix. The MPP can provide a pseudoinverse for any matrix. This technique is a useful tool for application with data analysis, optimization, neural network and machine learning applications [9].

Non-square binary matrices are used in error-correction coding, code-based cryptography and decoding algorithms [10] [11]. This present paper introduces an efficient algorithm for calculating all the generalized inverses of a binary matrix. A simplified algorithm is also given to construct a random generalized inverse matrix with lower processing time in comparison with Moore-Penrose and Gauss-Jordan methods.

The proposed algorithm of constructing a general inverse for systematic matrices expand in section 3 to non-systematic non-square binary matrices as well. This paper also provides PKC application for generalized inverse matrix construction in section 4. Three-tuple public key construction with specified key relations for encryption, decryption, signing, verification, and integrity check algorithms.

1.1 Binary Linear Block Codes

In modern communication systems, redundant bits are added to a message sequence to detect and correct errors introduced by a noisy channel. The encoder assigns a binary codeword $\boldsymbol{c} = (c_1, c_2, ..., c_n)$ to a message $\boldsymbol{m} = (m_1, m_2, ..., m_k)$. For a k-tuple message $\boldsymbol{m}$, there are 2^k distinct messages and thus codewords. The set of all 2^k codewords is referred to a $C(n,k)$ block code. The length of a $C(n,k)$ block code is shown by n and k denoting dimension where $k < n$.

The channel encoder adds redundancy in the binary information sequence to the transmitted codewords, so each codeword has $n-k$ redundant bits more than the message associated with it. The message can scramble, permute and change the bits in the corresponding codeword [12]. These redundant bits are used by the channel decoder at the receiver's end to detect and correct errors having occurred over a noisy channel.

A $C(n,k)$ code is linear when its codewords form a k-dimensional vector subspace of the n-tuple vector space. Therefore, there are k linearly independent codewords $\boldsymbol{g}_1, \boldsymbol{g}_2, ..., \boldsymbol{g}_k$ that are settled as the rows of the generator matrix. The systematic form of generator matrix G in linear code is given by

$$G_{k\times n} = (I_k | P_{k\times(n-k)}), \tag{1}$$

where I_k is the $k \times k$ identity matrix and $P_{k\times(n-k)}$ is called the parity matrix. This can be written as

$$G = \begin{pmatrix} & | & p_{1,1} & p_{1,2} & p_{1,3} & \cdots & p_{1,(n-k)} \\ & | & p_{2,1} & p_{2,2} & p_{2,3} & \cdots & p_{2,(n-k)} \\ I_k & | & p_{3,1} & p_{3,2} & p_{3,3} & \cdots & p_{3,(n-k)} \\ & | & \vdots & \vdots & \vdots & & \vdots \\ & | & p_{k,1} & p_{k,2} & p_{k,3} & \cdots & p_{k,(n-k)} \end{pmatrix}.$$

A parity check matrix H is an $(n-k) \times n$ matrix, such that $GH^T = \mathbf{0}$ where ^{T} denotes transpose, so H is a basis of the dual space of $C_{n,k}$. Thus, H generates the dual code $C^{\perp}(n,k)$ with 2^{n-k} codewords. This matrix can be employed to determine if a particular vector is a codeword. The H matrix can also be used for decoding algorithms [11]. A systematic parity check matrix has the form

$$H_{(n-k)\times n} = (P^T_{(n-k)\times k} | I_{n-k}). \tag{2}$$

which can be expressed as

$$H = \begin{pmatrix} p_{1,1} & p_{2,1} & p_{3,1} & \cdots & p_{k,1} & | & \\ p_{1,2} & p_{2,2} & p_{3,2} & \cdots & p_{k,2} & | & \\ p_{1,3} & p_{2,3} & p_{3,3} & \cdots & p_{k,3} & | & I_{n-k} \\ \vdots & \vdots & \vdots & & \vdots & | & \\ p_{1,(n-k)} & p_{2,(n-k)} & p_{3,(n-k)} & \cdots & p_{k,(n-k)} & | & \end{pmatrix},$$

denote the generalized inverse of this matrix as

$$H^{-1}_{n\times(n-k)} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,(n-k)} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,(n-k)} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,(n-k)} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,(n-k)} \end{pmatrix}, \tag{3}$$

so that $H_{(n-k)\times n}H^{-1}_{n\times(n-k)} = I_{n-k}$, which can be expressed as

$$\left(\begin{array}{ccccc|c} p_{1,1} & p_{2,1} & p_{3,1} & \cdots & p_{k,1} & \\ p_{1,2} & p_{2,2} & p_{3,2} & \cdots & p_{k,2} & \\ p_{1,3} & p_{2,3} & p_{3,3} & \cdots & p_{k,3} & I_{n-k} \\ \vdots & \vdots & \vdots & & \vdots & \\ p_{1,(n-k)} & p_{2,(n-k)} & p_{3,(n-k)} & \cdots & p_{k,(n-k)} & \end{array}\right) \times \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,(n-k)} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,(n-k)} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,(n-k)} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,(n-k)} \end{pmatrix} = I_{n-k}. \tag{4}$$

