Finite Fields and Their Applications 71 (2021) 101810

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A structural attack to the DME-$(3, 2, q)$ cryptosystem

Martin Avendaño [a,1], Miguel Marco [b,*,2]

[a] *Centro Universitario de la Defensa, Spain*
[b] *IUMA, Universidad de Zaragoza, Spain*

A R T I C L E I N F O

Article history:
Received 25 February 2020
Received in revised form 16 December 2020
Accepted 28 December 2020
Available online xxxx
Communicated by Neal Koblitz

MSC:
11T06

Keywords:
Cryptography

A B S T R A C T

We present a structural attack on the DME cryptosystem with parameters $(3, 2, q)$. The attack recovers 10 of the 12 coefficients of the first linear map. We also show that, if those 12 coefficients were known, the rest of the private key can be efficiently obtained by solving systems of quadratic equations with just two variables.

1. Introduction

DME stands for "double matrix exponentiation". It is a family of multivariate encryption primitives over finite fields, parametrized by two integers and a field size (in bits). It was developed by Luengo, and the version with parameters $(3, 2, 2^{48})$ was presented to the NIST call for quantum-resistant public-key cryptographic algorithms [1].

* Corresponding author.
E-mail address: mmarco@unizar.es (M. Marco).

[1] Partially supported by MTM2016-76868-C2-2-P.
[2] Partially supported by MTM2016-76868-C2-2-P and E22_20R.

https://doi.org/10.1016/j.ffa.2021.101810
1071-5797/

The encryption map consists of a composition of three secret linear maps and two public matrix exponentiations, defining a polynomial map with very high degree, and moderated number of monomials. This map can be inverted provided we know the secret linear maps.

During the revision process at NIST, Beullens claimed to have found an attack against DME-$(3, 2, 2^{48})$ consisting on using Weil descent to convert the map in a quartic one over $\mathbb{F}_2$ (with a much larger set of variables), and then decompose it in two quadratic ones. However, his claims about the complexity and/or feasibility of such an attack could not be proved (see [2]).

Later, Beullens proposed another attack ([3], [4]) against the submitted implementation that took advantage of the lack of a proper padding. This attack used 2^{24} decryption queries, and analyzed the cases where the decryption resulted in an error. It was practical, but did not essentially break the underlying mathematical problem, so it could be prevented by using a secure padding.

Here we present a structural attack against DME-$(3, 2, q)$ that reduces the difficulty of recovering the private key from the public one from the claimed 256 bits to just $log_2(q^2)$. It is completely passive in the sense that it does not require any interaction, just the knowledge of the public key. The attack does not rely on any implementation details, since it considers only the underlying mathematical problem.

2. Description of the system

We first describe the DME cryptosystem. We focus only on the mathematical description, ignoring all the implementation details (such as how bits are transformed into elements of $\mathbb{F}_q$, padding, etc).

2.1. Setup

The system requires a common setup for all users, consisting on the following:

- Two positive integers $m \geq n$.
- A finite field $\mathbb{F}_q$ of characteristic p.
- An explicit isomorphism of $\mathbb{F}_q$-vector spaces $\mathbb{F}_q^n \cong \mathbb{F}_{q^n}$.
- An explicit isomorphism of $\mathbb{F}_q$-vector spaces $\mathbb{F}_q^m \cong \mathbb{F}_{q^m}$.
- A $m \times m$ matrix E, whose nonzero entries are powers of p, that is invertible modulo $q^n - 1$, and whose rows have only two nonzero entries.
- A $n \times n$ matrix F, whose nonzero entries are powers of p, that is invertible modulo $q^m - 1$, and whose rows have only two nonzero entries.
- A permutation map $M : \mathbb{F}_q^{nm} \to \mathbb{F}_q^{nm}$ such that

$$M((\mathbb{F}_q^n \setminus \{0\})^m) \subseteq (\mathbb{F}_q^m \setminus \{0\})^n.$$

For the implementation submitted to the NIST call the following choices were made:

