Discrete Math. Appl., Vol. 2, No. 4, pp. 439–444 (1992)

On insecurity of cryptosystems based on generalized Reed–Solomon codes*

V. M. SIDELNIKOV and S. O. SHESTAKOV

Abstract — In papers [1, 2] methods of building public-key cryptosystems based on code-theoretic constructions have been suggested. Their background is an $(s+1) \times N$ non-secret matrix $\mathfrak{B}$ of the form $\mathfrak{B} = H\mathfrak{A}$ with its elements from a finite field $\mathbf{F}_q$. Here $\mathfrak{A}$ is some unknown matrix which is a check matrix of a q-ary generalized Reed–Solomon code. In this paper we suggest a method of finding the unknown matrices H, $\mathfrak{A}$ which determines the matrix $\mathfrak{B}$ in $O(s^4 + sN)$ arithmetical operations in $\mathbf{F}_q$. By this the insecurity of such public-key cryptosystems is demonstrated.

1. DESCRIPTION OF A PUBLIC-KEY CRYPTOSYSTEM

Let us apply the public-key cryptosystem suggested in [2] to the generalized Reed–Solomon code (GRS-code). Let $\mathbf{F}_q$ be a finite field with q elements and $\mathbf{F} = \mathbf{F}_q \cup \{\infty\}$, where ∞ has natural properties ($1/\infty = 0$, etc.). The symbol $\mathfrak{A}$ denotes a matrix with the elements from $\mathbf{F}_q$ of the form

$$\mathfrak{A}(\alpha_1, \ldots, \alpha_N; z_1, \ldots, z_N) = \begin{Vmatrix} z_1\alpha_1^0 & z_2\alpha_2^0 & \ldots & z_N\alpha_N^0 \\ z_1\alpha_1^1 & z_2\alpha_2^1 & \ldots & z_N\alpha_N^1 \\ & & \ddots & \\ z_1\alpha_1^s & z_2\alpha_2^s & \ldots & z_N\alpha_N^s \end{Vmatrix}, \tag{1}$$

where $\alpha_i \in \mathbf{F}$, $z_i \in \mathbf{F}_q \backslash \{0\}$, $\alpha_i \neq \alpha_j$ for $i \neq j$, and if $\alpha_j = \infty$ the corresponding column is defined as the vector of the form $z_j(0, \ldots, 0, 1)^T$. The matrix $\mathfrak{A}$ is a check matrix of the q-ary code $\mathbf{K} = \mathbf{K}(\mathfrak{A})$ of length N, which is a GRS-code shortened to $N < q + 1$ (see [3]). Let $\mathcal{E}$ be a collection consisting of all matrices of the form $\mathfrak{B} = H\mathfrak{A}$, where $\mathfrak{A}$ is a matrix of type (1) and H is a non-degenerate $(s+1) \times (s+1)$ matrix with the elements from $\mathbf{F}_q$. It follows from the definitions that the typical matrix $\mathfrak{B}$ of $\mathcal{E}$ has the form

$$\mathfrak{B} = \begin{Vmatrix} z_1 f_1(\alpha_1) & z_2 f_1(\alpha_2) & \ldots & z_N f_1(\alpha_N) \\ z_1 f_2(\alpha_1) & z_2 f_2(\alpha_2) & \ldots & z_N f_2(\alpha_N) \\ & & \ddots & \\ z_1 f_{s+1}(\alpha_1) & z_2 f_{s+1}(\alpha_2) & \ldots & z_N f_{s+1}(\alpha_N) \end{Vmatrix}, \tag{2}$$

where $f_j(x)$, $j = 1, \ldots, s+1$, are polynomials linearly independent over $\mathbf{F}_q$ of degree not higher than s. They are determined by the matrix H in a natural way ($f_j(\infty)$ is the coefficient of x^s).

We will briefly describe the public-key cryptosystem based on the ideas of [2]. In this system a user $\mathbf{X}$ randomly and equiprobably chooses a matrix $\mathfrak{B}$ of type (2) in $\mathcal{E}$.

*UDC 519.72. Originally published in *Diskretnaya Matematika* (1992) 4, No. 3 (in Russian). Translated by the authors.

