# A cryptosystem based on double discrete logarithm

Mieczysław Kula

(*Draft version*)

## 1 Preliminaries

In 1978 S. Pohling and M. Hellman [3] 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 Pohling-Hellman cryptosystem which proceeds in two consecutive exponentiations performed in two (different) 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. [4], [5]). The basic part of this algorithm called DDLM uses the matrix representations of finite fields. At the begining 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 Pohling-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 $\boldsymbol{f} \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $n$. If $(\boldsymbol{f})$ denotes the ideal of $\mathbb{F}_q[x]$ generated by $\boldsymbol{f}$, then the factor ring $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(\boldsymbol{f})$ 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 $\boldsymbol{f}$. Multiplications can be optimised by choosing $\boldsymbol{f}$ to be a trinomial. The element of $\mathbb{F}_q[x]/(\boldsymbol{f})$ represented by the monomial $x$ is reffered to as the *standard root* of the polynomial $\boldsymbol{f}$ in $\mathbb{F}_{q^n}$. If $\alpha$ denotes the standard root of $\boldsymbol{f}$ 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 $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

All non-zero elements of the field $\mathbb{F}_{q^n}$ forms a cyclic group of order $N = q^n - 1$. The polynomial $\boldsymbol{f}$ is called *primitive* if its standard root is a generator of the multiplicative group $\mathbb{F}_{q^n}^*$. If $\alpha$ is a standard root of $\boldsymbol{f}$ then $\mathbb{F}_{q^n}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{N-1}\}$. Denote by $M_n(\mathbb{F}_q)$ the algebra of all $n \times n$ matrices over $\mathbb{F}_q$. Recall, the subalgebra $S_n(\mathbb{F}_q) = \{aI \in M_n(\mathbb{F}_q) : \ a \in \mathbb{F}_q\}$ 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 generated by $A$. It is easy to show that every matrix $X$ in $\mathbb{F}_q(A)$ can be presented as $X = a_0 I + a_1 A + a_2 A^2 + \cdots + a_{n-1} A^{n-1}$. Assume that the characteristic polynomial $\boldsymbol{f}$ of $A$ is irreducible. Then the mapping $\Omega : \mathbb{F}_q[x] \longrightarrow M_n(\mathbb{F}_q)$ defined by $\Omega(\boldsymbol{h}) = \boldsymbol{h}(A) = h_0 I + h_1 A + \cdots + h_k A^k$ for every $\boldsymbol{h} = h_0 + h_1 x + \cdots + h_k x^k \in \mathbb{F}_q[x]$ is a ring homomorphism with $\ker \Omega = (\boldsymbol{f})$ and $\operatorname{im} \Omega = \mathbb{F}_q(A)$. Thus $\mathbb{F}_q(A)$ is a field isomorphic to $\mathbb{F}_{q^n}$. It is easy to show that $\Omega$ determines a field ispmorphism $\bar{\Omega} : \mathbb{F}_q(\alpha) \longrightarrow \mathbb{F}_q(A)$ such that $\bar{\Omega}(\alpha) = A$.

For given monic polynomial $\boldsymbol{f} = f_0 + f_1 x + ... + f_{n-1} x^{n-1} + x^n \in \mathbb{F}_q[x]$ we denote

$$C_{\boldsymbol{f}} = \begin{bmatrix} 0 & 0 & \dots & 0 & -f_0 \\ 1 & 0 & \dots & 0 & -f_1 \\ 0 & 1 & \dots & 0 & -f_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -f_{n-1} \end{bmatrix}$$

the companion matrix of $\boldsymbol{f}$. It is easy to see that the the characteristic polynomial of $C_{\boldsymbol{f}}$ is equal to $(-1)^n \boldsymbol{f}$. More information on finite fields can be found in [2].

## 2 Two round Pohling - Hellman cryptosystem

Now, we shall describe a general cryptosystem based on double exponentiation in two matrix representations of a finite field. Let $\mathbb{F}_q^n$ denote the vector space of column vectors over $\mathbb{F}_q$. For a given non-zero vector $\vec{r} \in \mathbb{F}_q^n$ we define the mapping $\varphi : \ M_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^n$ by $\varphi(X) = X\vec{r}$ for every matrix $X \in M_n(\mathbb{F}_q)$. For a matrix $A \in M_n(\mathbb{F}_q)$ with irreducible characteristic polynomial it is easy to show that the restriction of $\varphi$ to $\mathbb{F}_q(A)$ is a linear isomorphism.

