MODIFIED RANDOM LINEAR CODE SCHEME (RLCE) WITH USING PROPERTIES OF AUTOMORPHISM GROUP OF GOPPA CODE

B.P Tripathi, Renuka Sahu
Department of Mathematics, Gov. N.P.G. College Of Science, Raipur (C.G), India.

ABSTRACT

McEliece cryptosystem is a public-key cryptosystem predicated on error-redressing codes. In 2016, Y. Wang[4] introduced another Scheme known as Random Linear Code encryption scheme. In this paper, we present a modification of the Random Linear Code encryption scheme which invigorates its security. For this we utilize some properties of the automorphism groups of Goppa codes. Also we have given modified decryption scheme to increases its complexity. This greatly fortifies the system against the decoding attacks.

Keywords:
Binary Goppa codes, Automorphism Group of Goppa codes, t-Tower Decodability, Frobenius automorphism, linear Code, McEliece encryption scheme.

1. INTRODUCTION

With rapid development for quantum computing techniques, our society is concerned with the security of current Public Key Infrastructures (PKI) which are fundamental for Internet services. The core components for current PKI infrastructures are based on public cryptographic techniques such as RSA and DSA. However, it has been shown that these public key cryptographic techniques could be broken by quantum computers. Thus it is urgent to develop public key cryptographic systems that are secure against quantum computing.

Since McEliece encryption scheme [1] was introduced more than thirty years ago, it has withstood many attacks and still remains unbroken for general cases. The original McEliece cryptographic system is based on binary Goppa codes. Several variants have been introduced to replace Goppa codes in the McEliece encryption scheme.

The underlying idea results from a trade-off between the strong security of the system against structural attack and its much weaker security regarding decoding attacks. In [4] paper proposed linear code based encryption scheme RLCE which shares many characteristics with random linear codes. We allow ourselves to reduce the size of the space of public-keys weakening the system against structural attacks to increase the security of the system regarding the decoding attacks. This can be done by using to some property of the automorphism group of Goppa codes. Namely, whenever the Frobenius automorphism lies in the automorphism group of the code we can generate large sets of decodable error-words of a larger weight than the constructed error-correcting capability of the code. We show that whenever such sets are used in the system, the cost decoding attacks is significantly increased.
2. PRELIMINARY:

2.1. Goppa Code

Construction and properties

A binary Goppa code is defined by a polynomial \( g(x) \) of degree \( t \) over a \( GF(2^m) \) without multiple zeros, and a sequence \( L \) of \( n \) distinct elements from \( GF(2^m) \) that aren’t roots of the polynomial:

\[
\forall i \in \{1, \ldots, n-1\} : L_i \in GF(2^m) \land L_i \neq L_1 \land g(L_i) \neq 0
\]

Codewords belong to the kernel of syndrome function, forming a subspace of \( \{0,1\}^n \):

\[
\Gamma(L, g) = \left\{ c \in \{0,1\}^n : \sum_{i=1}^{n} c_i \mod g(x) = 0 \right\}
\]

Code defined by a tuple \( (g, L) \) has minimum distance \( 2t + 1 \) thus it can correct \( t = \left\lfloor \frac{2t+1-1}{2} \right\rfloor \) errors in a word of size \( n - mt \) using codewords of size \( n \). It also possesses a convenient parity-check matrix \( H \) in form

\[
H = VD = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \xi(L_1) & \xi(L_2) & \cdots & \xi(L_n) \\
1 & \xi(L_1) & \xi(L_2) & \cdots & \xi(L_n) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \xi(L_1) & \xi(L_2) & \cdots & \xi(L_n) \\
\end{pmatrix}
\]

Note that this form of the parity-check matrix, being composed of a Vandermonde matrix \( V \) and diagonal matrix \( D \), shares the form with check matrices of alternant codes, thus alternant decoders can be used on this form. Such decoders usually provide only limited error-correcting capability (in most cases \( t/2 \)).

2.2. Automorphism Group of Goppa Codes

Suppose the support field is \( F_{2^m} \), and let \( L = (a_1, \ldots, a_n) \) be a labeling of the support field. Let us consider the Goppa code \( \Gamma(L, g) \) where the generating polynomial \( g \) has coefficients in a subfield \( F_{2^t} \) of \( F_{2^m} \). Then we have

The automorphism group of \( \Gamma(L, g) \) contains the group generated by the Frobenius automorphism \( \xi : k \mapsto k^{2^t} \) of \( F_{2^t} / F_{2^m} \).

