RIGHT INVERSE IN PUBLIC KEY CRYPTOSYSTEM DESIGN

By Budi Murtiyasa

Department of Mathematics Education
Faculty of Education and Training Muhammadiyah University of Surakarta

Abstract

The theory of matrices becomes a potential tool in cryptographic research. The paper addresses to develop a public key cryptosystem based on right inverse of matrices. The idea is similar to the previous public key cryptosystem, that is McEliece’s public key and Wu-Dawson’s public key, in term of the usage of a coding theory. Properties of the public key cryptosystem are analyzed and compared with the previous public key cryptosystem.

Key word: right inverses, public key cryptosystem

Introduction

For a public key cryptosystem with information expansion, i.e. the length of ciphertext blocks is larger than that of plaintext blocks, it is possible that one plaintext block may correspond to several valid ciphertext blocks. For example, McEliece’s public key cryptosystem and Wu-Dawson’s public key cryptosystem have information expansion (Wu and Dawson, 1998:321). Both of them have an advantage that is fast encryption and decryption. Disadvantages need large key space and have message expansion.

This paper proposes a public key cryptosystem based on the right inverses of matrices in the field $\mathbb{Z}_2 = \{0, 1\}$. The algorithms of encryption and decryption, which are linear operation, can be performed very quickly. Properties and risk analysis of the public key cryptosystem are discussed by comparing with McEliece’s and Wu-Dawson’s public key cryptosystem.

Encryption by McEliece’s public key can be explained as follows. For a message $m$, ciphertext $c = mG^* \oplus e$, $G^* = SGP$, where $G$ is a $k \times n$ generator matrix of linear code $C[n,k]$, $S$ is a $k \times k$ nonsingular matrix, $P$ is a $n \times n$ permutation matrix, and $e$ is a binary vector of length $n$ with Hamming weight $t$. $G^*$ is public, and $G$, $S$, and $P$ are secret. Conversely, the decryption process of ciphertext $c$ to obtain the plaintext $m$ are : (1) compute $e_1 = cP^{-1}$, (2) $m_1 = e_1 \oplus e_t$, (3) retrieve $m_0$ from $m_0G = m_1$, (4) compute $m = m_0S^{-1}$ (Stinson, 1995:196). Meanwhile, Wu-Dawson’s public key can be summarized as in Table 1 below.

In Table 1, $c$ is a ciphertext of a message $m$, $G$ is a $k \times n$ generator matrix of linear code $C[n,k]$, $H$ is $(n-k) \times n$ parity check of matrix, $H^*$ is $n \times (n-k)$ generalized inverses of matrix $H$. (Wu and Dawson, 1998:323).

---

1 Presented on IndoMS Conference at Faculty of Mathematics and Natural Sciences Udayana University Denpasar Bali Indonesia, 26 – 30 July 2004.
2 E-mail : bdmurtiyasa@yahoo.com
Table 1. Wu-Dawson’s public key cryptosystem

<table>
<thead>
<tr>
<th>Public</th>
<th>G, H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>H' H</td>
</tr>
<tr>
<td>Encryption</td>
<td>c = mG ⊕ e(H)T</td>
</tr>
<tr>
<td>Decryption</td>
<td>(1) mG = c(I, ⊕ (H'H)T)</td>
</tr>
<tr>
<td></td>
<td>(2) retrieve m from mG</td>
</tr>
</tbody>
</table>

Left/Right Inverses of Matrices

For a nonsingular and square matrix $A$, the inverse of $A$ is $A^{-1}$, so that

$$AA^{-1} = A^{-1}A = I \tag{1}$$

If $A$ is singular, it is possible to find an inverse of $A$, called generalized inverses of $A$ (Israel and Greville, 1974). If $A$ is non-square, it is possible to find a left inverse or a right inverse of $A$.

**Definition 1.** For a matrix $A$, if $LA = I$ but $AL \neq I$, with more than one $L$, the matrices $L$ are called left inverse of $A$. Conversely, for a matrix $A$, if $AR = I$ but $RA \neq I$, with more than one $R$, the matrices $R$ are called right inverse of $A$.