- $m = 3$, $n = 2$.
- The field $\mathbb{F}_q$ is the field of 2^{48} elements, represented as polynomials in $\mathbb{F}_2[x]$ modulo the polynomial $x^{48} + x^{28} + x^{27} + x + 1$.
- The identification is done by considering $\mathbb{F}_{q^2}$ as the polynomials in $\mathbb{F}_q[T]$ modulo $T^2 + a \cdot T + b$, with
  $a = x^{43} + x^{38} + x^{36} + x^{34} + x^{29} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{13} + x^9 + x^8 + x^4 + x^3 + x + 1$
  $b = x^{47} + x^{46} + x^{45} + x^{43} + x^{40} + x^{39} + x^{38} + x^{37} + x^{35} + x^{31} + x^{30} + x^{27} + x^{26} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{16} + x^{14} + x^9 + x^8 + x^7 + x^3 + x^2 + 1$
  and taking coordinates in the basis $(1, T)$.
- The identification is done by considering $\mathbb{F}_{q^3}$ as the polynomials in $\mathbb{F}_q[S]$ modulo $S^3 + c \cdot S^2 + d \cdot S + e$ with
  $c = x^{43} + x^{42} + x^{41} + x^{40} + x^{38} + x^{37} + x^{36} + x^{34} + x^{33} + x^{29} + x^{26} + x^{24} + x^{22} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^3 + x^2 + x.$
  $d = x^{46} + x^{45} + x^{44} + x^{41} + x^{38} + x^{37} + x^{33} + x^{32} + x^{31} + x^{30} + x^{25} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$
  $e = x^{47} + x^{46} + x^{42} + x^{39} + x^{38} + x^{35} + x^{32} + x^{26} + x^{25} + x^{24} + x^{23} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^2 + x$
  and taking coordinates in the basis $(1, S, S^2)$.
- The matrix $E = \begin{pmatrix} 2^{24} & 2^{59} & 0 \\ 2^{21} & 0 & 2^{28} \\ 0 & 2^{29} & 2^{65} \end{pmatrix}$
- The matrix $F = \begin{pmatrix} 2^{50} & 2^{24} \\ 2^7 & 2^{88} \end{pmatrix}$
- M is the identity.

2.2. Matrix exponentiations

The scheme makes use of a special kind of map called matrix exponentiation. Consider a vector $\bar{x} = (x_1 \ldots, x_m) \in (\mathbb{F}_{q^n}^*)^m$, and the matrix E defined above. We define the vector $\bar{x}^E := (x_1^{E_{11}} \cdot x_2^{E_{12}} \cdots x_m^{E_{1m}}, \ldots, x_1^{E_{m1}} \cdot x_2^{E_{m2}} \cdots x_m^{E_{mm}})$.

Analogously, we define a map $(\mathbb{F}_{q^m}^*)^n \to (\mathbb{F}_{q^m}^*)^n$ by using the matrix F.

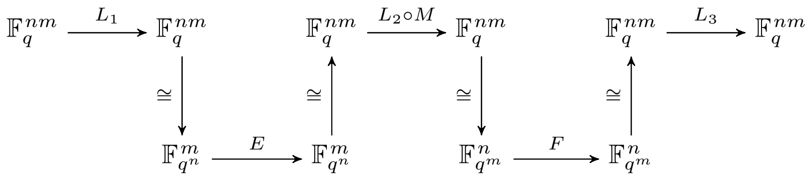
It is easy to check that these are polynomial maps, even considered as maps from $\mathbb{F}_q^{nm}$ to $\mathbb{F}_q^{nm}$ (by composing with the isomorphisms fixed in the setup). It is also easy to check that the inverse matrices (mod $q^n - 1$ and $q^m - 1$ respectively) determine inverse maps.

By abuse of notation, we use the same letter to represent both the matrix and the corresponding map.

2.3. Keys and encryption/decryption maps

With this setup, the private key is a triple of invertible $nm \times nm$ matrices over $\mathbb{F}_q$, (L_1, L_2, L_3) such that L_1 is a diagonal sum of m square blocks $L_{11}, \ldots, L_{1m}$ of size $n \times n$; L_2 and L_3 are diagonal sums of n blocks ($L_{21}, \ldots, L_{2n}$ and $L_{31}, \ldots, L_{3n}$ respectively) of size $m \times m$. They can be regarded as linear maps $\mathbb{F}_q^{nm} \to \mathbb{F}_q^{nm}$.