2 Generalized Inverse Matrix Construction

The matrix H^{-1} has $n-k$ columns, each of which can have 2^k different values, so the number of matrices is $2^{k\times(n-k)}$[13]. The i-th column of H^{-1} belongs to a column set Z_i which contains 2^k vectors of length n

$$Z_i = \left\{ \begin{array}{ccccc} z_{1,1} & z_{1,2} & z_{1,3} & \cdots & z_{1,2^k} \\ z_{2,1} & z_{2,2} & z_{2,3} & \cdots & z_{2,2^k} \\ z_{3,1} & z_{3,2} & z_{3,3} & \cdots & z_{3,2^k} \\ \vdots & \vdots & \vdots & & \vdots \\ z_{k,1} & z_{k,2} & z_{k,3} & \cdots & z_{k,2^k} \\ --- & --- & --- & -- & --- \\ z_{(k+1),1} & z_{(k+1),2} & z_{(k+1),3} & \cdots & z_{(k+1),2^k} \\ z_{(k+2),1} & z_{(k+2),2} & z_{(k+2),3} & \cdots & z_{(k+2),2^k} \\ z_{(k+3),1} & z_{(k+3),2} & z_{(k+3),3} & \cdots & z_{(k+3),2^k} \\ \vdots & \vdots & \vdots & & \vdots \\ z_{n,1} & z_{n,2} & z_{n,3} & \cdots & z_{n,2^k} \end{array} \right\}. \tag{5}$$

This set can be divided into two subsets, Z_i^1 and Z_i^2, where Z_i^1 contains rows 1 to k and Z_i^2 contains rows $k+1$ to n, so that

$$Z_i^1 = \begin{Bmatrix} z_{1,1} & z_{1,2} & z_{1,3} & \cdots & z_{1,2^k} \\ z_{2,1} & z_{2,2} & z_{2,3} & \cdots & z_{2,2^k} \\ z_{3,1} & z_{3,2} & z_{3,3} & \cdots & z_{3,2^k} \\ \vdots & \vdots & \vdots & & \vdots \\ z_{k,1} & z_{k,2} & z_{k,3} & \cdots & z_{k,2^k} \end{Bmatrix}, \tag{6}$$

$$Z_i^2 = \begin{Bmatrix} z_{(k+1),1} & z_{(k+1),2} & z_{(k+1),3} & \cdots & z_{(k+1),2^k} \\ z_{(k+2),1} & z_{(k+2),2} & z_{(k+2),3} & \cdots & z_{(k+2),2^k} \\ z_{(k+3),1} & z_{(k+3),2} & z_{(k+3),3} & \cdots & z_{(k+3),2^k} \\ \vdots & \vdots & \vdots & & \vdots \\ z_{n,1} & z_{n,2} & z_{n,3} & \cdots & z_{n,2^k} \end{Bmatrix}, \tag{7}$$

Z_i^1 contains all 2^k possible binary vectors from all zeros to all ones. For example, if $k=3$ then Z_i^1 contains the eight binary vectors of length 3

$$Z_i^1 = \begin{Bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{Bmatrix}.$$

For Z_i^2, the value of $z_{(k+b),d}$, $1 \le b \le n-k, 1 \le d \le 2^k$, is determined as follows. Multiplication of H by a column of Z_1 must satisfy

$$\begin{pmatrix} p_{1,1} & p_{2,1} & \cdots & p_{k,1} & | & \\ p_{1,2} & p_{2,2} & \cdots & p_{k,2} & | & I_{n-k} \\ \vdots & \vdots & & \vdots & | & \\ p_{1,(n-k)} & p_{2,(n-k)} & \cdots & p_{k,(n-k)} & | & \end{pmatrix} \times \begin{pmatrix} z_{1,d} \\ z_{2,d} \\ \vdots \\ z_{k,d} \\ --- \\ z_{(k+1),d} \\ z_{(k+2),d} \\ \vdots \\ z_{n,d} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{8}$$

Thus, for $b=1$ the result is 1, and otherwise, it is 0.