**Theorem 1.** A $m \times n$ matrix $A$ has left inverses only if $m \geq n$.

**Theorem 2.** A $m \times n$ matrix $A$ has right inverses only if $m \leq n$.

**Proof:** we prove that a contradictory result can be obtained as $m > n$ and $A$ having right inverse.

For $m > n$, let $A = \begin{pmatrix} X_{mn} \\ Y_{(m-n)\times n} \end{pmatrix}$, and suppose $nxm$ matrix $A^*$ is right inverse of $A$, $A^* = \begin{pmatrix} P_{nxn} & Q_{nx(m-n)} \end{pmatrix}$, then:

$$AA^* = \begin{pmatrix} X_{mn} \\ Y_{(m-n)\times n} \end{pmatrix} \begin{pmatrix} P_{nxn} & Q_{nx(m-n)} \end{pmatrix} = \begin{pmatrix} XP & XQ \\ YP & YQ \end{pmatrix} = I_m = \begin{pmatrix} I_n & 0 \\ 0 & I_{(m-n)} \end{pmatrix}$$

this means $XP = I$, $XQ = 0$, $YP = 0$, and $YQ = I$. Since $XP = I$ and both $X$ and $P$ are square matrices, then $P = X^{-1}$. Meanwhile,

$$YP = YY^{-1} = 0$$

$$YX^{-1}X = 0$$

(multiple by $X$)

$$Y = 0$$
and \( YQ = 0Q = 0 \neq I \). It is contradictory. Therefore, if \( m > n \), a \( m \times n \) matrix \( A \) has no right inverse.

**Theorem 3.** A \( m \times n \) matrix \( A \) has right inverse if rank of \( A \) is \( m \).

*Proof:* because \( A \) has rank \( m \), there exists a \( m \times m \) non-singular submatrix \( X \) of \( A \). Let \( A = (X_{m \times m} Y_{m \times (n-m)}) \), and suppose \( A^* = \begin{pmatrix} X_{m \times m}^{-1} \\ 0_{(n-m) \times m} \end{pmatrix} \) is right inverse of \( A \), then \( AA^* = I_m \).

From Theorem 2 and Theorem 3 above, it can be concluded that a \( m \times n \) matrix \( A \) has right inverses if and only if \( A \) has rank \( m \) and \( m \leq n \).

According to Ayres Jr (1982) a \( m \times n \) matrix \( A \) which has rank \( m \), there exists a \( n \times n \) nonsingular matrix \( Q \), so that:

\[
A = \begin{pmatrix} I_m & 0_{m \times (n-m)} \end{pmatrix} Q^{-1}
\]

**Theorem 4.** In form (2), the right inverse of \( A \) is

\[
A^* = Q \begin{pmatrix} I_m \\ W_{(n-m) \times m} \end{pmatrix}
\]

where \( W \) is an arbitrary.

*Proof:* \( AA^* = \begin{pmatrix} I_m & 0_{m \times (n-m)} \end{pmatrix} Q^{-1} Q \begin{pmatrix} I_m \\ W_{(n-m) \times m} \end{pmatrix} = I_m \).

**Lemma 1.** In the field \( \mathbb{Z}_2 = \{0, 1\} \), the number of right inverses of \( A \) in form (3) is \( 2^{(n-m) \times m} \).

*Proof:* the number of different right inverses of \( A \) is the number of different choices of \( W \) which is totally \( 2^{(n-m) \times m} \).

Moreover, \( A^\top \) is transpose of \( A \), and \( A^* \) is a right inverse of \( A \). For a \( m \times n \) matrix \( A \), can be verified that \((A^\top)^\top = (A^\top)^\top\). It can be explained as follows: by Definition 1 and Theorem 1, \( A^\top \) has left inverses, i.e. \((A^\top)^\top\), so that \((A^\top)^\top A^\top = I \). Meanwhile, in line with properties of matrix transpose:

\[
(A A^\top)^\top = (A^\top)^\top A^\top
\]

\[
(I)^\top = (A^\top)^\top A^\top
\]

\[
I = (A^\top)^\top A^\top
\]

Matrix \((A^\top)^\top\) is a left inverse of \( A^\top \). Thus, \((A^\top)^\top = (A^\top)^\top\).

