THE RAO-NAM SCHEME IS INSECURE AGAINST A CHOSEN-PLAINTEXT ATTACK

René Struik
Eindhoven University of Technology
Eindhoven, the Netherlands

Johan van Tilburg
PTT / Dr. Neher Laboratories
St. Paulustraat 4
2264 XZ Leidschendam, the Netherlands

ABSTRACT

The Rao-Nam scheme is discussed and generalized to F_q. It is shown that the scheme is insecure against a chosen-plaintext attack for practical code lengths. Based on observations an improved scheme is given, which is not vulnerable to the chosen-plaintext attacks as described.

1. INTRODUCTION

In 1978 McEliece [1] proposed a public-key cryptosystem based on the theory of linear algebraic codes. His scheme was a natural consequence of a paper by Berlekamp, McEliece and van Tilborg [2] in which it was proved that the general decoding problem for linear codes is NP-complete. The McEliece scheme is based on a class of Goppa-codes, which is an extension of the well-known class of BCH-codes. Since there exists fast decoding algorithms for these codes, data rates of 1 Mbits/s [1][3][4] can be obtained. Adams and Meijer [3] and Jorissen [4] computed the optimal values for the parameters of the McEliece system. The optimal values improves the cryptanalytic complexity and information rate of the system. Moreover Adams and Meijer showed that

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 445-457, 1988.

the existence of more than one trapdoor in the McEliece scheme is unlikely.

It is a well-known fact that public-key cryptosystems can be used as private-key cryptosystems. Therefore throughout the years Jordan [5], Rao and Nam [6] proposed to modify the McEliece scheme in order to use it in a classical way. Rao and Nam's aim was to increase the information rate and speed by keeping the generator matrix secret and by using simple error-correcting codes. They modified the McEliece scheme and used the error-correcting properties of the code to determine pre-defined error patterns. The error patterns used in the Rao-Nam scheme have an average Hamming weight of half the code length.

Rao and Nam [6] claimed that the determination of the encipher matrix in the modified scheme from a chosen-plaintext attack has a work factor of at least $T = \Omega(n^{2k})$. Based on the given attack it is suggested in their conclusion that the Rao-Nam scheme for private-key cryptosystems requires only simple codes such as Hamming codes with minimum distance 3 and 4 and is even computationally secure for small $k \approx 50$.

However as will be shown in this paper their exists better attacks from which one can conclude that the Rao-Nam scheme is insecure against a chosen-plaintext attack for practical code lengths. Based on observations we will give an improved scheme which is not vulnerable to the chosen-plaintext attacks as described.

In section 2 we will describe the Rao-Nam scheme for the general case $\mathbb{F}_q$. In section 3 the basic facts about the attack are given. In section 4 Hin's attack on the Rao-Nam scheme with adjacent errors is discussed. The generalized attack by Struik is described in section 5. A ciphertext-only attack, which makes use of an estimated encipher matrix obtained from a chosen-plaintext attack, is given in section 6. In section 7 an improved scheme is given. Finally in section 8 the results obtained are discussed and conclusions are drawn.

2. The Generalized Scheme

The Rao-Nam scheme as described in [6] is a binary scheme. Therefore

we shall first generalize this scheme to $\mathbb{F}_q$. For q = 2 the original Rao-Nam scheme is obtained.

Let G denote a (kxn) generator matrix for an [n,k,d]-code $\mathcal{C}$ over $\mathbb{F}_q$ with minimum distance d, dimension k and parity check matrix H. The encryption matrix E is combinatorically equivalent to the generator matrix G and is constructed as follows:

$$E = SGP,$$

where

S is a (kxk) non-singular matrix over $\mathbb{F}_q$ and
P is an (nxn) permutation matrix over $\mathbb{F}_q$.

A message $\underline{m} \in (\mathbb{F}_q)^k$ is <u>encrypted</u> into the ciphertext $\underline{c} \in (\mathbb{F}_q)^n$ as follows:

$$\underline{c} = \underline{m}E + \underline{z}P = (\underline{m}SG + \underline{z})P,$$

where

$\underline{z} \in (\mathbb{F}_q)^n$ is an error vector with an average Hamming weight $W_H(\underline{z}) = \frac{q-1}{q} n$.