Once these matrices are chosen, we can consider the following composition of maps



The result is a multivariate polynomial map from $\mathbb{F}_q^{nm}$ to itself. In the expanded expression of this map, the exponents that appear at the end depend only on the entries of E and F, hence are public. The public key will be the coefficients that appear in that expression. The structure of the system has been carefully designed to ensure that the number of monomials in this expansion is not too large.

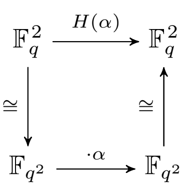
Note that each step in the composition is invertible (assuming we stay always inside $(\mathbb{F}_{q^n}^*)^m$ and $(\mathbb{F}_{q^m}^*)^n$ at the steps E and F respectively) by using the inverses of the involved matrices. That is, the whole map can be efficiently inverted if we know the private key.

3. Malleability of the private key

In this section we show how different private keys may correspond to the same public key. This fact will be used to assume that the private key has a special form.

From now on, we assume that $n = 2$ and $m = 3$, as in the version submitted to the NIST.

Take $\alpha \in \mathbb{F}_{q^2}^*$. The multiplication by α defines a map from $\mathbb{F}_{q^2}$ to itself that is $\mathbb{F}_q$-linear. So there exists a matrix $H(\alpha)$ such that the corresponding linear map makes the following diagram commute.



Analogously, for any $\lambda \in \mathbb{F}_{q^3}^*$ there exists a matrix $G(\lambda)$ whose corresponding linear map makes the following diagram commute

$$\begin{array}{ccc} \mathbb{F}_q^3 & \xrightarrow{G(\lambda)} & \mathbb{F}_q^3 \\ \cong \downarrow & & \uparrow \cong \\ \mathbb{F}_{q^3} & \xrightarrow{\cdot\lambda} & \mathbb{F}_{q^3} \end{array}$$

Clearly, $H(\alpha)^{-1} = H(\alpha^{-1})$ and $G(\lambda)^{-1} = G(\lambda^{-1})$.

Lemma 1. *Let $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}^*$ such that $\alpha^{E_{21}}\gamma^{E_{23}} = \delta \in \mathbb{F}_q^*$. Then the private keys*

- $(L_{11}, L_{12}, L_{13}, L_{21}, L_{22}, L_{31}, L_{32})$
- $(H(\alpha)L_{11}, H(\beta)L_{12}, H(\gamma)L_{13}, L_{21}\begin{pmatrix} \multicolumn{2}{c}{H(\alpha^{E_{11}}\beta^{E_{12}})^{-1}} & \begin{matrix} 0 \\ 0 \end{matrix} \\ 0 \quad 0 & & \delta^{-1} \end{pmatrix},$
  $L_{22}\begin{pmatrix} \delta^{-1} & 0 \quad 0 \\ \begin{matrix} 0 \\ 0 \end{matrix} & H(\beta^{E_{23}}\gamma^{E_{33}})^{-1} \end{pmatrix}, L_{31}, L_{32})$

correspond to the same public key.

Proof. Is a direct consequence of the commutativity of the previous diagrams, and the fact that

$$\begin{aligned} &(x_1, x_2, x_3)^E = (y_1, y_2, y_3) \\ &\quad \Longrightarrow (\alpha x_1, \beta x_2, \gamma x_3)^E = (\alpha^{E_{11}}\beta^{E_{12}}y_1, \alpha^{E_{21}}\gamma^{E_{23}}y_2, \beta^{E_{32}}\gamma^{E_{33}}y_3) \quad \square \end{aligned}$$

Analogously, we also have

Lemma 2. *Let $\lambda, \mu \in \mathbb{F}_{q^3}^*$. Then the private keys*

- $(L_{11}, L_{12}, L_{13}, L_{21}, L_{22}, L_{31}, L_{32})$
- $(L_{11}, L_{12}, L_{13}, G(\lambda)L_{21}, G(\mu)L_{22}, L_{31}G(\lambda^{F_{11}}\mu^{F_{12}})^{-1}, L_{32}G(\lambda^{F_{21}}\mu^{F_{22}})^{-1})$

produce the same public key.