**Design of Public Key Cryptosystem**

An arbitrary linear code \( C[n,k] \) can be treated as a vector subspace of \( V_n(\mathbb{Z}_2) \). A Generator matrix for \( C \) is a \( k \times n \) matrix \( G \) that has rank \( k \). For message \( m \), \( c = mG \) is codeword,
see for detail on error correcting code (Vanstone and Oorschot, 1989; MacWilliams and Sloane, 1993). By reconstruction of generator matrix $G$, that is $G = (P^T S^{-1})^T$, the ciphertext of plaintext $m$ with length $k$ is $c = mG$. $S$ is a $k \times k$ non-singular matrix, and $P$ is a $k \times n$ matrix with rank $k$. Matrix $G$ is public to encrypt message $m$. The decryption to obtain message $m$ can be performed as follows: compute $c(S^T P)^T = mG(S^T P)^T = m(P^T S^{-1})^T (S^T P)^T = m(S^T)^T (P^T S)^T = m$.

The above description can be summarized as in Table 2 below.

<table>
<thead>
<tr>
<th>Public</th>
<th>$G = (P^T S^{-1})^T$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>$R = SP$</td>
</tr>
<tr>
<td>Encryption</td>
<td>$c = mG$</td>
</tr>
<tr>
<td>Decryption</td>
<td>$m = c R^T$</td>
</tr>
</tbody>
</table>

A key generation of the public key cryptosystem can be performed according to the following steps: (1) select $G_1 = [I_k A]$ with an arbitrary $k \times (n-k)$ matrix $A$, (2) select an arbitrary $k \times k$ nonsingular matrix $S$, (3) $P = SG_1$, (4) find a right inverse of $P$, i.e. $P^-$, (5) find inverse of $S$, i.e. $S^-$, (6) $G = (P^T S^{-1})^T$, (7) $R = SP$. Thus, $R$ is a private key and $G$ is a public key.

Properties of the Cryptosystem

1. **Key space.**

The public key space is size of $G$, which is $kn$ bits. Meanwhile, the private key space is size of $R$, which is also $kn$ bits. So, the total of key space needs $2kn$ bits.

2. **Encryption and decryption complexity.**

I assume that both binary addition and multiplication are bit operation. For encryption, computation $c = mG$ needs $(k + k - 1)n = (2k - 1)n = 2kn - n$. Encryption complexity is the order of $O(kn)$. For decryption, ciphertext $c$ has length $n$, so that computation $m = cR^T$ needs $(n + n - 1)k = (2n - 1)k = 2kn - k$. Decryption complexity is the order of $O(kn)$. Therefore, both encryption and decryption process needs $2kn - n + 2kn - k = 4kn - k - n$. So, encryption and decryption complexity are also the order of $O(kn)$.

3. **Message expansion.**

A cryptosystem is said to have message expansion if the length of ciphertext blocks is longer than the length of plaintext blocks. If $r$ denotes the proportion of the length of the ciphertext blocks from the length of plaintext blocks, in my cryptosystem $r = n/k$. 
Table 3. Comparison of cryptosystem

<table>
<thead>
<tr>
<th>Cryptosystem</th>
<th>Private key space</th>
<th>Public key space</th>
<th>Complexity of encryption and decryption</th>
<th>Ratio of message expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>My cryptosystem</td>
<td>( k^n )</td>
<td>( k^n )</td>
<td>( 4kn - n - k \rightarrow O(kn) )</td>
<td>( n/k )</td>
</tr>
<tr>
<td>McEliece</td>
<td>( k^2 + kn + n^2 )</td>
<td>( kn )</td>
<td>( 2kn + (2n-1)n + (2k-1)k \rightarrow O(n^2) )</td>
<td>( n/k )</td>
</tr>
<tr>
<td>Wu-Dawson</td>
<td>( n^2 )</td>
<td>( 2kn )</td>
<td>( n^2 + 3n^2 - 2n \rightarrow O(n^2) )</td>
<td>( n/k )</td>
</tr>
</tbody>
</table>

