On the Structure of Randomly Permuted Concatenated Code

Nicolas Sendrier

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On the Structure of Randomly Permuted Concatenated Code

Nicolas SENDRIER

N° 2460

Janvier 1995

PROGRAMME 2

Rapport de recherche

On the Structure of Randomly Permuted Concatenated Code

—

Structure d'un Code Concaténé Permuté Aléatoirement

Nicolas Sendrier

Projet CODES,
INRIA, Domaine de Voluceau, Rocquencourt,
BP 105, 78153 Le Chesnay CEDEX, FRANCE

Abstract

Our purpose here is to show how it is possible to recover the structure of a randomly permuted concatenated code, and how to use this information for decoding. This result prohibits the use of first order concatenated codes in public-key cryptosystems based on error-correcting codes.

Résumé

Nous montrons ici comment il est possible de reconstituer la structure d'un code concaténé permuté aléatoirement et comment utiliser cette information pour le décodage. Ce résultat met en cause l'utilisation des code concaténés du premier ordre dans les systèmes de chiffrement à clé publique basés sur les codes correcteurs d'erreurs.

On the Structure of Randomly Permuted Concatenated Code

Nicolas Sendrier *

1 Introduction

In order to build a cryptosystem based on error-correcting codes, we need a family of linear codes with given parameters, that has some "good" cryptographic properties. The family must be large enough to forbid an exhaustive attack, and each code of the family must have a decoding algorithm of low algorithmic complexity to allow an easy decryption. Additionally, the codes should be such that after a random permutation of the coordinates, the algebraic structure of doesn't show.

In the two known systems, proposed by McEliece [McE78] and Niederreiter [Nie86], the public key is a permuted version of the code, either a permuted generating matrix (McEliece) or a permuted parity check matrix (Niederreiter).

There are two possible attacks of these systems. The first one consists in a try to decode a given encrypted message. We will refer to this as the direct attack, and it basically consist in decoding a random linear code. The second possible attack, the structural attack, consist in a try to recover the structure, or part of the structure, of the original code from the public key.

McEliece proposed in his original paper to use 50-error-correcting binary Goppa codes of length 1024. These codes are resistant to the direct attacks [LB88, vT90, Cha94, CC94], and no structural attack is known.

Sidelnikov and Shestakov gave a successful structural attack of a scheme using Generalized Reed-Solomon codes [SS92].

We investigate here the use of first order concatenated codes. These codes offer the advantage of a lower decoding complexity at the cost of a larger key size. We present a structural attack of a system based on such codes. The attack is practical with code parameters that are resistant to the direct attacks.

2 McEliece and Niederreiter cryptosystems

We consider a family of $C(n, k, \geq d)$ linear codes over $GF(q)$ that possess a low complexity d-bounded decoding procedure. Let $t = (d-1)/2$, $r = n - k$. Both Φ_C and Ψ_C used below

*Projet CODES, INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay CEDEX, FRANCE

are procedures that can be easily derived from the decoding procedure of C.

2.1 Description

McEliece cryptosystem

- **Secret key:**
  - an element C of the family,
  - a $k \times k$ non-singular matrix S,
  - a $n \times n$ permutation matrix P.
- **Public key:** $G' = SGP$, where G is a generating matrix of C.
- **Encryption:** $m \longrightarrow mG' + e$, e a random vector of weight t.
- **Decryption:** $y \longmapsto \Phi_C(yP^{-1})S^{-1}$, with $\Phi_C(xG + e) = x$ whenever the weight of e is t or less.

Niederreiter cryptosystem

- **Secret key:**
  - an element C of the family,
  - a $r \times r$ non-singular matrix S,
  - a $n \times n$ permutation matrix P.
- **Public key:** $H' = SHP$, where H is a parity check matrix of C.
- **Encryption:** $m \longrightarrow H'm^T$, the message m is of weight t.
- **Decryption:** $y \longmapsto \Psi_C(S^{-1}y)P$, with $\Psi_C(Hm^T) = m$ whenever the weight of m is t or less.

2.2 Goppa codes

Let n, m and t be positive integers, let $L = \{\alpha_1, \ldots, \alpha_n\}$ be an ordered subset of $GF(q)^m$ and let $g(z)$ be a monic polynomial in $GF(q^m)[z]$ of degree t such that $g(\alpha_i) \neq 0$ for all α_i in L.

The Goppa code $\Gamma(L, g)$ is the set of vectors $a = (a_1, \ldots, a_n)$ in $GF(q)^n$ such that

$$R_a(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i} \equiv 0 \mod g(z)$$

The code $\Gamma(L, g)$ has a minimum distance greater or equal to the designed distance $\delta = t + 1$ and a dimension at least equal to $n - rm$. There exists a δ-bounded (*i.e.* $(\delta - 1)/2$-error-correcting) decoding procedure of $\Gamma(L, g)$ with algorithmic complexity $O(n\delta)$.