We can use these facts to assume that the private key has a specific form

Lemma 3. *Every valid public key corresponds to a private key that satisfies the following form:*

- $L_{11} = \begin{pmatrix} * & 1 \\ * & 0 \end{pmatrix}$

- $L_{12} = \begin{pmatrix} * & 1 \\ * & 0 \end{pmatrix}$
- $L_{13} = \begin{pmatrix} * & a \\ * & b \end{pmatrix}$ *with either* $(a+bT)^{E_{23}} = 1+cT$ *for some* $c \in \mathbb{F}_q$ *or* $(a+bT)^{E_{23}} = T$
- $L_{21} = \begin{pmatrix} * & * & 1 \\ * & * & 0 \\ * & * & 0 \end{pmatrix}$
- $L_{22} = \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$

where the $*$ *symbols represent arbitrary elements of* $\mathbb{F}_q$*.*

Proof. If it comes from a secret key $(L_{11}, L_{12}, L_{13}, L_{21}, L_{22}, L_{31}, L_{32})$, we choose $\alpha, \beta \in \mathbb{F}_{q^2}^*$ as follows:

- α is the multiplicative inverse of the element of $\mathbb{F}_{q^2}$ corresponding (via the isomorphism) to the second column of L_{11}.
- β is the multiplicative inverse of the element of $\mathbb{F}_{q^2}$ corresponding to the second column of L_{12}.

This way, $H(\alpha)L_{11} = \begin{pmatrix} * & 1 \\ * & 0 \end{pmatrix}$ and $H(\beta)L_{12} = \begin{pmatrix} * & 1 \\ * & 0 \end{pmatrix}$.

Let τ be the element of $\mathbb{F}_{q^2}$ corresponding to the second column of L_{13}. Assume that $\alpha^{-E_{21}}\tau^{E_{23}} = \delta + \varepsilon T$ with $\delta \neq 0$. Choose $\gamma \in \mathbb{F}_{q^2}^*$ such that $\alpha^{E_{21}}\gamma^{E_{23}} = \delta^{-1}$ (this can be done easily by raising $\delta^{-1}\alpha^{-E_{21}}$ to the inverse of E_{23} modulo $q^2 - 1$). If $H(\gamma)L_{13} = \begin{pmatrix} * & a \\ * & b \end{pmatrix}$, then

$$(a + bT)^{E_{23}} = \gamma^{E_{23}}\tau^{E_{23}} = \delta^{-1}\alpha^{-E_{21}}\tau^{E_{23}} = \delta^{-1}(\delta + \varepsilon T) = 1 + cT$$

for some $c \in \mathbb{F}_q$.

If $\delta = 0$ we can do a similar computation using ε instead of δ, to get that $(a+bT)^{E_{23}} = T$.

Applying Lemma 1 with $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}^*$, we can construct a private key with L_{11}, L_{12}, L_{13} as in the statement.

Now choose λ, μ to be the inverse multiplicatives of the elements of $\mathbb{F}_{q^3}$ corresponding to the third column of L_{21} and the first column of L_{22} respectively.

Applying Lemma 2 to this new private key we obtain one where L_{21}, L_{22} are also as claimed. $\square$

4. Recovering information about the special private key from the public key

In this section we assume that the private key has the form obtained in the previous section. We show how to compute the unknown coefficients of L_1 from the coefficients in the public key. Moreover, we can also compute six coefficients from L_3.

Let's start by fixing some notation. Let l_{11}, l_{12} be the elements of $\mathbb{F}_{q^2}$ that correspond to the columns of L_{11}. As we have shown in the previous section, we can assume that $l_{12} = 1$. Analogously, l_{21}, l_{22} and l_{31}, l_{32} are the elements of $\mathbb{F}_{q^2}$ that correspond to the columns of L_{12} and L_{13}, respectively. As before, we can assume that $l_{22} = 1$ and $l_{32} = a + bT$ where $(a + bT)^{E_{23}}$ is either $1 + cT$ or T.

