Tatra Mt. Math. Publ. **25** (2002), 67–80

TATRA MOUNTAINS
Mathematical Publications

A CRYPTOSYSTEM BASED ON DOUBLE EXPONENTIATION

Mieczysław Kula

ABSTRACT. The paper contains a description and cryptanalysis of a cryptographic algorithm based on double exponentiation in matrix groups.

1. Preliminaries

In 1978 S. Pohlig and M. Hellman [6] proposed a private-key cryptosystem based on well-known difficulty in calculating discrete logarithm in a finite field. In this note we want to discuss a two round Pohlig-Hellman cryptosystem which proceeds in two consecutive exponentiations performed in two groups. This investigation is motivated by a cipher algorithm called Secure Encryption Device (SED) developed by Emile Musyck (protected by 3 patents BE no. 8900467, EUR no. 90870060 and USA no. 5010573) (cf. [7], [8]). The basic part of this algorithm called DDLM (Double Discrete Logarithm Multiplier) uses matrix representations of finite fields. At the beginning we describe a general outline of DDLM and then we show an equivalent algorithm which allows us to perform all computations in a finite field. It is easy to see that DDLM is at least as secure as the Pohlig-Hellman system. However, we shall point out that the encryption function used in the construction may contain a potential insecurity.

Let $q = p^l$ where p is a prime and l is a positive integer. Let $\mathbb{F}_q$ denote the field containing q elements and let $n > 1$ be a fixed integer. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n. If (f) denotes the ideal of $\mathbb{F}_q[x]$ generated by f, then the factor ring $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f)$ is a field which contains q^n elements. The elements of $\mathbb{F}_{q^n}$ are represented by polynomials over $\mathbb{F}_q$ of degree less than n where addition and multiplication are defined as addition and multiplication of polynomials mod f. Multiplication can be optimized by choosing f to be a trinomial. The element α of $\mathbb{F}_q[x]/(f)$ represented by the monomial x is referred to as the *standard root* of the polynomial f in $\mathbb{F}_{q^n}$. If

2000 Mathematics Subject Classification: 11T71, 94A60.
Keywords: cryptography, finite field discrete logarithm.

α is the standard root of f, then every element of $\mathbb{F}_{q^n}$ can be written uniquely as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Thus we write $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. The elements $1, \alpha, \ldots, \alpha^{n-1}$ will be called the standard basis of $\mathbb{F}_q(\alpha)$. All non-zero elements of the field $\mathbb{F}_{q^n}$ form a multiplicative cyclic group of order $N = q^n - 1$ denoted by $\mathbb{F}^*_{q^n}$. Every generator of $\mathbb{F}^*_{q^n}$ is called a *primitive element* of the field. The minimal polynomial of a primitive element is called *primitive* as well. More information on finite fields can be found in [5].

2. Matrix representations of a field

Denote by $M_n(\mathbb{F}_q)$ the algebra of all $n \times n$ matrices over $\mathbb{F}_q$ and let Θ_n be the all-zero $n \times n$-matrix. A matrix representation of $\mathbb{F}_{q^n}$ is a subalgebra $\mathcal{F}$ of $M_n(\mathbb{F}_q)$ which is a field isomorphic to $\mathbb{F}_{q^n}$. For a convenience of the reader we record a well-known construction of matrix representations of fields (cf. [1]). For every matrix $A \in M_n(\mathbb{F}_q)$ and every polynomial $h = c_0 + c_1x + \cdots + c_kx^k \in \mathbb{F}_q[x]$ we define the matrix $h(A) = c_0I + c_1A + \cdots + c_kA^k$. Recall that the subalgebra $S_n(\mathbb{F}_q) = \{aI \in M_n(\mathbb{F}_q) \colon a \in \mathbb{F}_q\}$ of scalar matrices is a field isomorphic to $\mathbb{F}_q$. For every matrix $A \in M_n(\mathbb{F}_q)$ we denote by $\mathbb{F}_q(A)$ the subalgebra of $M_n(\mathbb{F}_q)$ generated by $\{A\} \cup S_n(\mathbb{F}_q)$.

Lemma 1. *Let A be a fixed matrix in $M_n(\mathbb{F}_q)$ such that the characteristic polynomial f of A is irreducible in $\mathbb{F}_q[x]$.*

(a) *If α is the standard root of f in $\mathbb{F}_{q^n}$, then there is a unique field isomorphism $\Omega \colon \mathbb{F}_q(\alpha) \longrightarrow \mathbb{F}_q(A)$ such that $\Omega(a) = aI$ for all $a \in \mathbb{F}_q$ and $\Omega(\alpha) = A$.*

(b) *The matrices $I, A, \ldots, A^{n-1}$ form a basis of $\mathbb{F}_q(A)$ regarded as a vector space. In particular, every matrix X in $\mathbb{F}_q(A)$ can be uniquely presented as $X = a_0I + a_1A + a_2A^2 + \cdots + a_{n-1}A^{n-1}$ for suitable $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_q$.*

P r o o f. (a) Define a mapping $\overline{\Omega} \colon \mathbb{F}_q[x] \to M_n(\mathbb{F}_q)$ by $\overline{\Omega}(h) = h(A)$ for every $h \in \mathbb{F}_q[x]$. It is easy to check that $\overline{\Omega}$ is a ring homomorphism with $\operatorname{im} \overline{\Omega} = \mathbb{F}_q(A)$. The ideal of $\mathbb{F}_q[x]$ generated by the characteristic polynomial f of A is contained in the kernel of the homomorphism $\overline{\Omega}$, as $f(A) = \Theta_n$ by the Cayley-Hamilton theorem. If f is irreducible, then it generates a maximal ideal in $\mathbb{F}_q[x]$ so $(f) = \ker \overline{\Omega}$. By the isomorphism theorem (cf. [2, Chapter 10]) the homomorphism $\overline{\Omega}$ determines a unique field isomorphism $\Omega \colon \mathbb{F}_q(\alpha) \to \mathbb{F}_q(A)$ such that $\Omega(a) = aI$ for all $a \in \mathbb{F}_q$ and $\Omega(\alpha) = A$. Thus $\mathbb{F}_q(A)$ is a field isomorphic to $\mathbb{F}_q(\alpha) = \mathbb{F}_q[x]/(f)$.