Proposition 1 [MS77, p. 342] *If $g(z)$ is square-free, then $\Gamma(L, g) = \Gamma(L, g^2)$. Thus the minimum distance of $\Gamma(L, g(z))$ is at least equal to $2t + 1$.*

This proposition provides a t-error-correcting algorithm of $\Gamma(L, g)$ when $g(z)$ has no squared factor.

2.3 Parameters

McEliece uses a family of binary Goppa codes of length $n = 1024$, with $L = GF(1024)$ and $g(z)$ monic square-free in $GF(1024)[z]$ of degree $t = 50$. The codes obtained will have a dimension $k \geq 524$ and a designed distance $\delta = 2t + 1 = 101$. The actual minimum distance and dimension of these codes may be larger.

The characteristics of the two systems with this family are the following:

McEliece:

- Key size: 67 072 bytes.
- Transmission rate: 0.512.
- Number of codes: $\approx 2^{498}$.

Niederreiter:

- Key size: 32 750 bytes.
- Transmission rate: 0.568.
- Number of codes: $\approx 2^{498}$.

Remarks on the parameters:

- The substantial difference in the key sizes is due to the fact that Niederreiter system allows a public key in systematic form at no cost for security, as stated below.

  Proposition 2 *Let H' be the public-key of a cryptosystem using Niederreiter scheme. Let $\bar{H}' = UH'$ be a systematic form the parity check matrix H'. Any attack able to break a scheme using $\bar{H}'$ is able to break a scheme using H'.*

  Proof: Let W_t denote the set of words of weight t in $GF(q)^n$. We consider the two encryption procedures

  $$\begin{array}{rcccc} N & : & W_t & \longrightarrow & GF(q)^{n-k} \\ & & m & \longmapsto & H'm^T \end{array} \quad \text{and} \quad \begin{array}{rcccc} \bar{N} & : & W_t & \longrightarrow & GF(q)^{n-k} \\ & & m & \longmapsto & \bar{H}'m^T \end{array}$$

  These two mappings are injective. Let's assume that we have an oracle Φ able to compute $m = \Phi(y) = \bar{N}^{-1}(y)$ for all column vector y in $\bar{N}(W_t)$.

  Let y be an element of $N(W_t)$, we have $y = N(m) = H'm^T$ for some m in W_t. The column vector $Uy = UN(m) = UH'm^T = \bar{N}(m)$ is in $\bar{N}(W_t)$, and $\Phi(Uy) = m$. The oracle Φ can be used for breaking N. □

- The transmission rate for McEliece system is equal to k/n, that is the number of information symbols divided by the number of transmitted symbols.

  For Niederreiter system the number of possible messages is the number of q-ary words of weight t and length n, and the number of transmitted symbols is $n - k$. Thus the transmission rate is

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

- The number of codes is the number of monic square-free polynomials of degree 50 in $GF(1024)[z]$ that are relatively prime to $z^{1024} - z$.

Proposition 3 [LN83, pp. 92–93] *The number of monic irreducible polynomial of degree t over $GF(q)$ is equal to*

$$N_q(t) = \frac{1}{t} \sum_{s|t} \mu\left(\frac{t}{s}\right) q^s$$

where μ is the Moebius function.

The generating serie of the monic square-free polynomial over $GF(q^m)$ is given by

$$\prod_{s>0} (1 + z^s)^{N_{q^m}(s)}$$

(the number of such polynomials of degree t is equal to $[z^t]S(z)$, the coefficient of z^t in $S(z)$). And to obtain the number of such polynomials that are relatively prime to $z^{q^m} - z = \prod_{\beta \in GF(q^m)} (z - \beta)$ we just have to take out the factors of degree 1. Thus the generating serie is

$$S(z) = \prod_{s>1} (1 + z^s)^{N_{q^m}(s)}$$

Of course the formula for $S(z)$ cannot be computed, but we have $[z^t]S(z) = [z^t]\bar{S}(z)$ with

$$\bar{S}(z) = \prod_{s=1}^{t} \left(\sum_{i=0}^{\lfloor t/s \rfloor} \binom{N_q(s)}{i} z^{is} \right)$$

where $\lfloor \cdot \rfloor$ denotes the integer part, and $[z^t]\bar{S}(z)$ can be computed.

The number of monic square-free polynomials of degree 50 in $GF(1024)[z]$ that are relatively prime to $z^{1024} - z$ is $2^{498.56}$. Note that this number is very close do 2^{500} the number of monic polynomials of degree 50 in $GF(1024)[z]$.