The matrix $\mathfrak{B}$ is known, and the matrices H and $\mathfrak{A}$ are secret. A message B of a user **Y** addressed to the user **X** is transferred through a public channel and has the form of a column $B = \mathfrak{B}\bar{a}$, where the vector $\bar{a} \in (\mathbf{F}_q)^N$ has not more than $t = [s/2]$ non-zero coordinates and contains a transmitted confidential information. If the matrices H and $\mathfrak{A}$ are known and the message B is received, the user **X** can reconstruct the vector $\bar{a}$ 'fast enough' by means of one of the known algorithms of decoding a GRS-code. If the matrices H and $\mathfrak{A}$ are unknown, the reconstruction of the vector $\bar{a}$ becomes a 'difficult problem' which cannot be solved in satisfactorily short time.

The public-key cryptosystem suggested in [1] is different from the one described above, but if the code **K** is over $\mathbf{F}_q$, then the problem of its decryption is also equivalent to finding H and $\mathfrak{A}$ from $\mathfrak{B}$. If **K** is over some subfield of $\mathbf{F}_q$, then the reconstruction of H and $\mathfrak{A}$ from $\mathfrak{B}$ grows more difficult, but the authors are sure that this can be done by means of methods close to the suggested ones.

The principal aim of this work is to construct an algorithm for finding the matrices H and $\mathfrak{A}$ in $O(s^4 + sN)$ arithmetical operations in $\mathbf{F}_q$ when the matrix $\mathfrak{B}$ is known. Note that by using fast algorithms of linear algebra, the exponent 4 can be reduced to a smaller value.

2. ALGORITHM OF FINDING A SOLUTION OF THE EQUATION $\mathfrak{B} = H\mathfrak{A}$

The task is to find a non-degenerate matrix H, $x_1, \ldots, x_N \in \mathbf{F}$ and $z_1, \ldots, z_N \in \mathbf{F}_q \backslash \{0\}$ such that

$$\mathfrak{B} = H\mathfrak{A}(x_1, \ldots, x_N; z_1, \ldots, z_N) \tag{3}$$

provided the matrix $\mathfrak{B}$ is known. We solve the problem in two steps: first we find the numbers $x_1, \ldots, x_N$, and then the numbers $z_1, \ldots, z_N$ and the matrix H.

First some notes should be made. Let $(H, x_1, \ldots, x_N, z_1, \ldots, z_N)$ be some solution of equation (3), $a \neq 0$ and b be some elements of $\mathbf{F}_q$ and $h_{ij} \in \mathbf{F}_q$, $0 \leq i, j \leq s$, be such that

$$(ax + b)^i = \sum_{j=0}^{s} h_{ij} x^j.$$

Put $H_1 = \|h_{ij}\|$; $d_i = 1$ if $x_i \neq \infty$ and $d_i = a^{-s}$ if $x_i = \infty$. Direct evaluations show that

$$H_1\mathfrak{A}(x_1, \ldots, x_N; d_1 z_1, \ldots, d_N z_N) = \mathfrak{A}(ax_1 + b, \ldots, ax_N + b; z_1, \ldots, z_N);$$

besides, the matrix H_1 is triangular and therefore non-degenerate. It is easy to see from the equality

$$HH_1^{-1}\mathfrak{A}(ax_1 + b, \ldots, ax_N + b; d_1^{-1} z_1, \ldots, d_N^{-1} z_N) = H\mathfrak{A}(x_1, \ldots, x_N; z_1, \ldots, z_N) = \mathfrak{B}$$

that $(HH_1^{-1}, ax_1 + b, \ldots, ax_N + b; d_1^{-1} z_1, \ldots, d_N^{-1} z_N)$ is also a solution of equation (3). Similarly, if

$$H_2 = \begin{pmatrix} 0 & 0 & \ldots & 1 \\ & & \ddots & \\ 0 & 1 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{pmatrix}$$

and $d_i = x_i^{-s}$ for $x_i \neq 0, \infty$ and $d_i = 1$ otherwise, then

$$H_2\mathfrak{A}(x_1, \ldots, x_N; d_1 z_1, \ldots, d_N z_N) = \mathfrak{A}(1/x_1, \ldots, 1/x_N; z_1, \ldots, z_N).$$