so, if $b = 1$

$$z_{(k+1),d} = 1 + p_{1,1}z_{1,d} + p_{2,1}z_{2,d} + \cdots + p_{k,1}z_{k,d}, 1 \leq d \leq 2^k,$$

and if $b \neq 1$

$$z_{(k+b),d} = p_{1,b}z_{1,d} + p_{2,b}z_{2,d} + \cdots + p_{k,b}z_{k,d}, 1 \leq d \leq 2^k.$$

The columns of Z_2 satisfy

$$\begin{pmatrix} p_{1,1} & p_{2,1} & \cdots & p_{k,1} & | & \\ p_{1,2} & p_{2,2} & \cdots & p_{k,2} & | & I_{n-k} \\ \vdots & \vdots & \ddots & \vdots & | & \\ p_{1,(n-k)} & p_{2,(n-k)} & \cdots & p_{k,(n-k)} & | & \end{pmatrix} \times \begin{pmatrix} z_{1,d} \\ z_{2,d} \\ \vdots \\ z_{k,d} \\ --- \\ z_{(k+1),d} \\ z_{(k+2),d} \\ \vdots \\ z_{n,d} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \tag{9}$$

so for $b = 2$

$$z_{(k+2),d} = 1 + p_{1,2}z_{1,d} + p_{2,2}z_{2,d} + \cdots + p_{k,2}z_{k,d}, 1 \leq d \leq 2^k,$$

and for $b \neq 2$

$$z_{(k+b),d} = p_{1,b}z_{1,d} + p_{2,b}z_{2,d} + \cdots + p_{k,b}z_{k,d}, 1 \leq d \leq 2^k.$$

Similarly, the columns of Z_{n-k} must satisfy

$$\begin{pmatrix} p_{1,1} & p_{2,1} & \cdots & p_{k,1} & | & \\ p_{1,2} & p_{2,2} & \cdots & p_{k,2} & | & I_{n-k} \\ \vdots & \vdots & \ddots & \vdots & | & \\ p_{1,(n-k)} & p_{2,(n-k)} & \cdots & p_{k,(n-k)} & | & \end{pmatrix} \times \begin{pmatrix} z_{1,d} \\ z_{2,d} \\ \vdots \\ z_{k,d} \\ --- \\ z_{(k+1),d} \\ z_{(k+2),d} \\ \vdots \\ z_{n,d} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \tag{10}$$

so for $b = n-k$ the result is 1 and for $b \neq n-k$ the result is 0. Thus if $b = n-k$

$$z_{(k+(n-k)),d} = z_{n,d} = 1 + p_{1,(n-k)}z_{1,d} + p_{2,(n-k)}z_{2,d} + \cdots + p_{k,(n-k)}z_{k,d}), 1 \leq d \leq 2^k,$$

and if $b \neq n-k$

$$z_{(k+b),d} = p_{1,b}z_{1,d} + p_{2,b}z_{2,d} + \cdots + p_{k,b}z_{k,d}, 1 \leq d \leq 2^k.$$

2.1 Example

Let $n = 6$ and $k = 3$ with

$$G = (I_k|P_{k\times(n-k)}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

and

$$H = (P^T|I_{n-k}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

Thus, H^{-1} has $n-k = 3$ columns and there are three column sets Z_1, Z_2 and Z_3 available $(1 \leq i \leq n-k)$ with a total of $2^{k\times(n-k)} = 2^{3\times 3} = 512$ possible matrices. The sets Z_i^1 and Z_i^2 are defined as follows. Z_i^1 is common for all i and is given by

$$Z_i^1 = \begin{Bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{Bmatrix},$$

and Z_i^2 can be expressed as

$$Z^2 = \begin{Bmatrix} z_{(k+1),1} & z_{(k+1),2} & z_{(k+1),3} & z_{(k+1),4} & z_{(k+1),5} & z_{(k+1),6} & z_{(k+1),7} & z_{(k+1),8} \\ z_{(k+2),1} & z_{(k+2),2} & z_{(k+2),3} & z_{(k+2),4} & z_{(k+2),5} & z_{(k+2),6} & z_{(k+2),7} & z_{(k+2),8} \\ z_{(k+3),1} & z_{(k+3),2} & z_{(k+3),3} & z_{(k+3),4} & z_{(k+3),5} & z_{(k+3),6} & z_{(k+3),7} & z_{(k+3),8} \end{Bmatrix}.$$