2.4 Cryptanalysis

The cryptanalysis of the two systems are equivalent [LDW94]. There are mainly two guidelines to cryptanalyze these systems:

1. Decode a random linear code.

2. Recover the original structure of the code from the public key.

The first attack has been investigated at length in the last few years. Its efficiency is usually expressed as the average number of bits operation, called work factor, necessary to decode one instance of the cryptosystem.

In the original paper, McEliece gives a direct attack with a work factor of 2^{81}. A first improvement [LB88] leads to a work factor of 2^{71}, and the best known attacks today [Cha94, CC94] have a work factor of 2^{66}.

The knowledge of the structure of Goppa codes didn't allow, up to now, an efficient structural attack of Goppa codes. However, some other families are not safe, Sidelnikov and Shestakov [SS92] proved that the structure of a generalized Reed-Solomon code cannot be hidden by a permutation of the support.

3 Using first order concatenated codes in Niederreiter cryptosystem

Here an after we consider here the use a first order concatenated code in Niederreiter cryptosystem.

3.1 First order concatenated codes

3.1.1 Definition

Let's consider:

- a linear code $B(n_B, k_B, d_B)$ over $GF(q)$, called inner code,
- a linear code $E(n_E, k_E, d_E)$ over $GF(q^{k_B})$, called outer code,
- an isomorphism $\theta : GF(q^{k_B}) \rightarrow B$ of vector space over $GF(q)$.

We will denote by Θ the mapping:

$$\begin{array}{cccc} \Theta & : & (GF(q^{k_B}))^{n_E} & \longrightarrow & B^{n_E} \\ & & (a_1, \ldots, a_{n_E}) & \longmapsto & (\theta(a_1), \ldots, \theta(a_{n_E})) \end{array}$$

By definition the first order concatenated code of inner code B and outer code E is:

$$\mathcal{C} = B \Box_\theta E = \Theta(E)$$

3.1.2 Generating matrix

Let α be a primitive element of $GF(q^{k_B})$, the set $(1, \alpha, \ldots, \alpha^{k_B-1})$ is a basis of $GF(q^{k_B})$ over $GF(q)$, and the $k_B \times n_B$ matrix

$$G_{\theta,\alpha} = \begin{pmatrix} \theta(1) \\ \theta(\alpha) \\ \vdots \\ \theta(\alpha^{k_B-1}) \end{pmatrix} \tag{1}$$

is a generating matrix of B.

For any β in $GF(q^{k_B})$ we denote by A_β the matrix of the $GF(q)$-vector-space homomorphism of $GF(q^{k_B})$ that maps any element x into βx. The matrix A_0 is zero, and for any integer i in $\mathbf{Z}$, we have $A_{\alpha^i} = A_\alpha{}^i$.

Let $G_E = (\beta_{i,j})_{0 \le i < k_E, 0 \le j < n_E}$ be any generating matrix of E. Then the bloc matrix

$$\left(A_{\beta_{i,j}} G_{\theta,\alpha}\right)_{0 \le i < k_E, 0 \le j < n_E}$$

is a generating matrix of $\mathcal{C} = B \Box_\theta E$.

3.1.3 Parameters

In order to use error-correcting codes for public-key cryptosystems, we need a family of linear codes over $GF(q)$ of length n, dimension k, minimum distance $d \geq 2t+1$, and a low complexity decoding algorithm able to correct any t errors in a bloc.

We consider first order concatenated codes constructed from:

- a random binary inner code $B(16,7,5)$,
- a generalized Reed-Solomon (GRS) outer code $E(128,44,85)$ over $GF(2^7)$.

This leads to concatenated codes of parameters

$$B\square E = \mathcal{C}(2048, 308, \geq 425).$$

For these codes we have an efficient algorithm that can correct up to 212 errors in a bloc. The cost of the decoding is at most one third of the cost of the decoding of a 50-error-correcting binary Goppa code of length 1024.

Niederreiter cryptosystem using the concatenated codes described above have the following parameters:

- Key size: 66 990 bytes.
- Transmission rate: 0.562.
- Number of codes: $\approx 2^{944}$.

The number of binary codes of length n and dimension k is equal to [MS77, p. 698]:

$$\frac{(2^n-1)(2^n-2)\dots(2^n-2^{k-1})}{(2^k-1)(2^k-2)\dots(2^k-2^{k-1})}$$

Among these, we estimate that about 0.33% are of minimum distance greater or equal to 5 – We have generated $5\,10^8$ random codes of length 16 and minimum distance 7, among these, 1677051 had minimum distance 5 and 58 had minimum distance 6.

The number of distinct GRS codes of length 128 and given (non trivial) dimension over $GF(128)$ is 127^{127}.