Choose another matrix $B \in M_n(\mathbb{F}_q)$ such that the characteristic polynomials of $B$ is irreducible over $\mathbb{F}_q$ and choose a non-zero vector $\vec{s} \in \mathbb{F}_q^n$ Define linear isomorphisms $\psi : \ \mathbb{F}_q(B) \longrightarrow \mathbb{F}_q^n$ by $\psi(Y) = Y\vec{s}$ for all $Y \in \mathbb{F}_q(B)$. Note that $\Lambda = \psi^{-1}\varphi$ is a linear bijection between fields $\mathbb{F}_q(A)$ and $\mathbb{F}_q(B)$ but it is not a field isomorphism, in general. Recall, $N = q^n - 1$. Let $U(\mathbb{Z}/N\mathbb{Z})$ denote the group of units of the ring $\mathbb{Z}/N\mathbb{Z}$.

To encrypt a plain text represented by a vector $\vec{t} \in \mathbb{F}_q^n$ with 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

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

To recover the original message from the cipher text $\vec{c}$ we should find $l_1 := k_1^{-1} \bmod N$ and $l_2 := k_2^{-1} \bmod N$ 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 encryption and decryption is performed in the multiplicative group of non-singular 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 $\varphi$ and $\psi$ and their inversions which are public as matrices $A$ and $B$ and vectors $\vec{r}$ and $\vec{s}$ are publicly known. Thus DDLM is secure if the key $(k_1, k_2)$ is kept secret. The construction of DDLM may seem slightly complicated. But it is suitable to hardware implementation especially when $A$ and $B$ are companion matrices of irreducible trinomials. In this case multiplication by $A$ or $B$ may be performed by linear feedback shift registers (LFSR).

Obviously, finding the key in the Pohling-Hellman system is possible when we can compute the discrete logarithm. Is worth noticing that here the job is 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 makes the SED system more strengthen than the single Pohling-Hellman system.

On the other hand finding the key in the DDLM system is at least as hard as solving the discrete logarithm problem. If we would know 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 secret exponent $k$. Use the device to compute $Y := X^k$ and then to compute $Z = (\Lambda(Y))^k$, where $\Lambda = \psi^{-1}\varphi$. Now applying the algorithm $\mathcal{A}$ to the pair $X, Z$ we find the secret key $k$. 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 below).

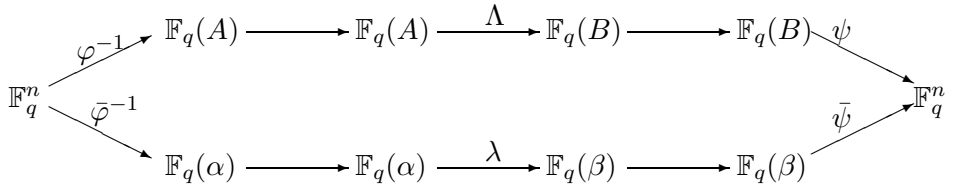
**Remark 1** 1. Let $\vec{\theta}$ denote the zero vector in $\mathbb{F}_q^n$. Observe, that $E(\vec{\theta}, k_1, k_2) = \vec{\theta}$ for all keys $k_1, k_2$, i.e., the zero vector is selfcoded. Moreover $\varphi^{-1}(\vec{r}) = I$ is the identity matrix, so $E(\vec{r}, k_1, k_2) = \psi(\psi^{-1}(\vec{r})^{k_2})$. This reduces finding $k_2$ to solving the simple discrete logarithm problem, since $\psi$ is public. Knowing $k_2$ it is easy to compute $\varphi(\varphi^{-1}x^{k_1}) = \psi^{-1}(E(x, k_1, k_2)^{k_2^{-1}})$ which allows us to find $k_1$ by solving the simple logarithm problem. Therefore the security of the system requries $\vec{r} = \vec{s}$. In this case $\vec{r}$ is a selfcoded vector for every key $(k_1, k_2)$, so no additional information about the key is available.