The matrices S, P and G form the secret key.

The choice of the error vector $\underline{z}$ is to prevent a chosen-plaintext attack by majority voting for each position of a row of the encipher matrix E in the McEliece scheme. If the error vectors have an average Hamming weight $\frac{q-1}{q} n$ the probability of estimating the correct matrix E is on average less than q^{-nk}. Obviously unique decoding is not possible without modifying the original scheme. Therefore Rao and Nam proposed two methods to realize unique decoding for which we have generalized the second method only.

<u>Method 1</u>. Use q=2 and i adjacent errors (ATE) for $\underline{z}$.
An ATE is a vector of length n with i adjacent errors, i.e. an ATE consists of n-i 0's and i consecutive 1's.

<u>Method 2</u>. Use a pre-defined set of error vectors (syndrome-error table).
A pre-defined set of error vectors, consisting of one vector from each coset of the standard array decoding table can be used for $\underline{z}$. Each

coset has a distinct syndrome. Therefore, we can select any set of vectors consisting of one from each of the q^{n-k} cosets. This set of pre-defined errors is part of the secret key.

It is important to note that due to the restricted set of error patterns the system is not optimally secure against a chosen-plaintext attack based on majority voting. For example, if majority voting is used in the Rao-Nam scheme using method 1, then one can use a majority vote with context. Since the number of different error patterns used is just a fraction of the possible number of error patterns we are always better off.

Decryption is straightforward. An enciphered message $\underline{m}$ is decrypted by the following steps.

1) Calculate $\underline{c}' = \underline{c}P^T = \underline{m}SG + \underline{z}$.
2) Determine $\underline{c}^* = \underline{c}'H^T$ and obtain the error pattern $\underline{z} \in (\mathbb{F}_q)^n$. As result $\underline{c}'' = \underline{c}' - \underline{z} = \underline{m}SG$ is obtained.
3) Calculate $\underline{m} = \underline{c}''(SG)^{-R}$, in which $(SG)^{-R}$ is a right inverse of the matrix (SG). The result is the plaintext $\underline{m}$.

In the attacks to be described we make use of an equivalent decoding algorithm. The decryption matrix D is HP, since $ED^T = (SGP)(HP)^T = 0$. Note that S is used before the coding process, therefore S has no impact on the error correction. The decoding algorithm is now as follows.

1) Determine $\underline{c}^* = \underline{c}D^T$ and obtain the permuted error pattern $\underline{z}P \in \mathbb{F}_q^n$. As result $\underline{c}' = \underline{c} - \underline{z}P = \underline{m}E$ is obtained.
2) Calculate $\underline{m} = \underline{c}'E^{-R}$, in which E^{-R} is a right inverse of the matrix E. The result is the plaintext $\underline{m}$.

3. Weaknesses of Rao-Nam Scheme

The three attacks which will be described make use of the same weaknesses of the Rao-Nam scheme.

The first weakness is the low number of different syndromes, which is for the proposed Hamming code using ATE's at most n, and for the

syndrome-error table q^{n-k}. If the number of different error patterns is N, then one has to encipher on average $N(\frac{1}{N} + \frac{1}{N-1} + .. + 1) = \theta(N \log N)$ times to obtain all error patterns. Observe that the minimum distance of the [n,k,d]-code $\mathcal{C}$ plays at this moment no role.

Let $R = \frac{k}{n}$ be the information rate. The number of cosets is $N = q^{n-k} = q^{n(1-R)}$. Consequently in the Rao-Nam scheme there exists a trade-off between information rate and security. For a high information rate R and a large number of cosets N the code length n will be impractical.

The second weakness is due to the leakage of information about the permutation matrix P if ATE's are used. An ATE and its one position shifted ATE (which is an ATE also) differ on exactly two places. After the permutation they still differ on two places. Since we know the structure of the original ATE we can estimate the permutation matrix.