Resistance to known attacks The Lee-Brickell work factor for the correction of 212 errors in a binary code of length 2048 and dimension 308 is 2^{71}, the same as for the Goppa codes of McEliece.

3.2 Some definitions

Definition 1 *The* support *of a word x in $GF(q)^N$, denoted* supp(x)*, is the set of its non zero position. By extension the support of a set is the union of the support of its elements.*

Definition 2 *Two linear codes C and C' of length n over $GF(q)$ are* equivalent *if there exist a permutation matrix P such that for any generating matrix G of C, the matrix $G' = GP$ is a generating matrix of C'.*

Definition 3 *Let $GF(q^m)$ be an extension of $GF(q)$, the* Frobenius field automorphism *of $GF(q^m)$ relatively to $GF(q)$ is the mapping*

$$\begin{array}{rcccc} F_q & : & GF(q^m) & \longrightarrow & GF(q^m) \\ & & x & \longmapsto & x^q \end{array}$$

Note that any power of F_q is also a field automorphism of $GF(q^m)$.

Definition 4 *Two linear codes C and C' of length n over $GF(q^m)$ are* F_q-equivalent *if there exist a permutation matrix P and a power F_q^s of the Frobenius such that for any generating matrix G of C, the matrix $G' = \overline{GP}$ is a generating matrix of C', where $\overline{GP}$ is obtained by applying F_q^s to the coefficients of GP.*

4 Structural attack

Let's consider the first order concatenated code $\mathcal{C}_o = B_o(n_B, k_B, d_B)\square_{\theta_o}E_o(n_E, k_E, d_E)$ over $GF(q)$. We assume that we know the code $\mathcal{C}'_o$ obtained from $\mathcal{C}_o$ by a random permutation of the support, and we wish to recover a concatenated structure of this code, that is a concatenated code $\mathcal{C} = B\square E$ equivalent to $\mathcal{C}'_o$. Note that B and E need not to be equal to the original inner and outer codes.

4.1 B-blocs of a concatenated code

Definition 5 (B-blocs) *For all i, $1 \leq i \leq n_E$, let e_i be the element of $GF(q^{k_B})$ with a "1" in i-th position and zeros everywhere else. We denote by* Vect(e_i) *the vector-space generated by e_i. The i-th B-*bloc *of the concatenated code $B\square_\theta E$ is defined to be the support of $\Theta(\mathrm{Vect}(e_i))$.*

4.1.1 Connected codes

Definition 6 *Two words x and y in $GF(q)^n$ are said to be* connected *if*

$$\mathrm{supp}(x) \cap \mathrm{supp}(y) \neq \emptyset.$$

Two positions i and j are said to be connected *by a subset S if there exist a sequence of words $x_0, x_1, \ldots, x_l$ in S such that*

- $i \in \mathrm{supp}(x_0)$ *and* $j \in \mathrm{supp}(x_l)$
- *for all i, $0 \leq i < l$, x_i and x_{i+1} are connected.*

A subset S of $GF(q)^n$ is said to be a connecting set *of a set I of positions (in short S connects I), if any two elements of I are connected by S. In particular, we have $I \subset \bigcup_{x \in S} \mathrm{supp}(x)$.*

procedure get_bloc($\mathcal{C}$)
    $j \leftarrow 0$
1: $x \leftarrow$ get_new_small_weight_codeword($\mathcal{C}^\perp$)
    for i **from** 1 **to** j **do**
        if $L_i \cap \operatorname{supp}(x) \neq \emptyset$ **then**
            $L_i \leftarrow L_i \cup \operatorname{supp}(x)$, **if** $|L_i| = n_B$ **then return**(L_i) **else goto** 1
    $j \leftarrow j+1$, $L_j \leftarrow \operatorname{supp}(x)$, **goto** 1

Table 1: Procedure to compute one B-bloc of $\mathcal{C}$

4.1.2 Dual of a concatenated code

Proposition 4 *[ZL84] If $B^\perp \neq \{0\}$, the dual distance of C is at most $d_B^\perp$.*

Proposition 5 *Any word of $C^\perp$ of Hamming weight less than $\min(d_E^\perp, 2d_B^\perp)$ has its support included in a single B-bloc.*

If the set $E_{B^\perp} = \{x \in B^\perp, d_B^\perp \leq w_H(x) < 2d_B^\perp\}$ connects $\operatorname{supp} B^\perp$, then the set $E_{\mathcal{C}^\perp} = \{x \in \mathcal{C}^\perp, d_B^\perp \leq w_H(x) < 2d_B^\perp\}$ connects any B-bloc of $\mathcal{C}$, and from Proposition 5 it cannot connect a set containing positions in more than one B-blocs.