Combining Z_i^1 and Z_i^2 gives

$$Z_i = \left\{\begin{array}{cccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ -- & -- & -- & -- & -- & -- & -- & -- \\ z_{4,1} & z_{4,2} & z_{4,3} & z_{4,4} & z_{4,5} & z_{4,6} & z_{4,7} & z_{4,8} \\ z_{5,1} & z_{5,2} & z_{5,3} & z_{5,4} & z_{5,5} & z_{5,6} & z_{5,7} & z_{5,8} \\ z_{6,1} & z_{6,2} & z_{6,3} & z_{6,4} & z_{6,5} & z_{6,6} & z_{6,7} & z_{6,8} \end{array}\right\}.$$

For $i = 1$, we have

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ - \\ z_{4,1} \\ z_{5,1} \\ z_{6,1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

so

$$\begin{aligned} z_{41} &= 1 + (0)(0) + (1)(0) + (1)(0) = 1, \\ z_{51} &= (1)(0) + (1)(0) + (0)(0) = 0, \\ z_{61} &= (1)(0) + (0)(0) + (1)(0) = 0. \end{aligned}$$

The elements of Z_1^2 are

$$\begin{aligned} z_{4,d} &= 1 + p_{1,1}z_{1,d} + p_{2,1}z_{2,d} + p_{3,1}z_{3,d}, \\ z_{5,d} &= p_{1,2}z_{1,d} + p_{2,2}z_{2,d} + p_{3,2}z_{3,d}, \\ z_{6,d} &= p_{1,3}z_{1,d} + p_{2,3}z_{2,d} + p_{3,3}z_{3,d}, \end{aligned}$$

so

$$Z_1 = \left\{\begin{array}{cccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ -- & -- & -- & -- & -- & -- & -- & -- \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right\}.$$

The elements of Z_2^2 are

$$\begin{aligned}
z_{4,d} &= p_{1,1}z_{1,d} + p_{2,1}z_{2,d} + p_{3,1}z_{3,d}, \\
z_{5,d} &= 1 + p_{1,2}z_{1,d} + p_{2,2}z_{2,d} + p_{3,2}z_{3,d}, \\
z_{6,d} &= p_{1,3}z_{1,d} + p_{2,3}z_{2,d} + p_{3,3}z_{3,d},
\end{aligned}$$

so

$$Z_2 = \left\{ \begin{array}{cccccccc}
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
-- & -- & -- & -- & -- & -- & -- & -- \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0
\end{array} \right\}.$$

The elements of Z_3^2 are given by

$$\begin{aligned}
z_{4,d} &= p_{1,1}z_{1,d} + p_{2,1}z_{2,d} + p_{3,1}z_{3,d}, \\
z_{5,d} &= p_{1,2}z_{1,d} + p_{2,2}z_{2,d} + p_{3,2}z_{3,d}, \\
z_{6,d} &= 1 + p_{1,3}z_{1,d} + p_{2,3}z_{2,d} + p_{3,3}z_{3,d},
\end{aligned}$$

so

$$Z_3 = \left\{ \begin{array}{cccccccc}
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
-- & -- & -- & -- & -- & -- & -- & -- \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1
\end{array} \right\}.$$

Selecting columns from each column set Z_1, Z_2, Z_3 in order gives $2^{k\times(n-k)} = 2^9 = 512$ H^{-1} matrices which satisfy $HH^{-1} = I_{n-k}$.

2.2 Random Generalized inverse Matrix Construction

An generalized inverse matrix H^{-1} can be divided into two parts, A_1 and A_2, where A_1 consists of rows 1 to k and A_2 consists of rows $k+1$ to n

$$H^{-1}_{n\times(n-k)} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,(n-k)} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,(n-k)} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,(n-k)} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{k,1} & a_{k,2} & a_{k,3} & \cdots & a_{k,(n-k)} \\ --- & --- & --- & -- & --- \\ a_{(k+1),1} & a_{(k+1),2} & a_{(k+1),3} & \cdots & a_{(k+1),(n-k)} \\ a_{(k+2),1} & a_{(k+2),2} & a_{(k+2),3} & \cdots & a_{(k+2),(n-k)} \\ a_{(k+3),1} & a_{(k+3),2} & a_{(k+3),3} & \cdots & a_{(k+3),(n-k)} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,(n-k)} \end{pmatrix} = \begin{pmatrix} A_1 \\ - \\ A_2 \end{pmatrix}. \qquad (11)$$

A random generalized inverse matrix H^{-1} can be constructed by selecting a random A_1 and constructing the corresponding matrix A_2. For example, if $n = 20$ and $k = 12$, then A_1 contains $n-k = 8$ random binary column vectors of length 12 such as