The third weakness is the possibility of estimating the rows of the encipher matrix E=SGP by means of constructing unit vectors $\underline{u}_i$ (= 0..010..0, i.e. the all zero vector with a 1 added on the i-th position). Therefore as suggested in [9] the linear transformation S should be replaced by a non-linear transformation.

4. Attack by Hin

In Hin [7] an attack on the Rao-Nam scheme using ATE's is described. As ATE's have a fixed and known structure, his approach makes use of the leakage of information about the permutation matrix P. In addition it is necessary that the permutation matrix P must transform an ATE into a non-ATE. We will describe his attack for non-cyclic ATE's only.

Let $\mathcal{A}$ denote the ordered set {11...10..0, 011...10..0, ..} of all possible ATE's. The unkown set of permuted ATE's is indicated by $\mathcal{P}$. Let $\mathcal{P}^{(0)}$ be the set of all possible encipherments of the message $\underline{m}=\underline{0}$. An ATE and its one position shifted ATE (which is an ATE also) differ on exactly two places. If the ATE's are distinct and not succesive, then they differ on more than two places. This also holds after permutation and consequently the set $\mathcal{P}^{(0)}$ can be ordered in the same way as $\mathcal{P}$. Hence from the ordered set $\mathcal{P}^{(0)}$ the permutation matrix P is constructed.

Next an ordered set $\mathcal{P}^{(i)}$ is obtained by enciphering the unit vector $\underline{u}_i$ at least N times until all possible error patterns have been appeared, with $1 \le i \le k$. The elements in $\mathcal{P}^{(i)}$ are arranged in such a way that the same permutation matrix P is obtained. The x-th elements of each of the sets in $\mathcal{P}^{(0)}$, $\mathcal{P}^{(1)}$, $\mathcal{P}^{(2)}$, ..., $\mathcal{P}^{(k)}$ possess the same error patterns since the sets are ordened in a unique way. Next, with $1 \le i \le k$, take the first element in $\mathcal{P}^{(0)}$ and subtract it from the first element in $\mathcal{P}^{(i)}$, i.e.: $(\underline{u}_i E + \underline{z}P) - \underline{z}P = \underline{u}_i E = \underline{e}_i$ which is the i-th row $\underline{e}_i$ of E. In this way the encipher matrix $E = (\underline{e}_1^T, \underline{e}_2^T, \ldots, \underline{e}_k^T)^T$ is constructed. Finally the decipher matrix D, the matrix E^{-1} are calculated and the syndrome-error table is constructed. In this way an (equivalent) decoding algorithm is obtained and the scheme is broken.

SUMMARY

1. Encipher the message $\underline{m} = \underline{0}$ as long as all the N error patterns have not yet appeared.

2. Order the (permuted) error patterns and obtain $\mathcal{P}^{(0)}$. Construct the permutation matrix P.

3. Repeat step 1 for $\underline{m} = \underline{u}_i$ with $1 \le i \le k$ and obtain the set $\mathcal{P}^{(i)}$. The elements in $\mathcal{P}^{(i)}$ are ordened according permutation matrix P. Take the first element in $\mathcal{P}^{(0)}$ and subtract it from the first element in $\mathcal{P}^{(i)}$ to obtain the i-th row $\underline{e}_i$ of the encipher matrix.

4. Construct the encipher matrix $E = (\underline{e}_1^T, \underline{e}_2^T, \ldots, \underline{e}_k^T)^T$, calculate the decipher matrix D, the matrix E^{-1} and construct the syndrome-error table.

Costs

$k\Theta(N \log N)$ encipherments on average,

$kO(n \log N)$ operations for ordening,

where

$N = n-i+1$ for a non-cyclic code.

Remark. The assumption that messages of the kind $\underline{m}=\underline{0}$ and $\underline{m}=\underline{u}_i$ are not allowed to obtain an increased security [6, p. 40] is merely outward

seeming. In the above attack it is not necessary to use the messages $\underline{m}=\underline{0}$ and $\underline{m}=\underline{u}_i$. One can take an arbitrary message $\underline{m}$. The unit vector $\underline{u}_i$ can be constructed by choosing a message $\underline{m}_i$ such that $\underline{m}_i = \underline{m} + \underline{u}_i$. The additional costs involved are k times a k-dimensional vector addition over $\mathbb{F}_q$ which can be neglected.