(b) Every element X in the subalgebra $\mathbb{F}_q(A)$ has the form $X = c_0 I + c_1 A + \cdots + c_k A^k = h(A)$ where k is a non-negative integer and $h = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{F}_q[x]$. There are polynomials $g_1, g_2 \in \mathbb{F}_q[x]$ such that $h = g_1 f + g_2$ and $\deg g_2 < \deg f = n$. Thus $h(A) = g_1(A) f(A) + g_2(A) = g_2(A) = a_0 I + a_1 A + \cdots + a_{n-1} A^{n-1}$ for suitable coefficients $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_q$. This shows that $I, A, \ldots, A^{n-1}$ generates the vector space $\mathbb{F}_q(A)$ over $\mathbb{F}_q$. Suppose there are coefficients $b_0, b_1, \ldots, b_{n-1} \in \mathbb{F}_q$ such that $b_0 I + b_1 A + \cdots + b_{n-1} A^{n-1} = \Theta_n$. Then for $g = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$ we have $g(A) = \Theta_n$, i.e., $g \in \ker \overline{\Omega} = (f)$. Hence $n - 1 \geq \deg g \geq \deg f = n$, a contradiction. This shows that the matrices $I, A, \ldots, A^{n-1}$ are linearly independent, so they form a basis of $\mathbb{F}_q(A)$. □

Lemma 2. *If a matrix A is a primitive element of a matrix representation $\mathcal{F}$ of $\mathbb{F}_{q^n}$ in $M_n(\mathbb{F}_q)$, then the characteristic polynomial of A is irreducible and $\mathcal{F} = \mathbb{F}_q(A)$.*

P r o o f. Since A is a primitive element of the field $\mathcal{F}$, it generates the multiplicative group $\mathcal{F}^*$ of non-zero elements which is cyclic and its order is equal to $N = q^n - 1$. Hence $\mathcal{F}^* \cup \{\Theta_n\} = \{I, A, \ldots, A^{N-1}\} \cup \{\Theta_n\} = \mathbb{F}_q(A)$. Let $\overline{\Omega}\colon \mathbb{F}_q[x] \to \mathbb{F}_q(A) = \mathcal{F}$ be the epimorphism defined by $\overline{\Omega}(h) = h(A)$ for all $h \in \mathbb{F}_q[x]$. The kernel of $\overline{\Omega}$ is a maximal ideal in $\mathbb{F}_q[x]$ and $f \in \ker \overline{\Omega}$ by the Cayley–Hamilton theorem. Obviously, $\ker \overline{\Omega}$ is generated by an irreducible polynomial g. Suppose $\deg g < \deg f = n$. Using similar arguments as in the proof of Lemma 1 one can show that the cardinality of $\mathbb{F}_q[x]/\ker \overline{\Omega}$ is equal to $q^{\deg g} < q^n$. This contradicts the fact that $\mathbb{F}_q[x]/\ker \overline{\Omega}$ is isomorphic to $\mathcal{F}$ which is a field of order q^n. Thus g and f are equal up to a constant factor, which completes the proof. □

The above Lemma shows that every matrix $A \in M_n(\mathbb{F}_q)$ with the irreducible characteristic polynomial generates a representation of the field $\mathbb{F}_{q^n}$ in the matrix algebra $M_n(\mathbb{F}_q)$. We have also seen that $\mathbb{F}_q(A)$ can be regarded as a vector space over $\mathbb{F}_q$. More information on matrix representations of finite fields can be found in [1].

Let $V_n = \mathbb{F}_q^n$ denote the n-dimensional vector space of column vectors over $\mathbb{F}_q$ and let θ_n be the all-zero vector of length n. For a given non-zero vector $\vec{r} \in V_n$ we define a mapping $\Phi\colon M_n(\mathbb{F}_q) \to V_n$ by $\Phi(X) = X\vec{r}$ for every matrix $X \in M_n(\mathbb{F}_q)$. One can easily prove that Φ is an $\mathbb{F}_q$-linear mapping. Let $\mathcal{F}$ be a subalgebra of $M_n(\mathbb{F}_q)$ isomorphic to $\mathbb{F}_{q^n}$ and let $\varphi = \Phi \restriction \mathcal{F}$. The next Lemma shows that φ establishes an explicit linear isomorphism of the vector spaces V_n and $\mathcal{F}$.

Lemma 3. *For every non-zero vector $\vec{r} \in V_n$ and every matrix representation $\mathcal{F}$ of $\mathbb{F}_{q^n}$, the mapping φ is a linear isomorphism of vector spaces $\mathcal{F}$ and V_n.*

P r o o f . It is enough to show that φ is an invertible mapping. Since $\mathcal{F}$ is a field, every nonzero matrix in $\mathcal{F}$ is invertible. Suppose that $X \in \ker\varphi \subset \mathcal{F}$, i.e., $\varphi(X) = X\vec{r} = \theta_n$. If X were non-zero matrix, then $\vec{r} = X^{-1}\theta_n = \theta_n$ which contradicts the choice of $\vec{r}$. Thus φ is injective. Moreover $\dim\mathcal{F} = \dim V_n$, so φ is bijective. $\square$

Lemma 3 states that φ is a linear isomorphism, but does not determine the inverse of the mapping. The following algorithm shows how to map a vector to a matrix.