Thus by computing all the codewords of weight $d^\perp$ to $2d^\perp - 1$ in $\mathcal{C}^\perp$, we can recover the B-blocs. In practice, it is not necessary to compute all these word, because there are many small subsets of $E_{\mathcal{C}^\perp}$ that will connect a given B-bloc. For instance the procedure described in Table 1 can be used.

If $d_B^\perp$ is small, computing $d_B^\perp$ is easy, and getting words of weight smaller than $2d_B^\perp$ in $\mathcal{C}^\perp$ can be efficiently done by any of the know algorithms [Leo88, Ste89, Cha94, CC94]. This procedure proved to be efficient for the proposed parameters; we obtained the 128 B-blocs in about one minute with a program in C running on a workstation DEC 3000.

4.2 Permutation between two equivalent codes

The problem we wish to solve now that we have the B-blocs is to have all of them in the same order. In other word, we wish to solve the following problem:

> *"Given two equivalent codes, how can we obtain the permutation between their supports?"*

4.2.1 Signature of a position

Let C and C' be two equivalent linear codes. Let J and J' denote respectively the supports of C and C'. We will assume that the automorphism group of C (and thus of C') is reduced to the identity element. Within this assumption, there is a unique bijection $\sigma : J' \to J$ that establish the one to one correspondence between the positions of C and C'. Our purpose is to compute σ.

For any subset I of J, we will denote by $C(I)$ the code obtained by deleting in C the positions of I.

Definition 7 *The* signature *of an element i of J, denoted S_i, is defined to be the weight distribution of the code $C(\{i\})$.*

We define an equivalence $\mathcal{R}$ over the set J:

$$i \,\mathcal{R}\, j \Leftrightarrow S_i = S_j$$

This equivalence induces a partition of J:

$$J = \mathcal{I}_1 \cup \ldots \cup \mathcal{I}_l$$

We assume that the equivalence classes of this relation are ordered according to any total ordering of the weight distribution.

If we apply the same process to C', we will obtain a partition $\mathcal{I}'_1 \cup \ldots \cup \mathcal{I}'_l$ such that for any s, $1 \leq s \leq l$, $\mathcal{I}_s$ and $\mathcal{I}'_s$ have same size and signature. Furthermore we have $\sigma(\mathcal{I}'_s) = \mathcal{I}_s$. Thus if all the equivalence classes have cardinality 1, we are able to produce σ.

If not, we can repeat the process for all s with the codes $C(\mathcal{I}_s)$ and $C'(\mathcal{I}'_s)$ which are equivalent too. By merging all the partitions, we can hope to obtain σ.

For the codes we have considered, this was sufficient, and all the B-blocs can be reordered in about 20 seconds with a program in C running on a workstation DEC 3000.

Remark 1

- This algorithm is susceptible to works only with codes that have an automorphism group reduced to the element identity. It will not work neither if the number of equivalence classes of $\mathcal{R}$ is small, say two or three, which happens for codes of small length (less than 10).
- Another drawback of this method is that it requires the computation of weight distributions. This practically limits the dimension (or codimension) of C to 30.

4.3 Finding the outer code

4.3.1 A constructive lemma

Let α be a primitive element of $GF(q^{k_B})$. For any β in $GF(q^{k_B})$ we will denote A_β the matrix of the homomorphism $x \mapsto \beta x$ in the basis $(1, \alpha, \ldots, \alpha^{k_B - 1})$.

Lemma 1 *Let $C = B(n_B, k_B, d_B)\Box_\theta E(n_E, k_E, d_E)$ be a concatenated code. Let $r_E = n_E - k_E$. Let's consider a generating matrix of C*

$$G_C = \begin{pmatrix} G_B & \ldots & 0 & G_{1,1} & \ldots & G_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \ldots & G_B & G_{k_E,1} & \ldots & G_{k_E,r_E} \end{pmatrix}$$

where G_B and each non-zero bloc $G_{i,j}$ is a generating matrix of B. For each pair (i,j), we put $G_{i,j} = H_{i,j} G_B$.

1. *There exists a non-singular matrix U such that for all pair (i,j), we have*

$$H_{i,j} = UA_{\beta_{i,j}}U^{-1}, \quad \beta_{i,j} \in GF(q^{k_B})$$

and

$$G_E = \begin{pmatrix} 1 & \dots & 0 & \beta_{1,1} & \dots & \beta_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \beta_{k_E,k_E} & \dots & \beta_{k_E,r_E} \end{pmatrix}$$

is a generating matrix of E.