This means that the code \( \Gamma(L, g) \) is invariant under the action of the Frobenius automorphism. If any word \( c \) of length \( n \) is labeled by \( L \), we have

\[
\forall \ c = (c_{a_1}, \ldots, c_{a_n}) \in \Gamma(L, g), \xi(c) = (c_{\xi(a_1)}, \ldots, c_{\xi(a_n)}) \in \Gamma(L, g)
\]

2.3. T-Tower Decodability

Let \( \varepsilon \) be a set of words of length \( n = 2^m \), let \( F_{2^t} \) be a subfield of \( F_{2^m} \) and \( \xi : k \mapsto k^{2^t} \) the Frobenius automorphism of the extension field. We say that \( \varepsilon \) is \( t \)-tower decodable if

1. for all \( e \in \varepsilon \), there exists a linear combination

\[
E = \sum_{i=0}^{t-1} e_i \xi^i(e), \quad e_i \in F_2
\]

having a Hamming weight less than \( t \), where \( \xi(e) \) denotes the action of the Frobenius on the word \( e \),

2. the knowledge of \( E \) enables the receiver to recover \( e \) in \( \varepsilon \) in a unique way.

In other words \( \varepsilon \) is a \( t \)-tower decodable set if there exists a linear combination of the powers of the Frobenius automorphism \( \xi \) that is a one-to-one mapping from \( \varepsilon \) into the vectors of length \( n \) and weight less than the correcting capability of the Goppa code.

The second condition in the definition is fundamental. It ensures that given a pattern we can invert all the operations to recover the original vector \( e \).

The first condition is simple to achieve:

Let us take \( \varepsilon \), the set of all the binary words \( e \) of length \( n \) satisfying

\[
\sum_{i=0}^{t-1} \xi^i(e) = 0
\]

However it does not satisfy the second condition. Namely every word in \( \varepsilon \) is mapped onto the null word.

t-tower decodability is intimately linked with classical decodability up to \( t \) in the family of Goppa codes with a non-trivial automorphism group:

Let \( \Gamma(L, g) \) be a Goppa code with generating vector of degree \( t \) over a subfield \( F_{2^t} \) of the support field \( F_{2^m} \), then any error vector of a \( t \)-tower decodable set \( \varepsilon \) is correctable in \( \Gamma(L, g) \).

3. RANDOM LINEAR CODE BASED ENCRYPTION SCHEME RLC

The Random Linear Code based Encryption scheme RLC proposed by Y Wang[4] proceeds as follows:
3.1. Key setup:

Let

\[ A = \begin{bmatrix} a_0 & \cdots & a_{n-1} \end{bmatrix} \]

be an \( n(r + 1) \times n(r + 1) \) nonsingular matrix.

(b) Let \( S \) be a random dense \( k \times k \) nonsingular matrix and \( P \) be an \( n(r + 1) \times n(r + 1) \) permutation matrix.

(c) Let \( k \times r \) matrices drawn uniformly at random \( x_0, x_1, \ldots, x_{r-1} \in GF(q)^k \times r \)

(d) \( k \times n(r + 1) \) matrix obtained by inserting the random matrices \( X_i \) into \( G_s \),

\[ G_A = [ g_0, x_0, g_1, x, \ldots, g_n, x_n ] \]

(e) The Public key is the \( k \times n(r + 1) \) matrix \( G = SG_A \) and the Private key is \( (S, G_s, P, A) \).

3.2. Encryption.

For a row vector message \( m \in GF(q)^k \), choose a random row vector \( e = [e_0, e_1, \ldots, e_{n(r+1)-1}] \in GF(q)^{n(r+1)} \) such that the Hamming weight of \( e \) is at most \( t \).

The cipher text is \( y = mG + e \).

3.3. Decryption.

For a received cipher text \( y = [y_0, y_1, \ldots, y_{n(r+1)-1}] \), compute

\[ y^{P^{-1}A^{-1}} = [y_{(r+1)}, \ldots, y_n] = mS + e \]

where

\[ A = \begin{bmatrix} a_0 & \cdots & a_{n-1} \end{bmatrix} \]

Let \( y_0 = [y_0, y_1, \ldots, y_{n(r+1)-1}] \) be the row vector of length \( n \) selected from the length \( n(r + 1) \) row vector \( y^{P^{-1}A^{-1}} \). Then \( y_0 = mS + e_0 \) for some error vector \( e_0 \in GF(q)^n \).