Take a matrix A which is a primitive element of $\mathcal{F}$ and define the matrix $R = \left[\vec{r}, A\vec{r}, \ldots, A^{n-1}\vec{r}\right]$ formed from column vectors $A^k\vec{r}$, $k = 0, 1, \ldots, n-1$. By Lemma 1 and 2, the matrices $I, A, \ldots, A^{n-1}$ are linearly independent, so the matrix R is invertible. According to Lemma 3, the mapping φ is invertible, so for every non-zero vector $\vec{u} \in V_n$ there exists $k \in \{1, \ldots, q^n - 1\}$ such that $\varphi(A^k) = \vec{u}$ or equivalently $\vec{u} = A^k\vec{r}$. To find the matrix $A^k = \varphi^{-1}(\vec{u})$ define $U = \left[\vec{u}, A\vec{u}, \ldots, A^{n-1}\vec{u}\right]$. This yields $U = \left[A^k\vec{r}, AA^k\vec{r}, \ldots, A^{n-1}A^k\vec{r}\right] = A^kR$ and consequently $A^k = UR^{-1}$.

The construction uses the matrix A which generates the field $\mathbb{F}_q(A)$ (considered as a subalgebra of $M_n(\mathbb{F}_q)$). But, it is worth noticing that φ and its inverse do not depend on the matrix itself, but on the field $\mathbb{F}_q(A)$ and the vector $\vec{r}$.

Finding the inverse of φ is more efficient if A is chosen to be the companion matrix of a monic primitive polynomial $f = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n \in \mathbb{F}_q[x]$ and $\mathcal{F} = \mathbb{F}_q(A)$. In this case the characteristic polynomial of A equals $(-1)^n f$, so it is irreducible. The matrix A is the transition matrix of the linear feedback shift register (LFSR) determined by the coefficients $-c_0, -c_1, \ldots, -c_{n-1}$. Suppose $[s_1, \ldots, s_n]$ is the current state the LFSR. Then the next state is equal to $[s_2, \ldots, s_n, s_{n+1}]$ where $s_{n+1} = -c_0s_1 - c_1s_2 - \cdots - c_{n-1}s_n$, i.e.,

$$\begin{bmatrix} s_2 \\ s_3 \\ \vdots \\ s_n \\ s_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & -c_2 & \ldots & -c_{n-1} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-1} \\ s_n \end{bmatrix}.$$

Thus the matrices R and U consist of the columns which are obtained as n consecutive states of the LFSR including the initial states $\vec{r}$ and $\vec{u}$, respectively. More information on LFSR can be found in [5, Chapter 8].

3. The DDLM algorithm

Now, we shall describe a general cryptosystem based on double exponentiation in two matrix representations of a finite field.

Choose two non-zero vectors $\vec{r}, \vec{s} \in V_n$ and define two linear mappings $\Phi, \Psi \colon M_n(\mathbb{F}_q) \to V_n$ by $\Phi(X) = X\vec{r}$ and $\Psi(X) = X\vec{s}$ for all $X \in M_n(\mathbb{F}_q)$. Now let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two representations of the field $\mathbb{F}_{q^n}$ in $M_n(\mathbb{F}_q)$. In practice these representations are determined by suitable matrices, for example by primitive matrices of those fields. To make the encoding and decoding algorithm more efficient it is recommended to take fields $\mathcal{F}_1$ and $\mathcal{F}_2$ which are generated by companion matrices of primitive polynomials of degree n, as it was pointed out above. Let $\varphi = \Phi \restriction \mathcal{F}_1$ and $\psi = \Psi \restriction \mathcal{F}_2$ be restrictions of Φ and Ψ to $\mathcal{F}_1$ and $\mathcal{F}_2$, respectively. According to Lemma 3, φ and ψ are $\mathbb{F}_q$-linear isomorphisms.

Note that $\Lambda = \psi^{-1}\varphi$ is a linear isomorphism of $\mathcal{F}_1$ and $\mathcal{F}_2$ considered as vector spaces over $\mathbb{F}_q$ but it is not a field isomorphism, in general.

Recall that all non-zero elements of the field $\mathbb{F}_{q^n}$ form a cyclic group of order $N = q^n - 1$ denoted by $\mathbb{F}^*_{q^n}$. Let $U(\mathbb{Z}/N\mathbb{Z})$ denote the group of units of the quotient ring $\mathbb{Z}/N\mathbb{Z}$.

To encrypt a plain text represented by a vector $\vec{t} \in V_n$ by using a key $(k_1, k_2) \in U(\mathbb{Z}/N\mathbb{Z}) \times U(\mathbb{Z}/N\mathbb{Z})$ the following computation should be performed

$$\vec{t} \overset{\varphi^{-1}}{\longmapsto} T \overset{\hat{}k_1}{\longmapsto} T^{k_1} \overset{\Lambda}{\longmapsto} C \overset{\hat{}k_2}{\longmapsto} C^{k_2} \overset{\psi}{\longmapsto} \vec{c}. \tag{1}$$

Thus the encryption function E is defined by

$$E(\vec{t}, k_1, k_2) = \vec{c} = \psi\Big(\Lambda\big(\varphi^{-1}(\vec{t})^{k_1}\big)^{k_2}\Big).$$

To recover the original message from the cipher text $\vec{c}$ we should find $l_1 := k_1^{-1} \mod N$ and $l_2 := k_2^{-1} \mod N$, the inverse of k_1 and k_2 in $U(\mathbb{Z}/N\mathbb{Z})$, respectively. These inverses can be found by using the extended Euclidean algorithm. Then we compute

$$\vec{c} \overset{\psi^{-1}}{\longmapsto} C \overset{\hat{}l_2}{\longmapsto} C^{l_2} \overset{\Lambda^{-1}}{\longmapsto} T \overset{\hat{}l_1}{\longmapsto} T^{l_1} \overset{\varphi}{\longmapsto} \vec{t}.$$

The construction of DDLM may seem slightly complicated. But it is suitable to hardware implementation especially when $\mathcal{F}_1$ and $\mathcal{F}_2$ are generated by companion matrices of primitive polynomials.