Define

- $f_1 + f_2T := {l_{11}}^{E_{21}} {l_{31}}^{E_{23}}$
- $g_1 + g_2T := {l_{11}}^{E_{21}} {l_{32}}^{E_{23}}$
- $h_1 + h_2T := {l_{12}}^{E_{21}} {l_{31}}^{E_{23}} = {l_{31}}^{E_{23}}$

where $f_1, f_2, g_1, g_2, h_1, h_2 \in \mathbb{F}_q$.

Lemma 4. *Let (η_1, η_2, η_3), (η_4, η_5, η_6) be the first column of L_{31} and L_{32} respectively.*

If we write the encryption map as a polynomial in $x_1, \ldots, x_6$, and $(a+bT)^{E_{23}} = 1+cT$, the terms that only involve the variables x_1 and x_6 in the i'th component are

- $\eta_i c^{F_{12}} (x_1^{E_{21}} x_6^{E_{23}})^{F_{11}+F_{12}}$ *for $i = 1, 2, 3$*
- $\eta_i c^{F_{22}} (x_1^{E_{21}} x_6^{E_{23}})^{F_{21}+F_{22}}$ *for $i = 4, 5, 6$.*

If $(a + bT)^{E_{23}} = T$ there are no terms that only involve these variables.

Similarly, the terms that only involve the variables x_1, x_5 are

- $\eta_i f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}}$ *for $i = 1, 2, 3$*
- $\eta_i f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}}$ *for $i = 4, 5, 6$*

Analogous formulas hold for the terms involving x_2, x_6 and x_2, x_5, using g_1, g_2 and h_1, h_2 instead of f_1, f_2 respectively.

Proof. We proof the case for x_1, x_5, and the rest are done similarly.

Let's start with the vector $(x_1, x_2, x_3, x_4, x_5, x_6)$ and apply the steps of the encryption map. After the first linear map L_1, we get a vector formed by stacking the three vectors $L_{11}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $L_{12}\begin{pmatrix} x_3 \\ x_4 \end{pmatrix}$ and $L_{13}\begin{pmatrix} x_5 \\ x_6 \end{pmatrix}$. The elements of $\mathbb{F}_{q^2}$ that correspond to these vectors are $x_1l_{11} + x_2l_{12}$, $x_3l_{21} + x_4l_{22}$ and $x_5l_{31} + x_6l_{32}$ respectively.

After applying the exponential maps that corresponds to E, we have the vectors corresponding to

- $(x_1 l_{11} + x_2 l_{12})^{E_{11}} (x_3 l_{21} + x_4 l_{22})^{E_{12}}$
- $(x_1 l_{11} + x_2 l_{12})^{E_{21}} (x_5 l_{31} + x_6 l_{32})^{E_{23}}$
- $(x_3 l_{21} + x_4 l_{22})^{E_{32}} (x_5 l_{31} + x_6 l_{32})^{E_{33}}$

In the expansion of those expressions, all terms involve variables that are not x_1 or x_5 except the in the second one, where there is the term $x_1^{E_{21}} x_5^{E_{23}} {l_{11}}^{E_{21}} {l_{31}}^{E_{23}}$. That is, the vector in $\mathbb{F}_q^6$ that we get at this stage is

$$\begin{pmatrix} \bullet\bullet\bullet \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet + f_1 x_1^{E_{21}} x_5^{E_{23}} \\ \bullet\bullet\bullet + f_2 x_1^{E_{21}} x_5^{E_{23}} \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet \end{pmatrix}$$

where the $\bullet\bullet\bullet$ symbols represent sums of terms that don't involve only the variables x_1 and x_5.