From Table 3 above, it can be concluded that the cryptosystem are:

1. efficient in key space, i.e. its total \( 2kn \) bits.
2. low complexity, i.e. the order of \( O(kn) \)
3. have a message expansion. This is a characteristic of cryptosystem based on coding theory.

Therefore the cryptosystem is efficient enough and faster in encryption and decryption than McEliece’s and Wu-Dawson’s cryptosystem.

**Risk Analysis**

The risk analysis is based on security of ciphertext \( c \), which is by possibly attacks by the intruder. If the intruder has known a private key \( R \), the ciphertext \( c \) can be broken. By computation \( m = cR^T \), the intruder will obtain message \( m \). The intruder will perhaps find out of the private key \( R \) by:

1. **Attack 1**: find a matrix that generate the private key \( R \). By procedure of key generation, \( P = SG_1 \), where \( G_1 = [I_k A] \). This means that matrix \( P \) depends on matrix \( S \) and \( A \). As a consequence, finding a matrix that generates matrix \( R \) means looking for a nonsingular matrix \( S_{n \times k} \) and an arbitrary matrix \( A_{k \times (n-k)} \). According to McWilliam and Sloane (1993), in the field of \( Z_2 = \{0,1\} \), the number of nonsingular matrix \( S = (2^k - 2^0)(2^k - 2^1)(2^k - 2^2) \ldots (2^k - 2^{k-1}) \). Meanwhile, the number of possibilities of matrix \( A \) is \( 2^{k(n-k)} \). So, the number of ways to findout the private key \( R \) is \( (2^k - 2^0)(2^k - 2^1)(2^k - 2^2) \ldots (2^k - 2^{k-1}) 2^{k(n-k)} \). It is very large to get one of the private keys \( R \).

2. **Attack 2**: find a right inverse of \( G \). Because of \( c = mG \), the message \( m \) will be found if the intruder got a right inverse of \( G \). Therefore, if \( G^* \) is right inverse of \( G \), by computation \( cG^* = mGG^* = ml_k = m \). Matrix \( G \) has a size \( kxn \) and rank \( k \), by lemma 1, the number of right
inverses of $G$ is $2^{(n-k)k}$. Matrix $G$ that satisfies the condition is only one. So, that the probability of the intruder will succeed is only $\frac{1}{2^{(n-k)k}}$. It is very small probability.

(3) \textit{Attack 3: try an arbitrary matrix $R$.} Matrix $R$ has size $kxn$, the number of element of matrix $R$ is $kn$. In the field $Z_2 = \{0, 1\}$, the number of possibilities of different matrix $R$ is $2^{kn}$. It is large enough to get one of the private keys $R$.

From above discussion, it can be concluded that if $k$ and $n$ are large, the ciphertext $c$ is still secure. I would like to point out that by removing error pattern in my cryptosystem, I hope my cryptosystem is still secure and efficient, because error patterns $e$, both in McElice’s and Wu-Dawson’s cryptosystem, became a weak key of the cryptosystem (Wu and Dawson, 1998).

\section*{Conclusion}

By the right inverses of matrices, a public key cryptosystem which has a good performance is proposed. It is shown that the theory of matrices became a potential tool in cryptographic research. The complexity of the matrix operation is low. Hence, it can work very quickly. It is anticipated that the theory of matrices over finite field may have more cryptographic applications.

I would like to remind that although I have found a method to find out right inverses in form (3), an efficient algorithm to find right inverses needs further investigation. Further research about authentication scheme of the cryptosystem is still needed.

\section*{References}