Summarizing, for a given field $\mathbb{F}_q$ the DDLM algorithm is completely determined by a positive integer n two vectors in V_n and two matrices with the irreducible characteristic polynomial. The subalgebras generated by these matrices are matrix representations of the extension of degree n of the field $\mathbb{F}_q$. The encryption and decryption is performed in the multiplicative group of nonsingular matrices but to save memory, plain and cipher texts are represented as vectors. The conversions of matrices to vectors and vice versa are performed by the mappings φ and ψ and their inversions which are public as the matrices and the vectors are publicly known. In particular, it is easy to compute $N = q^n - 1$, the order of the multiplicative group of the fields. If someone knows the encryption key $(k_1, k_2) \in U(\mathbb{Z}/N\mathbb{Z}) \times U(\mathbb{Z}/N\mathbb{Z})$, then it is easy to find the related decryption key. Indeed, $k_i \in U(\mathbb{Z}/N\mathbb{Z})$ implies $GCD(k_i, N) = 1$, so by the extended Euclid algorithm one can find integers l_i, m_i such that $l_i \in U(\mathbb{Z}/N\mathbb{Z})$ and $k_i l_i + N m_i = 1$ for $i = 1, 2$. By an easy computation one can check that (l_1, l_2) is the decryption key related to (k_1, k_2). Therefore the encryption key has to be kept secret, i.e., DDLM is a private key cryptosystem. The security of DDLM is based on a well-known difficulty in calculating discrete logarithm in a finite field. Note that finding the key in the DDLM system is at least as hard as solving the discrete logarithm problem. It means that if we knew a fast algorithm $\mathcal{A}$ of finding the key of the DDLM algorithm, then we could solve the discrete logarithm problem easily. Indeed, suppose that we have an encryption device which calculates X^k for any invertible matrix $X \in M_n(\mathbb{F}_q)$ with a secret exponent k. Use the device to compute $Y := X^k$ and then to compute $Z = \big(\Lambda(Y)\big)^k$, where $\Lambda = \psi^{-1}\varphi$. Now applying the algorithm $\mathcal{A}$ to the pair X, Z we find the secret key k.

On the other hand, it is worth noticing that finding the key in DDLM seems to be more difficult because the result of the first exponentiation as well as the base of the second exponentiation are hidden, so the known algorithms solving the discrete logarithm problem cannot be applied immediately. This probably (with no evidence) makes the SED system stronger than the single Pohlig–Hellman system. In Section 4 we describe how to reduce the problem of finding a key in the DDLM to solve two single logarithm problems. Although the running time of this reduction is greater than solving the discrete logarithm problem, the algorithm is much faster than the exhaustive search through the key space.

Obviously, breaking a cryptosystem is not equivalent to finding the key. In fact, there are cryptosystems where decoding message is possible even without knowing the key (cf. the Remark 5, below).

Remark 4. Let $\vec{\theta}$ denote the zero vector in V_n. Observe, that $E(\vec{\theta}, k_1, k_2) = \vec{\theta}$ for all keys (k_1, k_2), i.e., the zero vector is self-coded. Moreover $\varphi^{-1}(\vec{r}) = I$ is the identity matrix, so $E(\vec{r}, k_1, k_2) = \psi\big(\psi^{-1}(\vec{r})^{k_2}\big)$. This reduces finding k_2 to solving the simple discrete logarithm problem, since ψ is public. Knowing k_2 it is easy to compute $\varphi\big(\varphi^{-1}(x)^{k_1}\big) = \psi^{-1}\big(E(x, k_1, k_2)^{k_2^{-1}}\big)$ which allows us to find k_1 by solving the simple logarithm problem. Therefore the security of the system requires $\vec{r} = \vec{s}$. In this case $\vec{r}$ is a self-coded vector for every key (k_1, k_2), so no additional information about the key is available. On the other hand $\vec{r} = \vec{s}$ implies $\Phi = \Psi$. Therefore the fields $\mathcal{F}_1$ and $\mathcal{F}_2$ have to be distinct. Otherwise, $\varphi = \psi$ and $E(\vec{t}, k_1, k_2) = \varphi\big(\varphi^{-1}(\vec{t})^{k_1 k_2}\big)$, i.e., DDLM would be equivalent to the Pohlig-Hellman system.

Remark 5. If k_1, k_2 are fixed powers of $p = \operatorname{char} \mathbb{F}_q$, then the encryption function becomes an $\mathbb{F}_p$-linear mapping. In this case the given plain text attack allows us to decrypt any message even without knowing the key. Indeed, suppose we have collected a lot of pairs $(\vec{t}, \vec{c})$ of plain and cipher text with $\vec{c} = E(\vec{t}, k_1, k_2)$. It is likely to happen that there are pairs $(\vec{t}_1, \vec{c}_1), \dots, (\vec{t}_n, \vec{c}_n)$ such that vectors $\vec{t}_1, \dots, \vec{t}_n$ form a $\mathbb{F}_q$-basis of V_n. Denote $T = [\vec{t}_1, \dots, \vec{t}_n]$ and $C = [\vec{c}_1, \dots, \vec{c}_n]$ i.e., the columns of the matrices T and C are equal to $\vec{t}_i$ and $\vec{c}_i$, $i = 1, \dots n$, respectively. The unknown plain text $\vec{t}$ can be recovered from known cryptogram $\vec{c}$ as $\vec{t} = TC^{-1}\vec{c}$.