2. If $k_1, k_2$ are powers of $p =$ 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 $(\vec{t}, \vec{c})$ plain and cipher text with $\vec{c} = E(\vec{t}, k_1, k_2)$. It is likely to happen that there are pairs $(\vec{t}_1, \vec{c}_1), \ldots, (\vec{t}_n, \vec{c}_n)$ such that vectors $\vec{t}_1, \ldots, \vec{t}_n$ form a $\mathbb{F}_q$-basis of $\mathbb{F}_q^n$. Denote $T = [\vec{t}_1, \ldots, \vec{t}_n]$ $C = [\vec{c}_1, \ldots, \vec{c}_n]$ i.e., the columns of the matrices $T$ and $C$ are equal to $\vec{t}_i$ and $\vec{c}_i$, $i = 1, \ldots n$, respectively. The unknown plain text $\vec{t}$ can be recoverd form known cryptogram $\vec{c}$ as $\vec{t} = TC^{-1}\vec{c}$.

3. It is recomended 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 [K, Chapter 4]).

4. The mappings $\varphi^{-1}$ and $\psi$ in the diagramm (1) have no influence on the security of the algorithm because they are publicly known. The algorithm requires less memory and works faster without those mappings without affecting the security. The algorithm will be called a *reduced* DDLM.

Let $A$ and $B$ be matrices as above and let $\boldsymbol{f}$ and $\boldsymbol{g}$ be their characteristic polynomials, respectively. Let $\bar{\Omega}_A : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q(A)$ and $\bar{\Omega}_B : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q(B)$ be field isomorphisms such that $\bar{\Omega}(\alpha) = A$ and $\Omega(\bar{\beta}) = B$. Define $\bar{\varphi} = \varphi \circ \bar{\Omega}_A$ and $\bar{\psi} = \psi \circ \bar{\Omega}_B$. The maps $\bar{\varphi}$ and $\bar{\psi}$ establish immediate linear isomorphisms from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q^n$ and allow us to avoid computing exponents of matrices. Thus $\lambda = \bar{\psi}^{-1} \circ \bar{\varphi}$ an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_q^n$ corresponding to $\Lambda$. It is easy to see that the encryption function $\bar{E}$ defined by $\bar{E}(x, k_1, k_2) = \bar{\psi}(\lambda(\bar{\varphi}^{-1}(x^{k_1}))^{k_2})$ is equal to $E$. Thus we get an equivalent description of DDLM algorithm.




Now we shall describe a matrix representation of the encription and decription mapping which provides an efficient methods of computation. Let $R$ be the matrix whose columns are the vectors $\vec{r}, A\vec{r}, \ldots, A^{n-1}\vec{r}$. It is easy to check that

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

For a vector $\vec{c} = [c_0, c_1, \ldots, c_{n-1}]$ the corresponding element of the field is a "polynomial" in $\alpha$ which can be get as

$$\varphi^{-1}(\vec{c}) = [1, \alpha, \ldots, \alpha^{n-1}]R^{-1}\vec{c}.$$

Similarly let $S$ be the matrix whose columns are the vectors $\vec{s}, B\vec{s}, \ldots, B^{n-1}\vec{s}$. It is easy to check that $\bar{\psi}(b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1}) = S[b_0, b_1, \ldots, b_{n-1}]^T \in \mathbb{F}_q^n$. For a vector $\vec{d} = [d_0, d_1, \ldots, d_{n-1}]$ the corresponding element of the field is a "polynomial" in $\beta$ which can be obtained as $\bar{\varphi}^{-1}(\vec{d}) = [1, \beta, \ldots, \beta^{n-1}]S^{-1}\vec{d}$. Denote

$$L = S^{-1}R. \tag{2}$$

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

**Example 2** The polynomials $\boldsymbol{f} = 1+x^3+x^7$ , $\boldsymbol{g} = 1+x+x^7$ are irreducible over $\mathbb{F}_2$. Choose $\vec{r} = \vec{s} = [1,1,1,1,1,1,1] \in \mathbb{F}_2^n$ and $A = C_{\boldsymbol{f}}^T$ and $B = C_{\boldsymbol{g}}^T$ the transpose of the companion matrices of these polynomials. Then

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

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

Note that now all expontentions made for determine the value of $\bar{E}$ 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 comparable with 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 $\lambda$ in between two exponentiations makes the computation of the key more complicated, than solving a single discrete logarithm problem. The best choice for $\lambda$ is a non-linear function with good diffusion property. Unfortunately, a hardware implementation of such functions is usually difficult. In DDLM $\lambda$ is chosen to be linear, but this choice has to be done very carefully. We shall show that the encryption function DDLM used to define SED may contain a potential insecurity.