Using the efficient decoding algorithm,

One can compute \( m = mS \) and \( m = mS^{-1} \).

Finally, calculate the Hamming weight \( w = \text{weight}(y - mG) \). If \( w \leq t \) then output \( m \) as the decrypted plaintext. Otherwise, output error.

The stake of the system anticipate the difficult setback of decoding a convenience up to its error-correcting capability.

4. MODIFIED DECRYPTION SCHEME

Space of Secret Keys Let \( g_1 \) be an irreducible polynomial of degree \( t \) over \( F_{2^m} \). \( g_1 \) is called hiding polynomial. Let \( G \) be the family of the Goppa codes \( \Gamma(L, g) \) where \( g \) describes the family of irreducible polynomials of degree \( t \) over a subfield \( F_{2^e} \) of \( F_{2^n} \).

In our modified scheme the key setup, private key, public key and encryption procedure are almost same as per RLCE Scheme by Y.Wang[4].

4.1. Private Key

(a) \( k \times n \)-generating matrix \( G \) of a code \( \Gamma(L, g) \) randomly chosen in \( G \),

(b) \( n \times n \) permutation matrix \( P \),

(c) \( k \times k \) non-singular matrix \( S \),

(d) \( n(r + 1) \times n(r + 1) \) non-singular matrix \( A \).

4.2. Public Key

To the difference of the original scheme it consists in two parts:

(a) the product \( G\| = S G_A \),

(b) the way to generate a \( t \)-tower decodable set \( e \).

4.3. Encryption

Let \( z \) be the \( k \)-bit message that has to be transmitted. The sender chooses randomly a word \( e \) in \( e \), then sends \( z\| = zG\| + e \).

4.4. Decryption

The receiver first computes

\[ c = z\|P^{-1}A^{-1} \]

\[ = (zG\| + e)P^{-1}A^{-1} \]

\[ = zG\|P^{-1}A^{-1} + eP^{-1}A^{-1} \]

\[ = zS G_A P^{-1}A^{-1} + eP^{-1}A^{-1} \]

Since \( e \) is in the \( t \)-tower decodable set, from Definition of \( t \)-tower decodability there is a linear combination

\[ \sum_{i=0}^{m} b_i \xi^i(e) \]

of weight less than the error correcting capability \( t \) of \( \Gamma(L, g) \).
The receiver computes
\[\sum_{i=0}^{n-1} b_i \xi_i (z^{p-1}A^{-1}) = \sum_{i=0}^{n-1} b_i \xi_i (zSG) + \sum_{i=0}^{n-1} b_i \xi_i (e^{p-1}A^{-1})\]

Note that \(zSG\) is a word in the code \(\Gamma(L, g)\). However, by construction, \(\Gamma(L, g)\) is a subcode of \(\Gamma(L, g)\). Therefore we can consider that \(zSG\) is a word in \(\Gamma(L, g)\). Moreover, since \(\xi\) is in the automorphism group \(\Gamma(L, g)\) by construction,
\[\sum_{i=0}^{n-1} b_i \xi_i (zSG) = 0\]

is also a codeword of \(\Gamma(L, g)\). Since \(p^{-1}\) is a permutation we have
\[\sum_{i=0}^{n-1} b_i \xi_i (e^{p-1}A^{-1}) = \left(\sum_{i=0}^{n-1} b_i \xi_i (e)\right) p^{-1}A^{-1}\]

which is a decodable pattern in \(\Gamma(L, g)\).

The receiver gets thus the vector \(E = \left(\sum_{i=0}^{n-1} b_i \xi_i (e)\right)\) of weight less than \(t\). \(E\) can thus be recovered by applying the decoding algorithm of \(\Gamma(L, g)\). The knowledge of \(E\) provides a unique way to find \(e\).

Once receiver knows \(e\), then the code easily be revealed by removing that errors.

**4.5. Conditions on \(E\)**

From a cryptological point of view, the t-tower decodable set must satisfy the following conditions:

(a) \(E\) has to be a set of words of weight larger than the error-correcting capability of the code. This conditions strengthens the system against decoding attacks,

(b) \(E\) has to be large enough to avoid enumeration.