Thus $(HH_2^{-1}, x_1^{-1}, \dots, x_N^{-1}; d_1^{-1}z_1, \dots, d_N^{-1}z_N)$ is also a solution of (3). It is known that any birational transformation

$$\phi: \quad x \mapsto \frac{ax + b}{cx + d}, \qquad ad - bc \neq 0,$$

over $\mathbf{F}_q$ is a composition of the transformations $x \mapsto ax + b$ and $x \mapsto 1/x$. It follows that for any birational transformation ϕ there exist $z_1', \dots, z_N'$ and a matrix H_ϕ such that $(HH_\phi^{-1}, \phi(x_1), \dots, \phi(x_N); z_1', \dots, z_N')$ is a solution of equation (3) if $(H, x_1, \dots, x_N; z_1, \dots, z_N)$ is a solution of (3).

For any three different numbers $x_1, x_2, x_3 \in \mathbf{F}_q\{\infty\}$ it is possible to find a birational transformation ϕ such that $\phi(x_1) = 1$, $\phi(x_2) = 0$ and $\phi(x_3) = \infty$. It follows that there exist $x_4, \dots, x_N \in \mathbf{F}_q\{0, 1\}$, $z_1', \dots, z_N' \in \mathbf{F}_q\{0\}$ and a matrix H such that $(H; 1, 0, \infty, x_4, \dots, x_N; z_1', \dots, z_N')$ is a solution of equation (3). Since it is sufficient to find any solution, we will search for it in this form, that is with $x_1 = 1$, $x_2 = 0$ and $x_3 = \infty$.

Rewrite equation (3) as

$$\mathfrak{B} = H\mathfrak{A}_1(x_1, \dots, x_N)D = \|b_{ij}\|,$$

where $H = \|h_{ij}\|$, $\mathfrak{A}_1(x_1, \dots, x_N) = \mathfrak{A}(x_1, \dots, x_N; 1, \dots, 1)$, $D = \operatorname{diag}(z_1, \dots, z_N)$, so that

$$H\mathfrak{A}(x_1, \dots, x_N) = \|a_{ij}\|, \qquad a_{ij} = f_i(x_j), \qquad f_i(x) = \sum_{j=0}^{s} h_{ij}x^j,$$

and consequently, $b_{ij} = z_j f_i(x_j)$ (as before, $f(\infty)$ is equal to the coefficient of x^s of $f \in \mathbf{F}_q[x]$ with $\deg f \leq s$). In other words, the matrix D contains the unknowns z_j.

Find $c_{1i} \in \mathbf{F}_q$, $0 \leq i \leq s$, not all of which are equal to zero and such that the equalities $\sum_{i=0}^{s} c_{1i}b_{ij} = 0$ hold for any $j = 1, s + 2, \dots, 2s$. It suffices to solve the system of s homogeneous linear equations with $s + 1$ unknowns. Clearly, this system is solvable. Let

$$F_1(x) = \sum_{i=0}^{s} c_{1i}f_i(x), \qquad \beta_{1j} = \sum_{i=0}^{s} c_{1i}b_{ij}, \qquad 1 \leq j \leq N.$$

Then

$$\beta_{1j} = \sum_{i=0}^{s} c_{1i}z_j f_i(x_j) = z_j F_1(x_j),$$

and as all z_j are non-zero, it follows from the construction of $F_1(x)$ that $x_1, x_{s+2}, \dots, x_{2s}$ are the roots of F_1. All $x_1, x_{s+2}, \dots, x_{2s}$ are finite because $x_3 = \infty$; besides, $\deg F_1 \leq s$ because $\deg f_i \leq s$. Therefore

$$F_1(x) = a_1(x - x_1)(x - x_{s+2}) \dots (x - x_{2s}),$$

in particular, $F_1(x_j) \neq 0$ and $\beta_{1j} = z_j F_1(x_j) \neq 0$ for $j \notin \{1, s + 2, \dots, 2s\}$ and $\beta_{13} = z_3 F_1(x_3) = z_3 F_1(\infty) = a_1 z_3$.