5. Attack by Struik

Hin's attack is based on the imposed structure on the error patterns. Struik's [8] generalized version of Hin's attack does not assume any structure about the error patterns and is also applicable to the generalized Rao-Nam scheme as outlined in section 2.

An error pattern $\underline{z}$ is randomly selected from the set $\mathcal{Z} = \{\underline{z}^{(j)}\}_{j=1}^{N}$ which contains N different error patterns. After encipherment the error pattern is permuted; the set $\mathcal{Z}^P$ is defined as $\{\underline{z}^{(j)}P\}_{j=1}^{N}$. From the set $\mathcal{Z}$ we can define a set $\mathcal{Z}_\Delta$ of error pattern differences $\underline{z}^{(i,j)} = \underline{z}^{(i)}-\underline{z}^{(j)}$ and in the same way the set $\mathcal{Z}_\Delta^P = \{\underline{z}^{(i,j)}P\}_{i,j=1}^{N}$ can be obtained. A guessed error pattern is denoted by $\hat{\underline{z}}$ and the difference $\tilde{\underline{z}}^{(i,j)} = \hat{\underline{z}}^{(i)}-\underline{z}^{(j)}$. Because there are N distinct error patterns, there are N distinct permuted error patterns. For an arbitrary message $\underline{m}$ there are N distinct encipherments $\underline{c}^{(j)} = \underline{m}E+\underline{z}^{(j)}P$ possible, which will be denoted by the set $\mathcal{C} = \{\underline{c}^{(j)}\}_{j=1}^{N}$. For the construction of a unit vector $\underline{u}_i$ we choose a message $\underline{m}_i = \underline{m}+\underline{u}_i$. The set of encipherments of message $\underline{m}_i$ is denoted by $\mathcal{C}_i$.

The attack can now be described as follows. Encipher an arbitrary message $\underline{m}$ until all the N different cryptograms $\underline{c}^{(1)}$, $\underline{c}^{(2)}$, .. ,$\underline{c}^{(N)}$ are obtained. Construct with the N different encipherments a directed labeled graph $\Gamma=(\mathcal{C},\mathcal{Z}_\Delta^P)$. The vertices are $\underline{c}^{(1)}$, $\underline{c}^{(2)}$, .. ,$\underline{c}^{(N)}$ and the edge from vertex $\underline{c}^{(i)}$ to vertex $\underline{c}^{(j)}$ has label $\underline{z}^{(i,j)}P$. The relation follows from $\underline{c}^{(i)}-\underline{c}^{(j)} = (\underline{m}E+\underline{z}^{(i)}P) - (\underline{m}E+\underline{z}^{(j)}P) = \underline{z}^{(i,j)}P$. In the binary case (q=2) it follows that $\underline{z}^{(i,j)}P = \underline{z}^{(j,i)}P$. Subsequently construct the automorphism group Aut(Γ), i.e. all the permutations on $\mathcal{C}$ which leave all the labels $\underline{z}^{(i,j)}P$ invariant.

We choose a message $\underline{m}_i = \underline{m}+\underline{u}_i$. Again we encipher until all the N different cryptograms $\underline{c}_i^{(j)}$ are obtained. Subsequently the graph $\Gamma_i=(\mathcal{C}_i,\mathcal{Z}_\Delta^P)$ is constructed. Select at random one automorphism ϕ from