It is also recommended to avoid the keys of the weight 2, i.e., $k = p^i + p^j$. Such keys might be vulnerable to various attacks developed by Patarin and Shamir (cf. [4, Chapter 4]).

Now we shall describe an algorithm which is equivalent to DDLM, but does not require to perform any exponentiation of matrices. Suppose $\mathcal{F}_1$ and $\mathcal{F}_2$ are matrix representations of $\mathbb{F}_{q^n}$ in $M_n(\mathbb{F}_q)$ and let A and B be matrices such that $\mathcal{F}_1 = \mathbb{F}_q(A)$ and $\mathcal{F}_2 = \mathbb{F}_q(B)$. Let α and β be standard roots of the characteristic polynomials of A and B, respectively. According to Lemma 1, there exist field isomorphisms $\Omega_A\colon \mathbb{F}_{q^n} \to \mathbb{F}_q(A)$ and $\Omega_B\colon \mathbb{F}_{q^n} \to \mathbb{F}_q(B)$ such that $\Omega(\alpha) = A$ and $\Omega(\beta) = B$, respectively. Define $\bar{\varphi} = \varphi \circ \Omega_A$ and $\bar{\psi} = \psi \circ \Omega_B$. The maps $\bar{\varphi}$ and $\bar{\psi}$ establish immediate linear isomorphisms from $\mathbb{F}_{q^n}$ to V_n and allow us to avoid exponentiations of matrices. Thus $\lambda = \bar{\psi}^{-1} \circ \bar{\varphi}$ is a mapping corresponding to Λ. Obviously, λ is a composition of $\mathbb{F}_q$-linear isomorphisms, so it is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^n}$ considered as a vector space over $\mathbb{F}_q$. It is easy to see that the encryption function $\bar{E}$ defined by $\bar{E}(\bar{t}, k_1, k_2) = \bar{\psi}\Big(\lambda\big(\bar{\varphi}^{-1}(\bar{t})^{k_1}\big)^{k_2}\Big)$ is equal to E. Thus we get an equivalent description of the DDLM algorithm.

$$
\begin{tikzcd}
 & \mathbb{F}_q(A) \arrow[r] & \mathbb{F}_q(A) \arrow[r, "\Lambda"] & \mathbb{F}_q(B) \arrow[r] & \mathbb{F}_q(B) \arrow[dr, "\psi"] & \\
V_n \arrow[ur, "\varphi^{-1}"] \arrow[dr, "\bar{\varphi}^{-1}"'] & & & & & V_n \\
 & \mathbb{F}_q(\alpha) \arrow[r] & \mathbb{F}_\alpha \arrow[r, "\lambda"] & \mathbb{F}_q(\beta) \arrow[r] & \mathbb{F}_q(\beta) \arrow[ur, "\bar{\psi}"'] &
\end{tikzcd}
\tag{2}
$$

Now we shall describe a matrix representation of the mapping λ which provides an efficient method of computation.

Lemma 6. *Let R be the matrix whose columns are the vectors $\vec{r}, A\vec{r}, \dots, A^{n-}\vec{r}$. Similarly let S be the matrix whose columns are the vectors $\vec{s}, B\vec{s}, \dots, B^{n-1}\vec{s}$. Denote $L = S^{-1}R$. Then*

$$\lambda(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = [1, \beta, \dots, \beta^{n-1}]\, L\, [a_0, a_1, \dots, a_{n-1}]^T$$

for all $a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_q$.

P r o o f. It is easy to check that

$$\begin{aligned}\bar{\varphi}\big(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\big) &= \varphi\big(a_0 I + a_1 A + \cdots + a_{n-1}A^{n-1}\big)\\ &= \big(a_0 I + a_1 A + \cdots + a_{n-1}A^{n-1}\big)\vec{r}\\ &= a_0 I\vec{r} + a_1 A\vec{r} + \cdots + a_{n-1}A^{n-1}\vec{r}\\ &= R[a_0, a_1, \dots, a_{n-1}]^T \in V_n .\end{aligned}$$

Similarly $\bar{\psi}(b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1}) = S[b_0, b_1, \dots, b_{n-1}]^T \in V_n$. For a vector $\vec{d} = [d_0, d_1, \dots, d_{n-1}]^T \in V_n$ the corresponding element in the field is a "polynomial" in β which can be obtained as $\bar{\psi}^{-1}(\vec{d}) = [1, \beta, \dots, \beta^{n-1}]S^{-1}\vec{d}$. Then

$$\begin{aligned}\lambda\big(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\big) &= \psi^{-1} \circ \varphi\big(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\big)\\ &= [1, \beta, \dots, \beta^{n-1}]S^{-1}R[a_0, a_1, \dots, a_{n-1}]^T,\end{aligned}$$

as required. □

Note that L is the matrix of λ in the bases $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $\{1, \beta, \dots, \beta^{n-1}\}$ of the fields $\mathbb{F}_q(\alpha)$ and $\mathbb{F}_q(\beta)$ considered as vector spaces over $\mathbb{F}_q$.

Example 7. The polynomials $f = 1 + x^3 + x^7$, $g = 1 + x + x^7$ are irreducible over $\mathbb{F}_2$. Choose $\vec{r} = \vec{s} = [1,1,1,1,1,1,1] \in \mathbb{F}_2^n$ and $A = C_f^T$ and $B = C_g^T$ the transpose of the companion matrices of these polynomials. Then

$$R = \begin{bmatrix} 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&0\\ 1&1&1&1&1&0&0\\ 1&1&1&1&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&0&0&0&0&1\\ 1&0&0&0&0&1&1 \end{bmatrix}, \quad S = \begin{bmatrix} 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&0\\ 1&1&1&1&1&0&0\\ 1&1&1&1&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&0&0&0&0&0\\ 1&0&0&0&0&0&0 \end{bmatrix},$$

$$L = \begin{bmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&0&1&0\\ 0&0&1&0&0&0&1\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{bmatrix}.$$

Observe that the mappings $\bar{\varphi}^{-1}$ and $\bar{\psi}$ in the diagram (2) have no influence on the security of the algorithm because they are publicly known.