(c) the way to generate \(E\) must be public, and must not reveal information that could help an attacker

**4.6. Complexity of the Modified Scheme**

The complexity of the encryption is exactly the same as in the original system, since consisting in matricial products and picking up a random vector. The decryption requires additional operations. However, the cost strongly depends on the structure of the t-tower decodable set \(E\).

The complexity of RLCE is low as comparison to RSA but its complexity is more than McEliece scheme[2].

For **Encrypting the message** the work factor is :
\[W^C = \frac{nk}{2}\]

For **Decoding the message** the work factor is :
\[W^D = 3mnt + 4m^2t^2 + \frac{kt^2}{2}\]

(a) Number of binary operations per information bit for encryption:
\[\frac{W^C}{k} = 180\]

which is smaller than the binary operations per information bit required in the McEliece encryption procedure.

(b) Number of binary operations per information bit for the decryption:
\[\frac{W^D}{k} = 11748\]

which is much larger than the binary operations per information bit required in the McEliece decryption procedure.

**4.7. Importance of the Hiding Polynomial \(G_1\)**

We introduced the concept of hiding polynomial \(g_1\) to satisfy the third condition on \(E\). If we used for \(G\) the family of irreducible Goppa codes with generating polynomial over \(F_{2^n}\), by applying the support splitting algorithm to the public key \(G\) any attacker would be able to recover \(\xi\). Then one could apply linear transformations of the Frobenius automorphism and reduce the problem of finding the error vector \(e\) to the problem of finding the vector \(E\) of lower weight.

The codes \(\Gamma(L, g_1)\) are subcodes of the codes \(\Gamma(L, g)\) with a large structure. The introduction of the hiding polynomial scrambles the structure of the code rendering the automorphism group of \(\Gamma(L, g_1)\) trivial. Moreover, the hiding polynomial \(g_1\) can be published since its knowledge does not give any exploitable information.

**4.8. An example in support of our scheme**

The action of the Frobenius automorphism makes some orbits in the field. In [5] considered the field extension of size 5 for the action of Frobenius automorphism. And here for simplicity, we consider the field extension \(F_{2^7}\) of \(F_{2^3}\) and the corresponding Frobenius automorphism.
The definition of a decodable vector e follows:

\[ \xi : \mathbf{k} \to \mathbf{k}^{2^s} \]

The action of the Frobenius automorphism to \( \mathbb{F}_{2^s} \) makes \( N_z = (2^{2s} - 2^s)/7 \) orbits of size 7 and \( 2^s \) orbits of size 1.

In other words, a word \( \{z_{a_1}, z_{a_2}, \ldots, z_{a_m}\} \) can be rewritten in the following form after reordering its labeling \( L \):

\[ z = \{Z_1, Z_2, \ldots, Z_{N_z}, Z_0\} \]

where

\[ Z_i = [z_{\alpha_1}, z_{\alpha_2}, \ldots, z_{\alpha_{2^s}}] \]

for \( i \in \{1, \cdots, N_z\} \) denotes an orbit of length 7 generated by \( (\alpha_j) \), and then \( Z_0 \) denotes a sub-vector of length \( 2^s \) corresponding to the \( 2^s \) orbits of length 1 generated by \( 2^s \) distinct elements in \( \mathbb{F}_{2^s} \).

For the reordered coordinate, the action of the Frobenius automorphism \( \xi \) on a word \( x \) is given as follows:

\[ \xi(x) = \{\xi(Z_1), \ldots, \xi(Z_{N_z}), Z_0\} \]

where \( \xi(Z_i) \) is a left cyclic shift in \( Z_i \).

For example, for \( Z_{i_1} = \{1, 1, 1, 0, 0, 0, 0\} \) and \( Z_{i_2} = \{1, 1, 1, 0, 1, 0, 0\} \),

\[ \xi^1(Z_{i_1}) \text{ and } \xi^1(Z_{i_2}) \text{ for } l \in \{1, \ldots, 2^s\} \text{ are listed as follows:} \]

\[ (Z_{i_1}) = \{1, 1, 1, 0, 0, 0, 0\}, \quad (Z_{i_2}) = \{1, 1, 0, 1, 0, 1, 1\}, \]

\[ \xi^1(Z_{i_1}) = \{1, 1, 1, 0, 0, 0, 1\}, \quad \xi^1(Z_{i_2}) = \{1, 0, 1, 1, 1, 1, 0\}, \]