the automorphism group Aut(Γ). The mapping induced by ϕ from Γ_i on Γ gives N cryptograms $\underline{c}_i^{(1)}$, $\underline{c}_i^{(2)}$, .. ,$\underline{c}_i^{(N)}$ synchronized in a certain way with $\underline{c}^{(1)}$, $\underline{c}^{(2)}$, .. ,$\underline{c}^{(N)}$. Calculate $\underline{c}_i^{(1)}-\underline{c}^{(1)} = (\underline{m}_i E+\hat{\underline{z}}_i^{(1)}P) - (\underline{m}E+\underline{z}^{(1)}P) = \underline{e}_i+\tilde{\underline{z}}^{(1,1)}P$. With probability $|\mathrm{Aut}(\Gamma)|^{-1}$ the row $\underline{e}_i$ will be correctly estimated as there exists an automorphism ϕ for which $\tilde{\underline{z}}^{(1,1)}= 0$. The correctness of a row can not be verified independently from the other rows. On average we can expect that the cryptanalyst has to construct $|\mathrm{Aut}(\Gamma)|^k$ encipher matrices $\hat{E}$ before the correct one is obtained, calculate the decipher matrix $\hat{D}$, the matrix $\hat{E}^{-1}$ and construct the syndrome-error table via $\underline{c}^{(j)}-\underline{m}E = \underline{z}^{(j)}P$. In this way an (equivalent) decoding algorithm is obtained.

SUMMARY

1. Encipher a message $\underline{m}$ until all the N different cryptograms $\underline{c}^{(1)}$, $\underline{c}^{(2)}$, ... , $\underline{c}^{(N)}$ are obtained.

2. Construct the directed complete graph $\Gamma=(\mathcal{X},\mathcal{Z}_\Delta^P)$ and the automorphism group Aut(Γ).

3. For $1\le i\le k$, choose a message $\underline{m}_i$ such that $\underline{m}_i = \underline{m}+\underline{u}_i$. Repeat step 1 for $\underline{m} = \underline{m}_i$ and construct $\Gamma_i=(\mathcal{X}_i,\mathcal{Z}_\Delta^P)$.

4. For $1\le i\le k$ select at random a automorphism ϕ from the automorphism group Aut(Γ). Map Γ_i on Γ according ϕ and calculate $\hat{\underline{e}}_i = \underline{c}_i-\underline{c}$.

5. Construct the encipher matrix $\hat{E} = (\hat{\underline{e}}_1^T, \hat{\underline{e}}_2^T, \ldots, \hat{\underline{e}}_k^T)^T$, calculate the decipher matrix $\hat{D}$, the matrix $\hat{E}^{-1}$ construct the syndrome-error table and verify the solution. If the solution is not correct, repeat the steps 4 and 5.

Costs

Preliminary work

$k\Theta(N \log N)$ encipherments on average,

$O((k+|\mathrm{Aut}(\Gamma)|)\ n\ \lceil\log q\rceil))$ bits of memory,

$O(nN\lceil\log q\rceil)$ bits of temporal memory space,

$O(knN^2 \log N)$ operations.

Calculation of encipher matrix

$O(kn\ \lceil\mathrm{Log}\ q\rceil)$ bits,

$O(kn|\mathrm{Aut}(\Gamma)|^k)$ operations.

Validation costs are neglected.

From the costs it appears that the number of possible automorphisms $|Aut(\Gamma)|$ is a measure of the computational strength of the (generalized) Rao-Nam scheme. In the worst case situation where $|Aut(\Gamma)| = N$, the costs of this attack is the same as those of the attack described by Rao and Nam. There exist

$$q^{k(n-k+i)}$$

combination of error patterns each chosen from a distinct coset such that the upper bound

$$|Aut(\Gamma)| = q^{n-k}$$

is reached. From this result it follows that the probability of selecting the right combination randomly that leads to the maximum number of automorphisms is approximately q^{-kN}. For this reason the function that determines this set of error patterns must be highly structured and is also part of the secret key.

In the Rao-Nam scheme using ATE's the number of automorphisms ϕ from the group $Aut(\Gamma)$ if $N>2$ is given by:

$|Aut(\Gamma)| = 2$, iff the ATE's are cyclic and have Hamming weight $\frac{n}{2}$,
$|Aut(\Gamma)| = 1$, else.

If $|Aut(\Gamma)| = 1$ then the automorphism is: $\phi(\underline{z}) = \underline{z}$ and,
if $|Aut(\Gamma)| = 2$ then we have also $\phi(\underline{z}) = \underline{z} + \underline{1}$.

We can conclude that the Rao-Nam scheme is insecure against a chosen-plaintext attack in many cases. Only if the value $|Aut(\Gamma)|$ is large this attack wil not work. In the next section an attack is given which is efficient when the number of automorphisms $|Aut(\Gamma)|$ is large.