Now we choose $c_{2i} \in \mathbf{F}_q$, $0 \leq i \leq s$, not all of which are equal to zero and such that the equalities $\sum_{i=0}^{s} c_{2i}b_{ij} = 0$ hold for any $j = 2, s + 2, \dots, 2s$, and put

$$F_2(x) = \sum_{i=0}^{s} c_{2i}f_i(x), \qquad \beta_{2j} = \sum_{i=0}^{s} c_{1i}b_{ij}.$$

We have

$$\beta_{2j} = z_j F_2(x_j), \qquad F_2(x) = a_2(x - x_2)(x - x_{s+2})\dots(x - x_{2s}).$$

Since $\beta_{2j} \neq 0$ for $j = 3,\dots,s+1,2s+1,\dots,N$, one can calculate $b_j = \beta_{1j}/\beta_{2j}$ for these j. The equalities

$$\begin{aligned} b_j &= z_j F_1(x_j)/(z_j F_2(x_j)) \\ &= a_1(x_j - x_1)(x_j - x_{s+2})\dots(x_j - x_{2s})/a_2(x_j - x_2)(x_j - x_{s+2})\dots(x_j - x_{2s}) \\ &= a_1(x_j - x_1)/a_2(x_j - x_2), \\ b_3 &= \beta_{13}/\beta_{23} = a_1 z_3/a_2 z_3 = a_1/a_2 \end{aligned}$$

imply that

$$b_j = b_3(x_j - x_1)/(x_j - x_2), \qquad x_j = (b_3 x_1 - b_j x_2)/(b_3 - b_j).$$

Finally, it follows from $x_1 = 1$ and $x_2 = 0$ that $x_j = b_3/(b_3 - b_j)$ for $j = 4,\dots,s+1,2s+1,\dots,N$.

Now we choose c_{3i} and c_{4i} from $\mathbf{F}_q$, $0 \le i \le s$, such that for $j = 1,3,\dots,s+1$ and $j = 2,3,\dots,s+1$ the equalities $\sum_{i=0}^{s} c_{3i} b_{ij} = 0$ and $\sum_{i=0}^{s} c_{4i} b_{ij} = 0$ hold respectively. Let

$$F_3(x) = \sum_{i=0}^{s} c_{3i} f_i(x), \qquad F_4(x) = \sum_{i=0}^{s} c_{4i} f_i(x),$$

$$\beta_{3j} = \sum_{i=0}^{s} c_{3i} b_{ij}, \qquad \beta_{4j} = \sum_{i=0}^{s} c_{4i} b_{ij}, \qquad 1 \le j \le N.$$

It follows from the equality $F_3(x_3) = F_3(\infty) = 0$ that the coefficient of x^s in F_3 is zero, i.e., $\deg F_3 \le s - 1$. Using the equalities $F_3(x_1) = F_3(x_4) = \dots = F_3(x_{s+1}) = 0$, we find that

$$F_3(x) = a_3(x - x_1)(x - x_4)\dots(x - x_{s+1}).$$

Analogously,

$$F_4(x) = a_4(x - x_2)(x - x_4)\dots(x - x_{s+1}).$$

Therefore, for $j \ge s + 2$

$$\begin{aligned} \beta_{3j}/\beta_{4j} &= z_j F_3(x_j)/z_j F_4(x_j) \\ &= a_3(x_j - x_1)(x_j - x_4)\dots(x_j - x_{s+1})/a_4(x_j - x_2)(x_j - x_4)\dots(x_j - x_{s+1}) \\ &= a_3(x_j - x_1)/a_4(x_j - x_2). \end{aligned}$$

In particular, for $j = N$ these equalities yield

$$\beta_{3N}/\beta_{4N} = a_3(x_N - x_1)/a_4(x_N - x_2) = a_3 b_N/a_4 b_3,$$

hence

$$a_3/a_4 = b_3 b_{3N}/b_N b_{4N}, \qquad \beta_{3j}/\beta_{4j} = b_3 b_{3N}/b_N b_{4N}(x_j - x_1)/(x_j - x_2).$$

Let $b_j = \beta_{4N}/\beta_{3N}\beta_{3j}/\beta_{4j} b_N$ for $j = s+2,\dots,2s$. Then $b_j = b_3(x_j - x_1)/(x_j - x_2)$ and $x_j = b_3/(b_3 - b_j)$ for these j, as well as for the other values of j.