2. *For any U' such that*

$$H_{i_0,j_0} = U'A_{\beta'_{i_0,j_0}}U'^{-1}$$

for some pair (i_0,j_0) and β_{i_0,j_0} is not in a subfield of $GF(q^{k_B})$, we have

   (a) $\beta'_{i_0,j_0} = \beta_{i_0,j_0}^{q^s}$ *for some s, $0 < s < k_B - 1$,*

   (b) $H_{i,j} = U'A_{\beta'_{i,j}}U'^{-1}$, *with $\beta'_{i,j} = \beta_{i,j}^{q^s}$ for all pairs (i,j).*

The matrix

$$G_{E'} = \begin{pmatrix} 1 & \dots & 0 & \beta'_{1,1} & \dots & \beta'_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \beta'_{k_E,k_E} & \dots & \beta'_{k_E,r_E} \end{pmatrix}$$

obtained in the second part of the lemma is the generating matrix of a code $E'(n_E, k_E, d_E)$ which is F_q-equivalent to E.

The element β'_{i_0,j_0} is an arbitrary root in $GF(q^{k_B})$ of the minimal polynomial $p(X)$ of H_{i_0,j_0}. Thus $\beta'_{i_0,j_0} = \beta_{i_0,j_0}^{q^s}$ is a conjugate of β_{i_0,j_0}. We then compute a U' such that $H_{i_0,j_0} = U'A_{i_0,j_0}U' - 1$ (U' is not unique), the lemma assures that for all pair (i,j), we have $H_{i,j} = U'A_{\beta'_{i,j}}U'^{-1}$ and $\beta'_{i,j} = \beta_{i,j}^{q^s}$. This enables us to construct $G_{E'}$.

4.3.2 Construction of the outer code

slightlyAt that point, we assume that all the B-blocs have been recovered, and we order the position by putting one B-bloc after another. This leads after a Gaussian elimination to a generating matrix of the form:

$$G_C = \begin{pmatrix} G_B & 0 & \dots & 0 & G_{1,1} & \dots & G_{1,r_E} \\ 0 & G_B & \ddots & \vdots & G_{2,1} & \dots & G_{2,r_E} \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & G_B & G_{k_E,k_E} & \dots & G_{k_E,r_E} \end{pmatrix}$$

where G_B and each non zero $G_{i,j}$ is a generating matrix of the same code B equivalent to the original outer code. Note that if the outer code is MDS, then all the $G_{i,j}$ are non zero. We assume here that the k_E first B-blocs are such that they allow the bloc diagonal form of G_C.

Proposition 6 *Each bloc $G_{i,j}$ in G_C will be equal to*

$$G_{i,j} = UA_{\beta_{i,j}}U^{-1}G_B$$

where U is a $k_B \times k_B$ non singular matrix over $GF(q)$ and

$$G_E = \begin{pmatrix} 1 & 0 & \dots & 0 & \beta_{1,1} & \dots & \beta_{1,r_E} \\ 0 & 1 & \ddots & \vdots & \beta_{2,1} & \dots & \beta_{2,r_E} \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & \beta_{k_E,k_E} & \dots & \beta_{k_E,r_E} \end{pmatrix}$$

is the generating matrix of a code $E(n_E, k_E, d_E)$ over $GF(q^{k_B})$ F_q-equivalent to the original outer code and such that $C = B\Box E$.

Proof: The code B is equivalent to the original inner code B_o. Let Π_B denote the matrix of the permutation between the supports B and B_o.

Let Π_E denote the permutation between the B-blocs in C and their original position in C_o. We denote E' the outer code obtained by permuting the coordinates of E_o according to Π_E.

We have $C = B\Box_{\theta'}E'$, where $\theta'(\alpha^i) = \theta_o(\alpha^i)\Pi_B$, for all i, $0 \leq i \leq k_B - 2$. By use of lemma 1 we can construct an $E(n_E, k_E, d_E)$ code over $GF(q^{k_B})$ such that $C = B\Box E$, and E is F_q-equivalent to E' and thus by transitivity to E_o. □

4.4 Decoding the newly constructed code

Decoding the permuted version C_o' of $C_o = B_o\Box E_o$ is thus equivalent to decoding a concatenated code $B\Box E$ where B is equivalent to B_o and E is F_q-equivalent to E_o.

In any case, this proves that the original problem, can be divided in two problems, one for the inner code and one for the outer. Thus the concatenated structure is not hidden, though the structure of each of the component code is.

Furthermore we considered a random binary inner code a GRS outer code. Thus decoding B instead of B_o makes not difference at all. Since E is F_q-equivalent to E_o, E is also a GRS code, and from [SS92] we know that this is enough to decode E as easily as E_o.

References

[CC94] A. Canteaut and H. Chabanne. A further improvement of the work factor in an attempt at breaking McEliece cryptosystem. In P. Charpin, editor, *Livre des résumé - EUROCODE 94*, pages 163–167, Abbaye de la Bussière sur Ouche, France, October 1994. INRIA.