We define a new encryption mapping $\tilde{E}$ as follows

$$t \xmapsto{\hat{k}_1} t^{k_1} \xmapsto{\lambda} s \xmapsto{\hat{k}_2} c\,, \tag{3}$$

i.e., for a plain text represented by $t \in \mathbb{F}_q(\alpha)$ we calculate the cryptogram $c = s^{k_2} \in \mathbb{F}_q(\beta)$ where $s = \lambda(t^{k_1})$. This function will be called a *reduced* DDLM. Observe that reduced DDLM requires less memory and works faster than the DDLM, without affecting the security.

Note that now all expontentions made to determine the value of $\tilde{E}$ are performed in the field $\mathbb{F}_{q^n}$. A simple estimation gives the running time equal $\mathcal{O}(n^3)$ and the memory capacity $\mathcal{O}(n^2)$. This is better than known public key cryptosystems but it is worse than private key systems. It is worth noticing that this system may be vulnerable to a timing attack. Namely, the time of computation may depend on the Hamming weight and the value of the key. This effect can be reduced by a suitable implementation.

The mapping λ between two exponentiations seems to make the computation of the key more complicated than solving a single discrete logarithm problem. The best choice for λ is a non-linear function with good diffusion property. Unfortunately, a hardware implementation of such functions is usually difficult. In DDLM, λ is chosen to be linear, but this choice has to be made very carefully. We shall show that the encryption function DDLM used to define SED may contain a potential insecurity.

4. Frobenius automorphism method

We shall show that breaking n-bit DDLM can be reduced in the cost $\mathcal{O}(q^{n/2})$ to solve a single discrete logarithm problem. The known algorithm, discovered by D. Coppersmith (cf. [Cp]), of solving a single discrete logarithm problem in $\mathbb{F}_{2^n}$ has the cost $\exp\Big(\big(c+o(1)\big)\sqrt[3]{n\ln^2 n}\Big)$. Thus finding the key takes much less time than an exhaustive search of the key space. By the above considerations, we know that the cryptanalysis of the DDLM is equivalent to the cryptanalysis of the encryption function $\tilde{E}$ defined by (3), i.e., $\tilde{E}(t,k_1,k_2) = \big(\lambda(t^{k_1})\big)^{k_2}$, for all $t \in \mathbb{F}_q(\alpha)$.

In the beginning we sketch the main idea of the attack. Denote by σ the Frobenius automorphism of $\mathbb{F}_{q^n}$ defined by $\sigma(x) = x^q$ for all $x \in \mathbb{F}_{q^n}$. For any $u \in \mathbb{F}_{q^n}$ the mapping $\lambda \circ \sigma - u(\sigma \circ \lambda)$ is $\mathbb{F}_q$-linear. Suppose that there exists an element $u \in \mathbb{F}_{q^n}$ such that $\dim\ker\big(\lambda \circ \sigma - u(\sigma \circ \lambda)\big) \geq (n+1)/2$. Then

$P\left(\left\{x\colon \dfrac{\lambda\circ\sigma(x)}{\sigma\circ\lambda(x)} = u\right\}\right) \geq \sqrt{q^{-n+1}}$, i.e., the probability that u is taken as a value of $\dfrac{\lambda\circ\sigma(x)}{\sigma\circ\lambda(x)}$ is relatively high. If such an element actually exists, then it is uniquely determined. To find the key k_2 it is enough to find the most probable value v of the expression

$$v = \frac{\lambda(x^{qk_1})^{k_2}}{\big(\lambda(x^{k_1})\big)^{qk_2}} = \left(\frac{\lambda(x^{qk_1})}{\big(\lambda(x^{k_1})\big)^{q}}\right)^{k_2} = u^{k_2}.$$

and then solve the discrete logarithm problem $u^{k_2} = v$. When we know k_2, it is not hard to find k_1.

Now we shall show how to determine the element u. This method will be described in a more general setting. For any subset $U \subseteq \mathbb{F}_{q^n}$ define $P(U) = |U|/q^n$, which denotes the probability that a random element of $\mathbb{F}_{q^n}$ belongs to U.

Observe that for any $u \in \mathbb{F}_{q^n}$ the mapping $\mu_u\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined by $\mu_u(x) := ux$ for all $x \in \mathbb{F}_{q^n}$ is $\mathbb{F}_q$-linear. We shall call μ_u a *multiplication map.* For a given monic, irreducible polynomial $f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n \in \mathbb{F}_q[x]$, the matrix of the multiplication map μ_α in the standard basis of $\mathbb{F}_q(\alpha)$ is equal to

$$C_f^T = \begin{bmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{n-1} \end{bmatrix},$$

i.e., it is the transpose of the companion matrix of f. It is easy to see that the characteristic polynomial of C_f is equal to $(-1)^n f$. Let $\chi\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an arbitrary $\mathbb{F}_q$-linear mapping. We say that a multiplication map μ_u is a *good approximation* of χ if $\dim\ker(\chi - \mu_u) \geq (n+1)/2$. We want to find a multiplication map which is the best approximation of χ. For given $u \in \mathbb{F}_{q^n}$ define

$$Z(u) := \ker(\chi - \mu_u) = \big\{x \in \mathbb{F}_{q^n} : \chi(x) = ux\big\}.$$

It is easy to check that $Z(u)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$.