\[ \xi^2(Z_{i_1}) = \{1, 1, 0, 0, 0, 0, 1\}, \quad \xi^2(Z_{i_2}) = \{0, 1, 0, 1, 1, 1, 0\}, \]

\[ \xi^3(Z_{i_1}) = \{1, 0, 0, 0, 1, 1, 1\}, \quad \xi^3(Z_{i_2}) = \{1, 0, 1, 1, 1, 0, 0\}, \]

\[ \xi^4(Z_{i_1}) = \{0, 0, 0, 1, 1, 1, 1\}, \quad \xi^4(Z_{i_2}) = \{0, 1, 1, 1, 1, 0, 0\}, \]

\[ \xi^5(Z_{i_1}) = \{0, 0, 0, 1, 1, 1, 0\}, \quad \xi^5(Z_{i_2}) = \{1, 1, 1, 1, 1, 0, 0\}, \]

\[ \xi^6(Z_{i_1}) = \{0, 0, 1, 1, 1, 1, 0\}, \quad \xi^6(Z_{i_2}) = \{1, 1, 0, 1, 0, 1, 0\}. \]

### 4.8.1. t-Tower Decodable Vector

In the Loidreau’s modified cryptosystem [2], t-tower decodable vectors are used instead of random error vectors of weight \( t \).

The definition of a t-tower decodable vector is given as follows:

**Definition 1 (t-Tower Decodable Vector)** a t-tower decodable vector \( e \) is a word of length \( n \) satisfying the following three conditions:

- Larger-weight: \( \text{Hw}(e) > t \)
- Reducibility: There exists a linear combination \( f(\cdot) \) such that \( \text{Hw}(e) \leq t \) where
  \[ e = \sum_{i=0}^{m-1} b_i \cdot \xi_i(e), \quad \xi_i \in f_2 \]
- Recoverability: \( e \) is uniquely recoverable from the above

In [2], t-tower decodable vector \( e \) is generated as follows:

#### 4.8.2. Generation of a t-Tower Decodable Vector

**Output:** a t-tower decodable vector \( e \)

1. Set all the coordinates of \( e \) to 0.
2. Choose randomly \( p = \lfloor t/2 \rfloor \) orbits out of the \( N_z \) orbits of length 7.
3. Flip 4 bits each at random in the chosen \( p \) orbits.

The following \( f_1(\cdot) \) or \( f_2(\cdot) \) where

\[ e = f_1(e) = e + \xi(e) + \xi^2(e) \]

\[ e = f_2(e) = e + \xi^2(e) + \xi^3(e) \]

reduces the weight of \( e \) within \( t \) since \( \xi^i(Z_{i_t}) \) or \( \xi^i(Z_{i_t}) \) cover all the patterns of a vector of length 7 and weight 4, and then they are transformed into the following patterns:

\[ f_1(\xi^i(Z_{i_t})) = \xi^i(Z_{i_t}) + \xi(Z_{i_t}) + \xi^2(Z_{i_t}) \]

\[ f_2(\xi^i(Z_{i_t})) = \xi^i(Z_{i_t}) + \xi^2(Z_{i_t}) + \xi^2(Z_{i_t}) \]

\[ f_3(\xi^i(Z_{i_t})) = \xi^i(Z_{i_t}) + \xi^2(Z_{i_t}) + \xi^3(Z_{i_t}) \]

\[ f_4(\xi^i(Z_{i_t})) = \xi^i(Z_{i_t}) + \xi^2(Z_{i_t}) + \xi^3(Z_{i_t}) \]

The patterns \( Z_{i_t} \) and \( Z_{i_t} \) play dual roles. There exist linear combinations of \( Z_{i_t} \) and \( Z_{i_t} \) of their Frobenius images that enables one to reduce the weight of one pattern from 4 to 1 preserving the weight of the other. The average weight of the pattern is thus decreased. Namely we have where \( \xi^i(\cdot) \) denotes a \( i \)-bit left cyclic shift.