[Cha94] F. Chabaud. On the security of some cryptosystems based on error-correcting codes. In A. de Santis, editor, *pre-proceedings of EUROCRYPT'94*, pages 127–135, May 1994.

[LB88] P.J. Lee and E.F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In C.G. Günther, editor, *Advances in Cryptology - EUROCRYPT'88*, number 330 in LNCS, pages 275–280. Springer-Verlag, 1988.

[LDW94] Y.X. Li, R.H. Deng, and X.M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, January 1994.

[Leo88] J.S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, September 1988.

[LN83] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1983.

[McE78] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.*, Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, Jan.-Feb. 1978.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[Nie86] H. Niederreiter. Knapsack-type crytosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

[SS92] V.M. Sidelnikov and S.O. Shestakov. On insecurity of cryptosystem based on generalized Reed-Solomon codes. *manuscript*, 1992.

[Ste89] J. Stern. A method for finding codewords of small weight. In G. Cohen and J. Wolfmann, editors, *Coding theory and applications*, number 388 in LNCS, pages 106–113. Springer-Verlag, 1989.

[vT90] J. van Tilburg. On the mceliece cryptosystem. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO'88*, number 403 in LNCS, pages 119–131. Springer-Verlag, 1990.

[ZL84] V. Zinoviev and S. Litsyn. Shortening of codes. *Problemy Peredachi Informatsii*, 20(1):3–11, January 1984.

A Proof of Lemma 1

Let α be a primitive element of $GF(q^{k_B})$. For any β in $GF(q^{k_B})$ we will denote A_β the matrix of the homomorphism $x \mapsto \beta x$ in the basis $(1, \alpha, \ldots, \alpha^{k_B-1})$.

For any square matrix A, the centralizer of A, denote by $Z(A)$, is the set of the matrices that commutes with A. That is the set of all matrices C such that $CA = AC$.

Lemma 2 *Let β be an element of $GF(q^{k_B})$ which is not in a subfield. Let U and U' be two $k_B \times k_B$ non-singular matrices. The two following assertions are equivalent*

1. $UA_\beta U^{-1} = U'A_\beta U'^{-1}$
2. *for all γ in $GF(q^{k_B})$,* $UA_\gamma U^{-1} = U'A_\gamma U'^{-1}$

Proof: If the second assertion is true, then, in particular, the first one is true.

Reciprocally, since β is not in a subfield of $GF(q^{k_B})$, the set $(1, \beta, \ldots, \beta^{k_B-1})$ is a basis of $GF(q^{k_B})$, then any γ in $GF(q^{k_B})$ can be written

$$\gamma = \sum_{i=0}^{k_B-1} \gamma_i \beta^i, \quad \gamma_i \in GF(q)$$

and we also have

$$A_\gamma = \sum_{i=0}^{k_B-1} \gamma_i A_\beta^i, \quad \gamma_i \in GF(q)$$

This proves that $Z(A_\beta) \subset Z(A_\gamma)$ for all γ in $GF(q^{k_B})$.

Furthermore we have $UA_\gamma U^{-1} = U'A_\gamma U'^{-1}$ if and only if $U^{-1}U'$ is in $Z(A_\gamma)$. From the first assertion, we know that $U^{-1}U' \in Z(A_\beta)$, and thus $U^{-1}U' \in Z(A_\gamma)$ for all γ, and the second assertion is true. $\square$

Lemma 1 *Let $C = B(n_B, k_B, d_B)\Box_\theta E(n_E, k_E, d_E)$ be a concatenated code. Let $r_E = n_E - k_E$. Let's consider a generating matrix of C*

$$G_C = \begin{pmatrix} G_B & \ldots & 0 & G_{1,1} & \ldots & G_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \ldots & G_B & G_{k_E,1} & \ldots & G_{k_E,r_E} \end{pmatrix}$$

where G_B and each non-zero bloc $G_{i,j}$ is a generating matrix of B. For each pair (i,j), we put $G_{i,j} = H_{i,j}G_B$.

1. *There exists a non-singular matrix U such that for all pair (i,j), we have*

$$H_{i,j} = UA_{\beta_{i,j}}U^{-1}, \quad \beta_{i,j} \in GF(q^{k_B}) \tag{2}$$

and

$$G_E = \begin{pmatrix} 1 & \ldots & 0 & \beta_{1,1} & \ldots & \beta_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \ldots & 1 & \beta_{k_E,k_E} & \ldots & \beta_{k_E,r_E} \end{pmatrix}$$

is a generating matrix of E.