After applying L_2, we get

$$\begin{pmatrix} \bullet\bullet\bullet + f_1 x_1^{E_{21}} x_5^{E_{23}} \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet + f_2 x_1^{E_{21}} x_5^{E_{23}} \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet \end{pmatrix}.$$

Expressed as a vector in $\mathbb{F}_{q^3}^2$, this is

$$\begin{pmatrix} \bullet\bullet\bullet + f_1 x_1^{E_{21}} x_5^{E_{23}} \\ \bullet\bullet\bullet + f_2 x_1^{E_{21}} x_5^{E_{23}} \end{pmatrix},$$

where again, the $\bullet\bullet\bullet$ symbols represent a sum of terms that don't involve only x_1 and x_5, but this time with coefficients in $\mathbb{F}_{q^3}$, but notice that the coefficients that only involve x_1 and x_5 are actually elements of $\mathbb{F}_q$.

Now, applying the exponentiation corresponding to F, we get the vector in $\mathbb{F}_{q^3}^2$

$$\begin{pmatrix} \bullet\bullet\bullet + f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}} \\ \bullet\bullet\bullet + f_1^{F_{21}} f_2^{F_{22}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}} \end{pmatrix},$$

which corresponds to the vector in $\mathbb{F}_q^6$

$$\begin{pmatrix} \bullet\bullet\bullet + f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}} \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet + f_1^{F_{21}} f_2^{F_{22}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}} \\ \bullet\bullet\bullet \\ \bullet\bullet\bullet \end{pmatrix}.$$

Now, applying L_3 we get:

$$\begin{pmatrix} \bullet\bullet\bullet + f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}} \eta_1 \\ \bullet\bullet\bullet + f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}} \eta_2 \\ \bullet\bullet\bullet + f_1^{F_{11}} f_2^{F_{12}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{11}+F_{12}} \eta_3 \\ \bullet\bullet\bullet + f_1^{F_{21}} f_2^{F_{22}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}} \eta_4 \\ \bullet\bullet\bullet + f_1^{F_{21}} f_2^{F_{22}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}} \eta_5 \\ \bullet\bullet\bullet + f_1^{F_{21}} f_2^{F_{22}} (x_1^{E_{21}} x_5^{E_{23}})^{F_{21}+F_{22}} \eta_6 \end{pmatrix}. \quad \square$$

5. Recovering the coefficients of L_1

Now we see how to recover the coefficients of L_1 from the public key.

Assume $c \neq 0$ (otherwise, we can detect the case because there are no terms involving only x_1, x_6 in the public key; we can apply a linear change of variables to fall into this case).

From the previous section, we know the following column vectors

$$\begin{pmatrix} c^{F_{12}}\eta_1 \\ c^{F_{12}}\eta_2 \\ c^{F_{12}}\eta_3 \\ c^{F_{22}}\eta_4 \\ c^{F_{22}}\eta_5 \\ c^{F_{22}}\eta_6 \end{pmatrix}, \begin{pmatrix} f_1^{F_{11}} f_2^{F_{12}}\eta_1 \\ f_1^{F_{11}} f_2^{F_{12}}\eta_2 \\ f_1^{F_{11}} f_2^{F_{12}}\eta_3 \\ f_1^{F_{21}} f_2^{F_{22}}\eta_4 \\ f_1^{F_{21}} f_2^{F_{22}}\eta_5 \\ f_1^{F_{21}} f_2^{F_{22}}\eta_6 \end{pmatrix}, \begin{pmatrix} g_1^{F_{11}} g_2^{F_{12}}\eta_1 \\ g_1^{F_{11}} g_2^{F_{12}}\eta_2 \\ g_1^{F_{11}} g_2^{F_{12}}\eta_3 \\ g_1^{F_{21}} g_2^{F_{22}}\eta_4 \\ g_1^{F_{21}} g_2^{F_{22}}\eta_5 \\ g_1^{F_{21}} g_2^{F_{22}}\eta_6 \end{pmatrix}, \begin{pmatrix} h_1^{F_{11}} h_2^{F_{12}}\eta_1 \\ h_1^{F_{11}} h_2^{F_{12}}\eta_2 \\ h_1^{F_{11}} h_2^{F_{12}}\eta_3 \\ h_1^{F_{21}} h_2^{F_{22}}\eta_4 \\ h_1^{F_{21}} h_2^{F_{22}}\eta_5 \\ h_1^{F_{21}} h_2^{F_{22}}\eta_6 \end{pmatrix}.$$

Taking quotients between them we an eliminate the η_i, and hence we can know the values of $f_1^{F_{11}} \left(\frac{f_2}{c}\right)^{F_{12}}$ and $f_1^{F_{21}} \left(\frac{f_2}{c}\right)^{F_{22}}$.