Lemma 8. *An $\mathbb{F}_q$-linear endomorphism χ of $\mathbb{F}_{q^n}$ has at most one good approximation by a multiplicative map.*

Proof. Suppose that $u, v \in \mathbb{F}_{q^n}$ and both μ_u, μ_v are good approximations of χ. From $\dim Z(u) \geq (n+1)/2$ and $\dim Z(v) \geq (n+1)/2$ it follows that there is a non-zero element x in $Z(u) \cap Z(v)$. Thus $ux = \chi(x) = vx$, and consequently $u = v$. □

The next two lemmas say how to find such a good approximation provided it actually exists.

LEMMA 9. *If $u \in \mathbb{F}_{q^n}$ and μ_u is a good approximation of an $\mathbb{F}_q$-linear endomorphism $\chi\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, then for any $c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ there is a non-zero element $y \in \mathbb{F}_{q^n}$ such that $c\chi(y) = \chi(cy)$. Moreover $u = \chi(y)y^{-1}$.*

Proof. Set an element $c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. From $\dim Z(u) \geq (n+1)/2$ it follows that $c^{-1}Z(u)$ is a linear space with $\dim c^{-1}Z(u) \geq (n+1)/2$, so the intersection $Z(u) \cap c^{-1}Z(u)$ contains a non-zero element y. Hence $y, cy \in Z(u)$ and by the definition of $Z(u)$ we have $c\chi(y) = cuy$ and $\chi(cy) = ucy$. Thus $c\chi(y) = \chi(cy)$. Moreover, $c\chi(y) = cuy$ implies $u = \chi(y)y^{-1}$. □

From the above lemma it follows that all we need to find a good approximation of χ is to solve the equation $c\chi(y) - \chi(cy) = 0$ in the field $\mathbb{F}_{q^n}$, with fixed $c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ and then compute $u = \chi(y)y^{-1}$. Let g be an irreducible, monic polynomial of degree n and let $\beta \in \mathbb{F}_{q^n}$ be the standard root of g in $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$. Recall that C_g^T, the transpose of the companion matrix of g, is the matrix of μ_β in the standard basis of $\mathbb{F}_q(\beta)$. Finding the element y can be reduced to solving an easy linear algebra problem.

LEMMA 10. *Assume that μ_u is a good approximation of an $\mathbb{F}_q$-endomorphism χ and let H denote the matrix of χ in the standard basis of $\mathbb{F}_q(\beta)$. If $\vec{y} = [y_0, \dots, y_{n-1}]$ is a nonzero solution of the equation $\left(C_g^T H - H C_g^T\right)\vec{y} = \vec{\theta}$, then for $y = y_0 + y_1\beta + \dots + y_{n-1}\beta^{n-1}$ we have $u = \chi(y)y^{-1}$.*

Proof. By Lemma 9, for $c = \beta$ there is a nonzero element y in $\mathbb{F}_q(\beta) \setminus \mathbb{F}_q$ such that $\beta\chi(y) = \chi(\beta y)$. Let $\vec{y} = [y_0, \dots, y_{n-1}]^T$ be the coordinates of y with respect to the standard basis $1, \beta, \dots, \beta^{n-1}$. Since H is the matrix of χ and C_g^T is the matrix of μ_β, the coordinate vectors of $\beta\chi(y) = \mu_\beta \circ \chi(y)$ and $\chi(\beta y) = \chi \circ \mu_\beta(y)$ are equal $C_g^T H \vec{y}$ and $H C_g^T \vec{y}$, respectively. Thus, the coordinates of y can be obtained by solving the system of linear equations $\left(C_g^T H - C_g^T\right)\vec{y} = \vec{\theta}$. Applying Lemma 9 completes the proof. □

Remark 11. Having y computed it is easy to find $u = \chi(y)y^{-1}$ and check whether μ_u is a good approximation of χ, i.e., $\dim Z(u) \geq (n+1)/2$. Obviously, it may happen that either $\dim Z(u) < (n+1)/2$ for u computed above or $y = 0$ is the only solution of the equation $c\chi(y) - \chi(cy) = 0$. In the both cases the mapping χ does not have any good approximation by a multiplication map.

Now we can apply this method to $\chi = \lambda\sigma\lambda^{-1}\sigma^{-1}$. Suppose that there is $u \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ such that μ_u is a good approximation of χ. Define $W(u) = \{x \in \mathbb{F}_{q^n} : \lambda\sigma(x) = u\sigma\lambda(x)\}$. Then it is easy to see that $W(u)$ is a linear subspace of $\mathbb{F}_{q^n}$ such that $\sigma\lambda\big(W(u)\big) = Z(u)$, so $\dim Z(u) = \dim W(u) \geq (n+1)/2$.

Thus the probability that u is the value of $\dfrac{\lambda\sigma(x)}{\sigma\lambda(x)}$ is equal to the probability that a random element $x \in \mathbb{F}_{q^n}$ belongs to $Z(u)$ and both are greater than $q^{(-n+1)/2}$.

Recall that the matrix L defined in Lemma 6 is the matrix of λ in the bases $1, \alpha, \dots, \alpha^{n-1}$ and $1, \beta, \dots, \beta^{n-1}$ of $\mathbb{F}_{q^n}$. To find the matrix of $\chi = \lambda\sigma\lambda^{-1}\sigma^{-1}$ we need matrices of the Frobenius automorphism σ in the same bases. The entries of the matrices $F_\alpha = [a_{ij}]$ and $F_\beta = [b_{ij}]$ are defined by $\sigma(\alpha^{j-1}) = \alpha^{(j-1)q} = a_{1j} + a_{2j}\alpha + \dots + a_{nj}\alpha^{n-1}$ and $\sigma(\beta^{j-1}) = \beta^{(j-1)q} = b_{1j} + b_{2j}\beta + \dots + b_{nj}\beta^{n-1}$ for $j = 1, 2, \dots, n$. Then the matrix of χ equals $H = LF_\alpha L^{-1}F_\beta^{-1}$.