Remark. In theory this attack can be applied to the McEliece scheme too. In this case the order of the automorphism group is one and contains the identity automorphism only. However the N possible error patterns is astronomically large. Therefore this attack fails due to

the large amount of preliminary work involved.

6. Extended Attack by Struik

In the following attack an estimated generator matrix is used to perform a ciphertext-only attack. The attack can be divided into two parts. The first part is based on the chosen-plaintext attack to obtain an estimated generator matrix $\hat{E}$. The second part is a ciphertext-only attack from which the unkown message $\hat{\underline{m}}$ is guessed. With this attack we do not obtain the correct generator matrix, however we do obtain the unknown message.

FIRST PART - Chosen-Plaintext Attack

The first part of the attack is the same as described in section 5. We stop after the first estimate of the generator matrix E. The guessed generator matrix is denoted by $\hat{E}$, where $\hat{\underline{e}}_i = \underline{e}_i + \tilde{\underline{z}}^{(i,i)}P$. Since each automorphism is a translation, the rows must be equal to $\hat{\underline{e}}_i = \underline{e}_i + \underline{v}_i$ for a certain unkown $\underline{v}_i \in V$, which is a sub-space of $(\mathbb{F}_q)^n$.

SECOND PART - Ciphertext-Only Attack

Let $\hat{\underline{c}}$ denote the encipherment $\hat{\underline{m}}E + \hat{\underline{z}}P$ of the unknown message $\hat{\underline{m}}$.

$$\tilde{\underline{c}} = \hat{\underline{c}} - \underline{c} = (\hat{\underline{m}} - \underline{m})E + (\hat{\underline{z}} - \underline{z})P = \tilde{\underline{m}}E + \tilde{\underline{z}}P \ ,$$

where $\tilde{\underline{m}} = \hat{\underline{m}} - \underline{m}$ and $\tilde{\underline{z}} = \hat{\underline{z}} - \underline{z}$.

Since $\hat{\underline{e}}_i = \underline{e}_i + \underline{v}_i$ it follows that

$$\tilde{\underline{c}} = \tilde{\underline{m}}\hat{E} + \tilde{\underline{z}}P - \sum_{i=1}^{k} \tilde{m}_i \underline{v}_i$$

If the cryptanalyst knows $\tilde{\underline{z}}P - \sum \tilde{m}_i \underline{v}_i$ then he can solve $\tilde{\underline{m}}$ from the above equation. The cryptanalyst picks at random a vector $\underline{w} \in V$ and calculates:

$$\underline{a} = \tilde{\underline{c}} - \underline{w} = \tilde{\underline{m}}\hat{E} + (\tilde{\underline{z}}P - \sum_{i=1}^{k} \tilde{m}_i \underline{v}_i - \underline{w})$$

Suppose $\tilde{\underline{z}}P - \sum \tilde{m}_i \underline{v}_i - \underline{w} = \underline{0}$, then $\tilde{\underline{m}}$ can be solved from $\tilde{\underline{m}}\hat{E} = \underline{a}$. Repeat until a sensible plaintext $\underline{m} + \tilde{\underline{m}}$ is obtained. Note that $\forall\, \underline{z}\ \exists\, \underline{w}\ [\ \underline{z}\tilde{P} - \sum \tilde{m}_i \underline{v}_i - \underline{w} = \underline{0}\ ]$. The expected number of attempts is at most N.

Costs

$O(k^2nN)$ operations,

$O(kn\lceil \log q \rceil)$ bits memory space.

A refinement of this attack will be given in a paper to apear.