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Hence, the elements of A_2 are

$$A_2 = \begin{pmatrix} a_{(k+1),1} & a_{(k+1),2} & a_{(k+1),3} & \cdots & a_{(k+1),(n-k)} \\ a_{(k+2),1} & a_{(k+2),2} & a_{(k+2),3} & \cdots & a_{(k+2),(n-k)} \\ a_{(k+3),1} & a_{(k+3),2} & a_{(k+3),3} & \cdots & a_{(k+3),(n-k)} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,(n-k)} \end{pmatrix}, \qquad (12)$$

where

$$a_{(k+b),d} = \sum_{i=1}^{k} p_{ib} a_{id}, (b \neq d),$$

and

$$a_{(k+b),d} = 1 + \sum_{i=1}^{k} p_{ib} a_{id}, (b = d).$$

In general, this can be expressed as

$$a_{(k+b),d} = 2^{|b-d|} \bmod 2 + \sum_{i=1}^{k} p_{ib} a_{id}. \tag{13}$$

For example, $a_{(k+1),1}$ in A_2 is given by

$$a_{(k+1),1} = 1 + p_{11}a_{11} + p_{21}a_{21} + \cdots + p_{k1}a_{k1}.$$

The result in matrix form to construct A_2 is shown as follows.

Let $B_1 = P^T_{(n-k)\times k}$ and $B_2 = I_{n-k}$, so

$$\begin{aligned} HH^{-1} &= \Big(B_1|B_2\Big) \times \begin{pmatrix} A_1 \\ - \\ A_2 \end{pmatrix} = I_{n-k}, \\ &= B_1A_1 + B_2A_2 = I_{n-k}, \\ A_2 &= B_1A_1 + I_{n-k}, \end{aligned} \tag{14}$$

so $A_2 = B_1A_1 + I_{n-k}$ and then

$$\begin{aligned} HH^{-1} &= \Big(B_1|B_2\Big) \times \begin{pmatrix} A_1 \\ - \\ A_2 \end{pmatrix} = \Big(B_1|B_2\Big) \times \begin{pmatrix} A_1 \\ \hline B_1A_1 + I_{n-k} \end{pmatrix}, \\ &= B_1A_1 + B_2(B_1A_1 + I_{n-k}) = B_1A_1 + B_1A_1 + I_{n-k} = I_{n-k}. \end{aligned}$$

The next section provides the analysis of the proposed algorithm for constructing a random generalized inverse matrix.

2.3 Construction Comparison and Analysis

In this section, the processing time of Moore-Penrose pseudoinverses and the proposed method for constructing random generalized inverse matrices are compared.
The computation time is given in Table 1 for several parameter values. As an example, the processing time required to construct the random generalized inverse of H matrix with 524×1568 would be 594 millisecond using the proposed method, compared with 2172 milliseconds using the Moore-Penrose pseudoinverse.

Matrix size	Moore-Penrose (ms)	Proposed (ms)
$k = 213$, $n = 500$	94	16
$k = 524$, $n = 1568$	2172	594
$k = 768$, $n = 2048$	5109	2368
$k = 1024$, $n = 2896$	14735	5211

Table 1: Processing time

An algorithm's computational efficiency depends on the number of arithmetic operations, algorithm complexity and the amount of resources, including time and memory, needed to run the algorithm.
Solving a system of n equations with n variables using Gauss-Jordan row elimination requires approximately $(2n^3 + 3n^2 - 5n)/3$ arithmetic operations to achieve the row echelon form (REF) [14], and $(n^3 + 3/2n^2 - 5/2n)$ arithmetic operations to form RREF which is about fifty percent more than the number of REF arithmetic operations. Hence, the number of arithmetic operations that Gauss-Jordan elimination required to form RREF for a parity check matrix H with $(n-k) \times n$ index would be $(n-k)^3 + 3/2(n-k)^2 - 5/2(n-k)$.

After performing RREF, Gauss-Jordan needs to solve a system of linear equations using the null-space approach to find the set of associated vectors. Therefore, not all the augmented matrices can form RREF, known as inconsistent matrices. When RREF is formed, additional $n(n-k-1)$ arithmetic operations need to construct a generalized inverse matrix.

There are many different choices of row combinations to perform Gauss-Jordan row elimination on large-size matrices, and finding an optimum choice of linear combinations is NP-hard [15]. In fact, there are numerous different execution sequences and therefore time complexity is exponential [15].
Moore-Penrose requires $(n-k)^2(2n-1)$ arithmetic operations to construct a full-rank HH^T and approximately $(n-k)(2n^2 - 2nk - n)$ arithmetic operations, exclude determi-

nant, to construct $H^T[HH^T]^{-1}$ of a parity check matrix H. The algorithm is less complex than Gauss-Jordan, and in fact, it is faster than the Guass-Jordan elimination algorithm.