## 3 Frobenius automorphism method

We shall show that breaking $n$-bit DDLM can be reduced in a cost $\mathcal{O}(q^{n/2})$ to solve a single discrete logarithm problem. Since known algorithm of solving a single discrete problem in $\mathbb{F}_{2^n}$ of size $n$ has a cost $\exp((c+o(1))\sqrt[3]{k\ln^2 k})$. Thus finding the key takes much less time than the the exuastive search the key space. According to Remark 1.4 the cryptanalysis of the algorithm can be restricted to a reduced encryption mapping $E_r$ defined as follows:

$$t \stackrel{\gamma_{k_1}}{\longmapsto} t^{k_1} \stackrel{\lambda}{\longmapsto} p \stackrel{\gamma_{k_2}}{\longmapsto} c.$$

for a plain text represented by $t \in \mathbb{F}_q(\alpha)$ we calculate the cryptogram $c = p^{k_2} \in \mathbb{F}_q(\beta)$ where $p = \lambda(t^{k_1})$.

At the beginning we sketch the main idea of the attack. Denote $\sigma$ the Frobenius automorphism of $\mathbb{F}_{q^n}$ defined by $\sigma(x) = x^q$. 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 $\dim \ker(\lambda \circ \sigma - u(\sigma \circ \lambda)) > n/2$. Then the probability $P(\{x \mid \dfrac{\lambda \circ \sigma(x))}{\sigma \circ \lambda(x)} = u\}) > \sqrt{q^{-n}}$. If such an element actually exists, then it is uniquely determined. To find the key $k_2$ it is enough to find the most probably value $v$ of the expression

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

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. Observe that for any $u \in \mathbb{F}_{q^n}$ the mapping $\mu_u : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ defined by $\mu_u(x) := ux$ for all $x \in \mathbb{F}_{q^n}$ is $\mathbb{F}_q$-linear. We shall call $\mu_u$ a *multiplication map*. Let $\chi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ be an arbitrary $\mathbb{F}_q-$linear mapping. We say that a multiplication map $\mu_u$ is a *good approximation* of $\chi$ if $\dim \ker(\chi - \mu_u) > n/2$. We want to find the best approximation of $\chi$ by a multiplication map. For given $u \in \mathbb{F}_{q^n}$ define

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

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

**Lemma 3** *If $u, v \in \mathbb{F}_{q^n}$ and both $\mu_u, \mu_v$ are good approximations of $\chi$, then $u = v$.*

*Proof*. It follows from $\dim Z(u) > n/2$ and $\dim Z(v) > n/2$ that there is a non-zero element $x$ in $Z(u) \cap Z(v)$. Thus $ux = \chi(x) = vx$, and consequently $u = v$. ∎

So we proved that a linear mapping has at most one good approximation. The next lemma says how to find such a good aproximation provided it actually exists.

**Lemma 4** *Let $u \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ such that $\dim Z(u) > n/2$. 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 $c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. It follows from $\dim Z(u) > n/2$ that $c^{-1}Z(u)$ is a linear space with $\dim c^{-1}Z(u) > n/2$, 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 $u = \chi(y)y^{-1}$. ∎

It follows from the above lemma that all we need to find a good approximation of $\chi$ by a multiplication map 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 $u = \chi(y)y^{-1}$. This is an easy linear algebra problem. Let $\beta$ be the standard root of $\boldsymbol{g}$ in $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$. Then elements $1, \beta, \ldots, \beta^{n-1}$ form an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ (called standard) and every element in $\mathbb{F}_{q^n}$ is a value of a polynomial of degree less than $n$ in $\beta$. It is easy to check that the matrix of $\mu_\beta$ in this basis is equal to $C_{\boldsymbol{g}}$ the companion matrix of $\boldsymbol{g}$. Suppose $y = y_0 + y_1\beta + \cdots + y_{n-1}\beta^{n-1}$ with unknown coefficients $y_0, y_1, \ldots, y_{n-1} \in \mathbb{F}_q$. Let $H$ denote the matrix of $\chi$ in the standard basis. Then the coefficients of $y$ can be obtained by solving the system of linear equations $(C_{\boldsymbol{g}}H - HC_{\boldsymbol{g}})[y_0, \ldots, y_{n-1}]^T = \theta$. Having $y$ computed it is easy to find $u = \chi(y)y^{-1}$ and check whether $\mu_u$ is a good approximation of $\chi$, i.e., $\dim Z(u) > n/2$.