7. Modified Scheme

Almost all the proposed attacks on the Rao-Nam scheme are based on estimating the rows of the encipher matrix E=SGP by constructing unit vectors or by solving a system of linear equations. Therefore to avoid such attacks the S-matrix should be replaced by a non-linear function. In general S can be replaced by a secret invertible function f which transforms a message $\underline{m} \in (\mathbb{F}_q)^k$ into a word $\underline{m}' \in (\mathbb{F}_q)^k$. As special case this function may depend on the error vector $\underline{z}$ used too, as we can determine $\underline{z}$ from the cryptogram in a unique way. In this case the following enciphering scheme is obtained:

$$\underline{c} = f(\underline{m},\underline{z}).E + \underline{z},$$

where E = GP and f chosen such that

$$\forall \underline{z}\ \forall \underline{m} \quad f^{-1}(f(\underline{m},\underline{z}),\underline{z}) = \underline{m}.$$

The decoding algorithm is almost the same as described before if f^{-1} is used instead of S^{-1} and is as follows.

1) Determine $\underline{c}^* = \underline{c}D^T$ and obtain the error pattern $\underline{z} \in (\mathbb{F}_q)^n$.
   As result $\underline{c}' = \underline{c} - \underline{z} = f(\underline{m},\underline{z})E$ is obtained.
3) Calculate $\underline{m}' = \underline{c}'E^{-R} = f(\underline{m},\underline{z})$, in which E^{-R} is a right inverse of the matrix E.
4) The final result is the plaintext $\underline{m} = f^{-1}(\underline{m}',\underline{z})$.

This scheme is not vulnerable to chosen-plaintext attacks as described. This can be seen easily from the fact that the secret function f can be chosen such that it does not allow construction of unit vectors to estimate a row in the E=GP matrix. Hence this scheme

provides a higher security level.

8. Conclusion

The Rao-Nam scheme is generalized to $\mathbb{F}_q$. For this general scheme 3 chosen-plaintext attacks are discussed.

It is shown that the Rao-Nam scheme using ATE's is completely insecure against a chosen-plaintext attack. If a pre-defined set of error vectors is used then it appears that the number of possible automorphisms $|\mathrm{Aut}(\Gamma)|$ is a measure for the computational strength of the (generalized) Rao-Nam scheme. If the value $|\mathrm{Aut}(\Gamma)|$ is small then the attack described in section 5 is efficient, otherwise the attack described in section 6 will break the scheme.

We have given an improved scheme in which the linear transformation S in the encipher matrix E=SGP is replaced by a non-linear funtion. This improved scheme is not vulnerable to the chosen-plaintext attacks as described.

ACKNOWLEDGEMENT

The authors thank J.P. Boly, P.J.M. Hin, H. Meijer and H.C.A. van Tilborg for helpful conversations.

REFERENCES

[1] **McEliece, R.J.,** "A Public-Key Cryptosystem Based On Algebraic Coding Theory", DSN Progress Report 42-44, Pasadena, JPL, pp.114-116, 1978.

[2] **Berlekamp, E.R., McEliece, R.J, and van Tilborg, H.C.A,** "On the Inherent Intractability of Certain Coding Problems", IEEE Trans. Inform. Theory. IT-24, pp.384-386, 1978.

[3] **Adams, C, Meijer, H,** "Security relating comments regarding the McEliece Public-Key Cryptosystem, presented at crypto'87.

[4] **Jorrissen, F,** "A Security Evaluation of the Public-Key Cipher System Proposed by R.J. McEliece, used as Combined Scheme", Katholieke Universiteit Leuven, Lab. ESAT, 1986.

[5] **Jordan, J.P.,** "A Variant of a Public Key Cryptosystem based on Goppa Codes", Sigact news, vol 15, no: 1, pp. 61-66, 1983.

[6] **Rao, T.R.N., Nam, K.H.,** "Private-Key Algebraic-Coded Cryptosystem", in: Advances in Cryptology - CRYPTO'86, A.M. Odlyzko (Ed.), Lecture Notes in Computer Science #263, Springer, pp 35-48, 1987.

[7] **Hin, P.J.M.,**"Channel-Error-Correcting Privacy Cryptosystems", Thesis, Delft Univ. of Techn., 1986 (in Dutch).

[8] **Struik, R.,** "Algebraic Coded Cryptosystems", Private Communication, July 1987.

[9] **van Tilburg, J.,** "Private-Key Cryptosystems based on Algebraic Coding Theory", Pub 87 DNL/53, PTT/DNL, the Netherlands, 1987.