The number of arithmetic operations the proposed method requires to construct a random generalized inverse would equal the number of operations to build $A_2 = B_1A_1 + I_{n-k}$, which would be $(2k-1)(n-k)^2 + (n-k)$. Therefore, the multiplication of B_1 with index $(n-k) \times k$ and A_1 with index $k \times (n-k)$ required $(2k-1)(n-k)^2$ number of arithmetic operations.

The arithmetic computation is given in Table 2 for Gauss-Jordan elimination, Moore-Penrose, and the proposed algorithm for constructing a random non-square binary generalized inverse matrix. The introduced method provides optimum choices to construct a random generalized inverse matrix with less processing time and complexity than Moore-Penrose and Gauss-Jordan elimination methods.

Gauss-Jordan Elimination	Moore-Penrose	Proposed
$(n-k)^3 + 3/2(n-k)^2 - 5/2(n-k) + n(n-k-1)$	$(n-k)^2(4n-1) - n(n-k)$	$(2k-1)(n-k)^2 + (n-k)$

Table 2: Computational Cost

2.4 Key change interval comparison

Based on the security key management, it is recommended to increase the system security by changing the keys in shorter time intervals. Every time that a new key is selected, the generator matrix and its associated parity-check matrix will be replaced, the Gauss-Jordan elimination method ought to transform the H matrix to RREF and find out the associated vectors to construct a random generalized inverse matrix. For instance, finding the optimum choice of linear combinations of an H matrix with 1280 rows $(n = 2048, k = 768)$ to form RREF is time-consuming and may affect the performance of the system applications. The Moore-Penrose pseudoinverse also is slower than the proposed method. In fact, any time matrix H changes, the proposed algorithm can construct a random generalized inverse matrix with less complexity and lower processing time. This fact could make the proposed algorithm a suitable candidate for any system that requires changing the key (including the code-based public key with G and H matrices) periodically in a shorter time interval.

3 Random Inverse for Non-Systematic Matrices

The section expands the idea for non-systematic non-square binary matrices. lets assume matrix B is a non-systematic binary matrix with m rows and n columns $(m < n)$ such

$$B_{m\times n} = \begin{pmatrix} B_1 b_1 & B_2 b_2 & \dots & B_x b_y \end{pmatrix}, \tag{15}$$

where $(B_1)_{m\times n_1}, (B_2)_{m\times n_2}, \dots, (B_x)_{m\times n_x}$
with y column vectors $(b_i)_{m\times 1}$
and $(n_1) + (n_2) + \dots + (n_x) + (y) = n$.

As a full rank matrix, the matrix B should have minimum m independent linear combination column vectors $(b_i)_{m\times 1}, 1 \le i \le y$ that can be anywhere within the matrix B in a group or individual.

Lets assume matrix A is an inverse matrix of non-syestematic non-square binary matrix B with n rows and m columns such

$$A_{n\times m} = \begin{pmatrix} A_1 \\ a_1 \\ A_2 \\ a_2 \\ \vdots \\ A_x \\ a_y \end{pmatrix}, \tag{16}$$

where $(A_1)_{n_1\times m}, (A_2)_{n_2\times m}, \dots, (A_x)_{n_x\times m}$
with x times row matrix $(a_i)_{1\times m}$

Hence the A is an inverse of the B matrix, then

$$BA = \begin{pmatrix} B_1 b_1 & B_2 b_2 & \dots & B_x b_y \end{pmatrix} \times \begin{pmatrix} A_1 \\ a_1 \\ A_2 \\ a_2 \\ \vdots \\ A_x \\ a_y \end{pmatrix} = I_{m\times m},$$

$$\Big(B_1A_1 + b_1a_1 + B_2A_2 + b_2a_2 + \quad \dots \quad + B_xA_x + b_ya_y\Big) = I_{m\times m}$$

$$\sum_{i=1}^{x} B_iA_i + \sum_{i=1}^{y} b_ia_i = I_{m\times m} \tag{17}$$

A random generalized inverse matrix A can be constructed by selecting a random $A_1, A_2, \dots, A_x$ and constructing the corresponding row matrix $a_1, a_2, \dots, a_y$ variables.