2. For any U' such that

$$H_{i_0,j_0} = U' A_{\beta'_{i_0,j_0}} U'^{-1}$$

for some pair (i_0, j_0) and β_{i_0,j_0} is not in a subfield of $GF(q^{k_B})$, we have

(a) $\beta'_{i_0,j_0} = \beta^{q^s}_{i_0,j_0}$ for some s, $0 < s < k_B - 1$,

(b) $H_{i,j} = U' A_{\beta'_{i,j}} U'^{-1}$, with $\beta'_{i,j} = \beta^{q^s}_{i,j}$ for all pairs (i, j).

Proof: Let

$$G_E = \begin{pmatrix} 1 & \dots & 0 & \beta_{1,1} & \dots & \beta_{1,r_E} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \beta_{k_E,k_E} & \dots & \beta_{k_E,r_E} \end{pmatrix}$$

be a generating matrix of E. Let α be a primitive element of $GF(q^{k_B})$, and let $G_{\theta,\alpha}$ be the generating matrix of B defined by equation (1). Since G_B is also a generating matrix of B, there exist a non-singular matrix U such that $G_B = UG_{\theta,\alpha}$.

We also know that the matrix

$$G = \begin{pmatrix} G_{\theta,\alpha} & \dots & 0 & A_{\beta_{1,1}} G_{\theta,\alpha} & \dots & A_{\beta_{1,r_E}} G_{\theta,\alpha} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \dots & G_{\theta,\alpha} & A_{\beta_{k_E,1}} G_{\theta,\alpha} & \dots & A_{\beta_{k_E,r_E}} G_{\theta,\alpha} \end{pmatrix}$$

is a generating matrix of G. If we multiply each bloc-line of G by U, the resulting matrix is

$$\begin{pmatrix} G_B & \dots & 0 & UA_{\beta_{1,1}} U^{-1} G_B & \dots & UA_{\beta_{1,r_E}} U^{-1} G_B \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & \dots & G_{\theta,\alpha} & UA_{\beta_{k_E,1}} U^{-1} G_B & \dots & UA_{\beta_{k_E,r_E}} U^{-1} G_B \end{pmatrix}$$

and is still a generating matrix of $\mathcal{C}$. Furthermore this matrix coincide with $G_{\mathcal{C}}$ on a set of information position, it is thus equal to $G_{\mathcal{C}}$. We then have for all pair (i, j)

$$UA_{\beta_{i,j}} U^{-1} G_B = G_{i,j} = H_{i,j} G_B$$

Since G_B is a matrix of rank k_B, we have

$$H_{i,j} = UA_{\beta_{i,j}} U^{-1}$$

for all pair (i, j). This proves the first part of the lemma.

Let U' and β'_{i_0,j_0} be such that

$$H_{i_0,j_0} = U' A_{\beta'_{i_0,j_0}} U'^{-1} = UA_{\beta_{i_0,j_0}} U^{-1}$$

The element β'_{i_0,j_0} has the same minimal polynomial as H_{i_0,j_0}, and thus the same as β_{i_0,j_0}. This imply that $\beta'_{i_0,j_0} = \beta^{q^s}_{i_0,j_0}$ is a conjugate of β_{i_0,j_0}.

For any pair (i, j), we have $H_{i,j} = UA_{\beta_{i,j}} U^{-1}$. If F^s_q is the s-th power of the Frobenius and is identified with its matrix as a vector-space-homomorphism over $GF(q)$, we have

$$H_{i,j} = UA_{\beta_{i,j}} U^{-1} = UF_q^{-s} A_{\beta^{q^s}_{i,j}} F^s_q U^{-1}$$

In particular, if β_{i_0,j_0} is not in a subfield of $GF(q^{k_B})$, we have

$$H_{i_0,j_0} = UF_q^{-s} A_{\beta_{i_0,j_0}^{q^s}} F_q^s U^{-1} = U' A_{\beta_{i_0,j_0}^{q^s}} U^{-1},$$

and from Lemma 2, we have $U'^{-1} H_{i,j} U' = A_{\beta_{i,j}^{q^s}}$ for all pair (i,j). □

There is a small difficulty if no matrix $H_{i,j}$ is such that its minimal polynomial has degree k_B. If this happens, we will consider the field $GF(q^m)$ generated by all the $\beta_{i,j}$ (this is possible from the knowledge of the $H_{i,j}$).

- If $m = k_B$, then a linear combination of some $H_{i,j}$ will provide a matrix $H = UA_\beta U$ that will have a minimal polynomial of degree k_B.
- If not, if we replace $GF(q^{k_B})$ by $GF(q^m)$ in Lemma 2, it is still true, and it provides a similarly useful result.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes - IRISA, Campus universitaire de Beaulieu 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)
Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399

* R R . 2 4 6 8 *