Let us briefly describe the algorithm for finding the numbers x_j once more.

(1) Find $c_{1i}, c_{2i} \in \mathbf{F}_q$, $0 \le i \le s$, such that for $j = 1, s+2, \dots, 2s$ and $j = 2, s+2, \dots, 2s$ the equalities $\sum_{i=0}^{s} c_{1i} b_{ij} = 0$ and $\sum_{i=0}^{s} c_{2i} b_{ij} = 0$ hold respectively ($O(s^3)$ operations in $\mathbf{F}_q$).

(2) Calculate $\beta_{1j} = \sum_{i=0}^{s} c_{1i} b_{ij}$ and $\beta_{2j} = \sum_{i=0}^{s} c_{2i} b_{ij}$ for $j = 3, \dots, s+1, 2s+1, \dots, N$, and find $b_j = \beta_{1j}/\beta_{2j}$ ($O(sN)$ operations).

(3) Find $c_{3i}, c_{4i} \in \mathbf{F}_q$, $0 \le i \le s$, such that for $j = 1, 3, \dots, s+1$ and $j = 2, 3, \dots, s+1$ the equalities $\sum_{i=0}^{s} c_{3i} b_{ij} = 0$ and $\sum_{i=0}^{s} c_{4i} b_{ij} = 0$ hold respectively ($O(s^3)$ operations).

(4) Calculate $\beta_{3j} = \sum_{i=0}^{s} c_{3i} b_{ij}$ and $\beta_{4j} = \sum_{i=0}^{s} c_{4i} b_{ij}$ for $j = s+2, \dots, 2s, N$, and find $b_j = (b_N \beta_{4N}/\beta_{3N})\beta_{3j}/\beta_{4j}$ for $j = s+2, \dots, 2s$ where b_N is found at step (2) ($O(s^2)$ operations).

(5) Put $x_1 = 1$, $x_2 = 0$, $x_3 = \infty$ and $x_j = b_3/(b_3 - b_j)$ for $4 \le j \le N$ ($O(N)$ operations).

(6) Choose some $a \in \mathbf{F}_q$ differing from all x_j, $1 \le j \le N$, and replace each x_j with $1/(a - x_j)$ ($O(N)$ operations). The new set of x_j is also a part of some solution of (3), however containing no $x_j = \infty$.

Now we will find the numbers z_j and the matrix H. If each element of the matrix D is multiplied by some fixed $a \in \mathbf{F}_q$ and each element of H is multiplied by a^{-1}, then the product $H\mathfrak{A}_1 D$ will be the same. We therefore can presume that $z_1 = 1$.

Find $c_1, \dots, c_{s+2} \in \mathbf{F}_q$, not all of which are equal to zero and such that the equalities

$$\sum_{j=1}^{s+2} c_j b_{ij} = 0, \qquad 0 \le i \le s, \tag{4}$$

hold. It is sufficient to solve the system of $s+1$ homogeneous linear equations with $s+2$ unknowns. All of the numbers c_j are non-zero because otherwise the matrix $\mathfrak{B}$ would contain $s+1$ linearly dependent columns. Since $b_{ij} = z_j f_i(x_j)$, equalities (4) can be written as

$$\sum_{j=1}^{s+2} c_j z_j f_i(x_j) = 0, \qquad 0 \le i \le s,$$

or in the matrix form, $AC\bar{z} = 0$, where $A = \|a_{ij}\|$, $a_{ij} = f_i(x_j)$, $0 \le i \le s$, $1 \le j \le s+2$, $C = \operatorname{diag}(c_1, \dots, c_{s+2})$, $\bar{z} = (z_1, \dots, z_{s+2})^T$. But $A = H\mathfrak{A}_1(x_1, \dots, x_{s+2})$, and therefore $H\mathfrak{A}_1(x_1, \dots, x_{s+2})C\bar{z} = 0$. Multiplying the last equality by H^{-1} we get $\mathfrak{A}(x_1, \dots, x_{s+2})C\bar{z} = 0$, consequently the relations