**Remark 5** Obviously, it may happen that $\dim Z(u) \leq n/2$ for $u$ computed above or $u = 0$ is the only solution to the equation $c\chi(y) - \chi(cy) = 0$. In the both cases the mapping $\chi$ has no good approximation by a multiplication map.

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

Thus the probability that the value of

$$\frac{\lambda\sigma(x)}{\sigma\lambda(x)}$$

equals $u$ is equal to the probability that a random element $x \in \mathbb{F}_{q^n}$ belongs to $Z(u)$ and is greater then $q^{-n/2}$.

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

**Example 6** 1. Let $n = 7$ , $q = 2$ , $\boldsymbol{f} = x^7 + x^3 + 1$ and $\boldsymbol{g} = x^7 + x + 1$ , $\vec{r} = \vec{s} = [1, 1, 1, 1, 1, 1, 1]$.
It is easy to check that

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

are the matrices of the Frobenius automorphism in bases $1, \alpha, \ldots, \alpha^{n-1}$ and $1, \beta, \ldots, \beta^{n-1}$, respectively.

Now we can compute the matrices $H = LF_\alpha L^{-1}F_\beta^{-1}$ and $M = C_{\boldsymbol{g}}H - HC_{\boldsymbol{g}}$.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \qquad M = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Solving the equation $(C_{\boldsymbol{g}}H - HC_{\boldsymbol{g}})\vec{y} = 0$ 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 in the hexadecimal form. This means that $u = 1 + \beta + \beta^2$

2. A similar computation perfomed for $n = 17$ , $q = 2$ , $\boldsymbol{f} = 1 + x^3 + x^{17}$ , $\boldsymbol{g} = 1 + x^5 + x^{17}$ gives the vector of coefficients $\vec{u} = [10011000000000000]$ or $\vec{u} =$\$13000 in the hexadecimal form. This means that $u = 1 + \beta^3 + \beta^4$.

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

$$\begin{aligned} \vec{u} &= 00010000011001011000111101011110111011011000110101010110000011 \\ &\quad 0 \\ &\quad 11010111101010110100011111001110110111011100000001110001110110 \\ &\quad 11 \\ &= \$0832C7AF76C6AB06D7AB47CEDDC071DB \qquad (127 - \text{bit integer}) \end{aligned}$$

**Remark 7** 1. The practical application of the procedure described above to attack the SED algorithm is the following: Suppose we have a device $\mathcal{E}$ which compute 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 $(k_1, k_2) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Moreover, assume that we have already computed $u \in \mathbb{F}_q$ which is the most probaly value of $\dfrac{\lambda \circ \sigma(x)}{\sigma \circ \lambda(x)}$ for $x \in \mathbb{F}_{q^n}$. To find the key proceed as follows:

Step 1 Choose a random element $x \in \mathbb{F}_{q^n}$ and compute the following: $z = x^2$, $c = \mathcal{E}(z)$ and $d = (\mathcal{E}(x))^2$, $v = cd^{-1}$

Step 2 Find $k_2 \in \mathbb{Z}/N\mathbb{Z}$ such that $u^{k_2} = v$.

Step 3 Compute $l_2 = k_2^{-1}$ the inverse of $k_2$ in $\mathbb{Z}/N\mathbb{Z}$ and find $k_1 \in \mathbb{Z}/N\mathbb{Z}$ 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 – 3.

For $n = 127$ we expect to run this algorithm $2^{64}$ times. This means that finding the key still a hard job but it is much faster than the exhaustive search through the entire key space.

2. All SED systems constructed for irreducible trinomials of degree 7, 17, 127 are vulnerable to this attack.

3. To protect the system from this attack the matrix $L$ has to be chosen in a such way that $LF_\alpha L^{-1} F_\beta^{-1}$ has no good approximation by a multiplication map.

# References


[1] N. Koblitz; Algebraic Aspects of Cryptography. Springer-Verlag 1998.

[2] R. Lidl, H. Niederreitr; Finite Fields. Addison-Wesley Publ. Comp. Reading, Massachsetts 1983.

[3] S. Pohling, M. Hellman; An improved algorithm for computing logarithms over $\mathbf{GF}(p)$ and its cryptographic significance. IEEE Trans. on Inform. Theory 24 (1978) pp. 106-110.

[4] Y. Roggeman, E. Musyck; A block Cipher based on Discrete Logarithms. (preprint)

[5] Y. Roggeman, E. Musyck; A block Cipher based on Discrete Logarithms. (preprint)