More formally, let \( p_1 \) and \( p_2 \) denote the number of \( \xi^i(Z_{i_t}) \) for any \( i \) and \( \xi^i(Z_{i_t}) \) for any \( i \) in \( e \), respectively. Since

\[ p_1 + p_2 = \lfloor t/2 \rfloor \]

\[ \min(f_1(e), f_2(e)) = \min(3p_1 + p_2, p_1 + 3p_2) \]
\[= \min\left(\frac{2}{g_1y} + \frac{t}{2}, \frac{t}{2} + \frac{2}{g_2y}\right)\]
\[\leq 2 \cdot \frac{t}{2}\]
\[\leq t,\]

one can reduce the weight of \(e\) within \(t\) using either \(f_1()\) or \(f_2()\).

Using the corrected vector \(e\), one can uniquely recover the corresponding \(t\)-tower decodable vector \(e\) since both \(f_1()\) and \(f_2()\) are one-to-one mappings.

The optimal parameters for \(e\) are \(2p = t\). In this case each word in \(e\) has weight \(3t/2\). With this method one can decode up to one half beyond the error-correcting capability \(t\).

5. APPLICATION TO THE CRYPTOSYSTEM

Section 4 was dedicated to the modification of Random linear code encryption scheme by using the general properties of \(t\)-tower decodability to strengthen the system against decoding attacks. In this section we apply this modification with the \(t\)-tower decodable sets previously defined over extensions of degree 7. In particular we show that it is possible to publish how to generate \(e\) without giving the possibility for an attacker to reduce the complexity of the attacks on the system.

5.1. Parameters of the System

Family of Goppa Codes As a hiding polynomial we take an irreducible polynomial \(g_1\) of degree 2 over \(F_{2^7}\). Let \(L\) be a labeling of the field \(F_{2^7}\), we consider the family \(G\) of Goppa codes \( \Gamma(L, g_1g) \) where \(g\) has degree \(t\) and coefficients over \(F_{2^7}\).

Private Key

It consists of 4 parts:

- a \(k \times n\)-generating matrix \(G\) of a code \( \Gamma(L, g_1g) \) randomly chosen in \(G\)
- a \(n \times n\) permutation matrix \(P\),
- a \(k \times k\) non-singular matrix \(S\),
- a \(n(r + 1) \times n(r + 1)\) nonsingular matrix \(A\).

Public Key

It consists in two parts

- the product \(G\theta = S G_{r}AP\),

\[z P^{-1} A^{-1} = z S G_{\theta} + e P^{-1} A^{-1}\]

Since permuting the coordinates does not change the structure of the automorphism group, we can consider that \(e P^{-1} A^{-1}\) is still in \(e\). It was shown in section 4 that \(e\) is \(t\)-tower decodable, therefore by applying the right linear combinations of the powers of the Frobenius automorphism, the receiver first recovers \(e P^{-1} A^{-1}\), then recovers \(z\).

5.3 Security of the System

In the conception of the scheme the positions of the \(N_{7}\) orbits of cardinality 7 in the generating vector \(L\).

Note that if the positions of the orbits are in some way canonical the size of the public-key can be made as low as the size of \(G\).

5.2 Encryption-Decryption

Since the positions of the orbits are public, the sender can generate the set \(\epsilon\) of \(t\)-tower decodable words described in the previous section.

Encryption

Let \(z\) be the \(k\)-bit plaintext one has to transmit, the sender chooses randomly a word \(e\) in \(\epsilon\) he first picks up \(\lfloor t/2 \rfloor\) orbits out of the \(N_{7}\) possible and puts randomly 4 bits on each orbit.

The corresponding ciphertext is \(z^\theta = z G\theta + e\).

Decryption

The receiver computes \(z = z S G_{\theta} + e P^{-1} A^{-1}\). By considering the Random linear code parameters we show that this system provides a better security against decoding attacks than the original scheme.

Table 1. Comparison between McEliece Scheme and Modified RLCE Scheme.
From the above graph it is shown that on encrypting any message it takes less operation but for decryption it requires more binary operation and thus increases its complexity.

6. CONCLUSION

In the paper, properties of automorphism group of Goppa codes are used to increase the security and complexity of Random Linear Code encryption scheme. However, in the example developed above concerning the extensions of degree 7 the size of the family of codes to enumerate remains largely beyond the capabilities of the computers. Such an approach can be generalized to any finite field extension. Still, in that case the problem is to find t-tower decodable sets satisfying the simple cryptographical constraints such as being a large set of large-weight words. The ideal would be to find a decodable set whose words have weight larger than half of the code-length.
7. REFERENCE