$$\sum_{j=1}^{s+2} c_j z_j x_j^i = 0, \qquad 0 \le i \le s,$$

are satisfied. Since the numbers c_j and x_j are already known and $z_1 = 1$, we have a linear system of $s+1$ equations with $s+1$ unknowns $z_2, \dots, z_{s+2}$. This system has a unique solution because its determinant is equal to $c_2 \dots c_{s+2} \det \mathfrak{A}_1(x_2, \dots, x_{s+2}) \neq 0$. Solving this system yields the sought numbers $z_1, \dots, z_{s+2}$.

If $H = \|h_{ik}\|$, $0 \le i, k \le s$, then

$$b_{ij} = z_j \sum_{k=0}^{s} h_{ik} x_j^k.$$

Fix some i, $0 \le i \le s$, and vary j from 1 to $s+1$. We get the following system of linear equations for $h_{i0}, \dots, h_{is}$:

$$\sum_{k=0}^{s} h_{ik} x_j^k = z_j^{-1} b_{ij}, \qquad 1 \le j \le s+1.$$

The determinant of this system is the Wandermond determinant, so the numbers $h_{i0}, \ldots, h_{is}$ can be determined uniquely. Solving this system for every i, $0 \leq i \leq s$, we find the matrix H.

The multiplication of equality (3) by H^{-1} gives $\mathfrak{A}(x_1, \ldots, x_N; z_1, \ldots, z_N) = H^{-1}\mathfrak{B}$. Since the first row of the matrix $\mathfrak{A}(x_1, \ldots, x_N; z_1, \ldots, z_N)$ is $(z_1, \ldots, z_N)$, the last numbers z_j are determined by the equalities

$$z_j = \sum_{i=0}^{s} h'_{0i} b_{ij}, \qquad s + 3 \leq j \leq N,$$

where $H^{-1} = \|h'_{ij}\|$. It is not necessary to calculate the whole matrix H^{-1} for finding h'_{0i}; it is sufficient to solve the system

$$\sum_{i=0}^{s} h'_{0i} h_{i0} = 1, \qquad \sum_{i=0}^{s} h'_{0i} h_{ij} = 0, \qquad 1 \leq j \leq s.$$

We however need the matrix H^{-1} for decoding, so it is convenient to calculate it in this stage.

Let us in short describe the algorithm for finding the matrices H and $D = \mathrm{diag}(z_1, \ldots, z_N)$ once more.

(1) Find $c_1, \ldots, c_{s+2} \in \mathbf{F}_q$ such that $\sum_{j=1}^{s+2} c_j b_{ij} = 0$, $0 \leq i \leq s$ ($O(s^3)$ operations).

(2) Put $z_1 = 1$ and find such $z_2, \ldots, z_{s+2} \in \mathbf{F}_q$ that $\sum_{j=1}^{s+2} c_j z_j x_j^i = 0$, $0 \leq i \leq s$ ($O(s^3)$ operations).

(3) For each i, $0 \leq i \leq s$, find $h_{i0}, \ldots, h_{is} \in \mathbf{F}_q$ such that $\sum_{k=0}^{s} h_{ik} x_j^k = z_j^{-1} b_{ij}$, $1 \leq j \leq s + 1$, and put $H = \|h_{ij}\|$ ($O(s^4)$ operations).

(4) Find the matrix $H^{-1} = \|h'_{ij}\|$ and calculate $z_j = \sum_{i=0}^{s} h'_{0i} b_{ij}$, $s + 3 \leq j \leq N$ ($O(s^4 + sN)$ operations).

Solving equation (3) by means of the suggested algorithm requires $O(s^4 + sN)$ operations in $\mathbf{F}_q$.

REFERENCES

1. R. J. McEliece, A public-key cryptosystem based on algebraic coding theory. In: *DSN Progress Report 42–44, Jet Propulsion Lab.* Pasadena, 1978, pp. 114–116 .
2. H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control and Inform. Theory*, (1986), **15**, 19–34.
3. F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.