Lets call A_a as a coressponded varibale matrix such

$$(A_a)_{m\times m} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_y \end{pmatrix}, (B_b)_{m\times m} = \begin{pmatrix} b_1 & b_2 & \dots & b_y \end{pmatrix}$$

Therefore,

$$\sum_{i=1}^{x} B_iA_i + B_bA_a = I_{m\times m}$$

$$B_bA_a = I_{m\times m} + \sum_{i=1}^{x} B_iA_i$$

$$A_a = (B_b)^{-1}(I_{m\times m} + \sum_{i=1}^{x} B_iA_i) \tag{18}$$

Hence all the columns of the (B_b) matrix are linearly independent. Therefore the determinant of (B_b) matrix is equal to 1, and the (B_b) is an invertible matrix.

For example, B is a non-systematic-non-square binary matrix with index $n = 9$ and $m = 5$ such

$$B_{5\times 9} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

where $x = 1$ and $y = 5$ (five colorful columns in two groups, green and yellow)

Therefore,

$$A_a = (B_b)^{-1}(I_5 + B_1A_1)$$

so by selecting a random A_1 and constructing $(B_b)^{-1}$

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}, B_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and constructing $(B_b)^{-1}$

$$(B_b)_{5\times 5} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, (B_b)^{-1} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

the A_a can be constructed as

$$A_a = (B_b)^{-1}(I_5 + B_1 A_1)$$

$$(A_a)_{5\times 5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Having random A_1, and A_a the inverse matrix A can be constructed such

$$A_{9\times 5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

where $B_{(5\times 9)} \times A_{(9\times 5)} = \boldsymbol{I}_{5\times 5}$

4 PKC Application

The PKC is a generalized inverse matrix construction application that can generate public and private keys for encryption, decryption, and digital signature (signing and verification) algorithms. The proposed random inverse matrix construction is used in [16] for the public key infrastructure of the scheme to define three-tuple public keys for a new code-based digital signature algorithm.

Public Key Infrustructure

$(pk, sk) \leftarrow Gen(\lambda)$ where λ denotes the key generation scheme.

The following matrices are used in the proposed public key infrustructure in [16].

- G, a generator matrix of size $k \times n$.
- H, a parity check matrix of size $(n-k) \times n$.
- S, a non-singular scrambling matrix of size $k \times k$.
- P, a permutation matrix of size $n \times n$.
- L, a non-singular matrix of size $(n-k) \times (n-k)$.

The proposed algorithm in [16] generates a public key (pk) and a private key $(pr(sk))$.

Key Generation Algorithm $Gen(\lambda)$

---

1. Obtain a generator matrix G and corresponding parity matrix H for $C(n,k)$.
2. Select a random H^{-1} from the $2^{k\times(n-k)}$ choices using a random matrix A_1 and constructing the corresponding matrix A_2
   $H^{-1} = \frac{A_1}{A_2}$.
3. As in the McEliece cryptosystem, use the generator matrix G, the scrambling matrix S and the permutation matrix P to mask G
   $p_1 = G^{'} = SGP$.
4. Use the non-singular random matrix L and P to mask H^{-1}
   $p_2 = L^{-1}(H^{-1})^T P$.
5. Verification of the digital signatures requires
   $p_3 = P^{-1}(H^{-1}H)^T P$.

6. Construct a parity check matrix corresponding to $G^{'} = SGP$
   $Q = H^{'T} = P^{-1}H^{T}L\, H^{'} = L^{T}H(P^{-1})^{T}$.

7. Public key: $pk \leftarrow (p_1, p_2, p_3)$.

8. Private key: $pr(sk) \leftarrow (S^{-1}, P^{-1}, G, Q)$, where sk denotes the secret key.

It is shown in [16] that the key relations defined by Lemma 1 and Lemma 2 are used in the signing, verification, and integrity check algorithms of the new code-based digital signature.

Lemma 1. *The public key $pk = (p_1, p_2, p_3)$ satisfies the following*

$$(p_1)(p_3) = \mathbf{0} \tag{19}$$
$$(p_2)(p_3) = p_2 \tag{20}$$
$$(p_3)(p_3) = p_3 \tag{21}$$

Lemma 2. *The public key $pk = (p_1, p_2, p_3)$ and the secret key (Q) are related as follows.*

$$(p_1)(Q) = \mathbf{0} \tag{22}$$
$$(p_2)(Q) = \boldsymbol{I} \tag{23}$$
$$(p_3)(Q) = Q \tag{24}$$
$$(Q)(p_2) = p_3 \tag{25}$$

It was shown that the proposed generalized inverse matrix could construct $2^{k\times(n-k)}$ inverse matrices. Therefore it is also proven in [16] that the probability of an adversary constructing a secret key using the public key is $2^{-(k\times(n-k))}$. Therefore, the probability of an adversary forging the algorithm by finding the exact secret key is negligible, and the algorithm is secure against an structural public key attack.

$$Pr[(Adv, \gamma) = 1] < \frac{1}{2^{k\times(n-k)}}.$$

5 Conclusion

This paper considered the construction of all H generalized inverse matrices of a non-square $(n \neq k)$ matrix H. The matrix H^{-1} has $n-k$ columns. The paper proposes a column set Z_i where $1 \leq i \leq n-k$. The "i" column of H^{-1} belongs to a column set Z_i that contains 2^k vectors. It also divides the column set Z_i into two subsets which simplifies the calculation of all 2^k vectors and leads to the construction of all the $2^{k\times(n-k)}$ generalized inverse matrices.