Example 12. 1. Let $n = 7$, $q = 2$, $f = x^7 + x^3 + 1$ and $g = x^7 + x + 1$, $\vec{r} = \vec{s} = [1, 1, 1, 1, 1, 1, 1]$.

It is easy to check that

$$F_\alpha = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \quad F_\beta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

are the matrices of the Frobenius automorphism in bases $1, \alpha, \dots, \alpha^6$ and $1, \beta, \dots, \beta^6$, respectively. Now we can compute the matrices $H = LF_\alpha L^{-1}F_\beta^{-1}$ and $M = C_g^T H - HC_g^T$.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad M = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Solving the equation $\left(C_g^T H - HC_g^T\right)\vec{y} = 0$ yields $\vec{y} = [0, 1, 1, 1, 1, 0, 1]^T$.

Thus we get the vector of coefficients of $\vec{u} = [1110000]$ or $\vec{u} = 70_{\mathrm{x}}$ in the hexadecimal form. This means that $u = 1 + \beta + \beta^2$.

2. A similar computation performed for $n = 127$ $q = 2$ $f = 1 + x^{63} + x^{127}$ $g = 1 + x^{30} + x^{127}$ gives the vector of coefficients

$$\begin{aligned}\vec{u} &= [0001000000110010110001111010111101110110110001101010 10\\ &\quad 11000001101101011110101011010001111100111011011101 1100\\ &\quad 000001110001110110 11]\\ &= \mathrm{0832C7AF76C6AB06D7AB47CEDDC071DB_x} \qquad \text{(127-bit integer).}\end{aligned}$$

Remark 13. The practical application of the procedure described above to attack the SED algorithm is the following. Suppose we have a device $\mathcal{E}$ which computes the reduced DDLM $\mathcal{E}(x) = E_r(x, k_1, k_2)$ for every input $x \in \mathbb{F}_{q^n}$ and secret, unknown key $(k_1, k_2) \in U(\mathbb{Z}/N\mathbb{Z}) \times U(\mathbb{Z}/N\mathbb{Z})$. Moreover, assume that we have already computed $u \in \mathbb{F}_{q^n}$ which is the most probable value of $\frac{\lambda\sigma(x)}{\sigma\lambda(x)}$ for $x \in \mathbb{F}_{q^n}$, i.e., μ_u is a good approximation of $\lambda\sigma\lambda^{-1}\sigma^{-1}$. To find the key proceed as follows:

Step 1. Choose a random element $x \in \mathbb{F}_{q^n}$ and compute the following elements $z = x^q$, $c = \mathcal{E}(z)$, $d = \big(\mathcal{E}(x)\big)^q$ and $v = cd^{-1}$.

Step 2. Find $k_2 \in U(\mathbb{Z}/N\mathbb{Z})$ such that $u^{k_2} = v$ (by solving the discrete logarithm problem $u^{k_2} = v$).

Step 3. Compute $l_2 = k_2^{-1}$, the inverse of k_2 in $U(\mathbb{Z}/N\mathbb{Z})$, and find $k_1 \in U(\mathbb{Z}/N\mathbb{Z})$ such that $z^{k_1} = \lambda^{-1}(c^{l_2})$.

Step 4. Check if the pair (k_1, k_2) is a proper key. If not, repeat the steps 1–4.

Conclusion. 1. According to Remark 11, we are able to detect whether the mapping λ is chosen in such a way that $\chi = \lambda\sigma\lambda^{-1}\sigma^{-1}$ has a good approximation. If this is the case, we perform the steps 1–4 until we find the key, i.e, the computed value $v = \frac{\mathcal{E}(x^q)}{(\mathcal{E}(x))^q}$ becomes equal to u^{k_2}. For randomly chosen $x \in \mathbb{F}_{q^n}$ this happens with the probability greater than or equal to $\frac{q^{(n+1)/2}}{q^n} = \frac{1}{q^{(n-1)/2}}$. So the expected number of iterations of the above algorithm does not exceed $q^{(n-1)/2}$. In particular, for $q = 2$ and $n = 127$ we expect to run this algorithm 2^{63} times. This means that finding the key is still a hard job but it is much faster than the exhaustive search through the entire key space.

2. The SED system with parameters recommended in [7] and [8] is vulnerable to this attack.

3. To protect the system from this attack, the matrix L has to be chosen in such a way that $LF_\alpha L^{-1}F_\beta^{-1}$ does not have any good approximation by a multiplication map.

REFERENCES

[1] BEARD, J. T. B. Jr.: *A canonical form for matrix fields*, Acta Arith. **25** (1974), 331–335.

[2] COHN, P. M.: *Algebra*, John Willey & Sons, 1974.

[3] COPPERSMITH, D.: *Fast evaluation of logarithms in field of characteristic 2*, IEEE Trans. Inform. Theory **30** (1984), 587–594.

[4] KOBLITZ, N.: *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin, 1998.

[5] LIDL, R.—NIEDERREITER, H.: *Finite Fields*, Addison-Wesley Publ. Comp. Reading, Massachusetts, 1983.

[6] POHLIG, S.—HELLMAN, M.: *An improved algorithm for computing logarithms over* $\mathbf{GF}(p)$ *and its cryptographic significance*, IEEE Trans. Inform. Theory **24** (1978), 106–110.

[7] ROGGEMAN, Y.—MUSYCK, E.: *A block cipher based on discrete logarithms*, (preprint).

[8] http: `www.ulb.ac.be/di/scsi/classicsys`.

Received April 4, 2002

Institute of Mathematics
Silesian University
PL–40 007 Katowice
POLAND

E-mail: mkula@us.edu.pl