Furthermore, the random generalized inverse matrix construction method presented, introduces matrix A_1 and A_2, where A_1 consists of $n-k$ binary vectors. In simple term, the elements of the matrix A_1 can be selected on a random basis and the matrix A_2 can be constructed using a simplified proposed equation. In fact, the proposed approach provides a shorter processing time and computational simplicity to construct a random generalized inverse matrix that can be suitable for applications that demand new keys to be generated periodically in shorter interval times.

The proposed approach was compared with the restricted applicability of Moore-Penrose and Gauss-Jordan methods, and it showed that it is faster with less computational cost. The PKC application and three tuples public key generation algorithm for digital signature and encryption was given. The three tuple key relations were given in Lemma1 and Lemma2 that can be used for encryption, decryption, signing, verification, and integrity check algorithms. It also was shown that the proposed PKC is secure against structural public key attacks.

References

[1] C. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.,*, vol. 27, no. 3, pp. 379-423, 1948.

[2] R. Acharya, "Undrestanding satellite navigation," *Mobile geographic info systems*, Academic press, electronic books, 2014.

[3] Alexander Thomasian, "Storage Systems: Organization, Performance, Coding, Reliability, and Their Data Processing," *Storage systems book*, publisher Waltham, Massachusetts, Elsevier, 2011.

[4] S. Saraf, S. Dhingra, and G. Pinheiro, "Parallel algorithm for finding inverse of a matrix and its application in message sharing (coding theory)," *International Journal of Computer Applications*, vol. 975, p. 8887, 2016.

[5] P. S. Stanimirović and M. D. Petković, "Gauss–Jordan elimination method for computing outer inverses," *Applied Mathematics and Computation*, vol. 219, no. 9, pp. 4667–4679, Jan. 2013.

[6] J.C.A. Barata, M.S. Hussein, "The Moore-Penrose Pseudoinverse. A Tutorial Review of the Theory," *Instituto de F ´ısica, Universidade de S˜ao Paulo*, C.P. 66318, 05314-970 S˜ao Paulo, SP, Brazil, Oct. 2011.

[7] H. Chen and Y. Wang, "A family of higher-order convergent iterative methods for computing the Moore–Penrose inverse," *Applied Mathematics and Computation*, vol. 218, no. 8, pp. 4012–4016, Dec. 2011.

[8] N. Guglielmi, M. L. Overton, and G. Stewart, "An efficient algorithm for computing the generalized null space decomposition," *SIAM Journal on Matrix Analysis and Applications*, vol. 36, no. 1, pp. 38–54, 2015.

[9] J Tapson, A van Schaik, "Learning the inverse solution to network weights," *Neural networks*, vol. 45, pp. 94–100, 2013.

[10] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Jet Propulsion Lab*, DSN Tech. Rep. 42.44, pp. 114–116, 1978.

[11] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Problems of Control and Information Theory*, vol. 15, pp. 159–166, 1986.

[12] M. Esmaeili, T.A.Gulliver, "Joint channel coding-cryptography based on random insertions and deletions in quasi-cyclic-low-density parity check codes," *IET communications*, vol.9 (12), pp. 1555-1560, 2015.

[13] M. Esmaeili, T.A.Gulliver, "Application of Linear Block Codes in Cryptography," *University of Victoria department of Electrical and Computer Engineering*, Chapter 5, Security analysis. pp. 45-53, 2019.

[14] Farebrother, R.W., "Linear least squares computations," *Statistics, textbooks and monographs*, London. Taylor and Francis. pp. 12, 2017.

[15] Fang Xin, Havas George, "On the worst-case complexity of integer Gaussian elimination," *International Conference on Symbolic and Algebraic Computation*, ISSAC 97, Proceedings of the 1997 international symposium on Symbolic and algebraic computation. pp. 28-31, July 1997.

[16] F. Haidary Makoui, T.A. Gulliver, M. Dakhilaian "A New Code-Based Digital Signature Based on the McEliece Cryptosystem," *IET communications*, published online, doi: cmu2.12607, April 2023.