Since the exponentiation map is invertible, these two values allow us to recover f_1 and $\frac{f_2}{c}$. Analogously, we can also recover g_1, $\frac{g_2}{c}$, h_1 and $\frac{h_2}{c}$.

Let's denote $f_2' := \frac{f_2}{c}$, $g_2' := \frac{g_2}{c}$ and $h_2' := \frac{h_2}{c}$.

Now we have the equations

$$\begin{aligned} f_1 + cf_2'T &= f_1 + f_2T = {l_{11}}^{E_{21}} {l_{31}}^{E_{23}} \\ g_1 + cg_2'T &= g_1 + g_2T = {l_{11}}^{E_{21}} (1 + cT) \\ h_1 + ch_2'T &= h_1 + h_2T = {l_{31}}^{E_{23}} \end{aligned}$$

So $(f_1 + cf_2'T)(1 + cT) = (g_1 + cg_2'T)(h_1 + ch_2'T)$. In this expression the only unknown is c. This is an equation in $\mathbb{F}_{q^2}$ that translates into two quadratic equations in $\mathbb{F}_q$ on c, that must have at least one common nonzero solution. Note that one of them has no constant term, so one of its solution is zero. That is, we can determine c completely.

With the value of c, we also get f_2, g_2 and h_2. So we have ${l_{31}}^{E_{23}} = h_1 + h_2 T$. Raising to the inverse of E_{23} modulo $q^2 - 1$, we recover l_{31}. We can also compute ${l_{11}}^{E_{21}} = \frac{f_1 + f_2 T}{h_1 + h_2 T}$ and hence l_{11}. Moreover, from $1 + cT$ we can recover a, b such that $(a + bT)^{E_{23}} = 1 + cT$, and hence, we have completely recovered the matrices L_{11} and L_{13}.

Since we have c and $c^{F_{12}} \eta_i$, we can also compute η_i.

Summarizing, we have proved the following:

Theorem 1. *Given a valid public key, there exists a corresponding private key of the form:*

$$L_{11} = \begin{pmatrix} * & 1 \\ * & 0 \end{pmatrix}, L_{12} = \begin{pmatrix} ? & 1 \\ ? & 0 \end{pmatrix}, L_{13} = \begin{pmatrix} * & * \\ * & * \end{pmatrix},$$

$$L_{21} = \begin{pmatrix} ? & ? & 1 \\ ? & ? & 0 \\ ? & ? & 0 \end{pmatrix}, L_{22} = \begin{pmatrix} 1 & ? & ? \\ 0 & ? & ? \\ 0 & ? & ? \end{pmatrix}$$

$$L_{31} = \begin{pmatrix} * & ? & ? \\ * & ? & ? \\ * & ? & ? \end{pmatrix}, L_{32} = \begin{pmatrix} * & ? & ? \\ * & ? & ? \\ * & ? & ? \end{pmatrix}$$

where the coefficients marked as $*$ can be efficiently computed from the public key.

Notice that, if we could find the two missing coefficients of L_{12}, we would be able to precompose the map with the inverse of L_1, and then with the inverse of E, leaving us with a map consisting only on a known matrix exponentiation map composed on both sides with two (partially) unknown linear maps.

6. Recovering L_2 and L_3

With the previous steps, we would only need to find two missing coefficients of L_{12} to reduce the problem to attacking a weaker variant of the scheme, with the following structure in the case $3, 2$:

$$\begin{array}{ccccccc} \mathbb{F}_q^6 & \xrightarrow{L_2} & \mathbb{F}_q^6 & & \mathbb{F}_q^6 & \xrightarrow{L_3} & \mathbb{F}_q^6 \\ & & \downarrow \cong & & \uparrow \cong & & \\ & & \mathbb{F}_{q^3}^2 & \xrightarrow{F} & \mathbb{F}_{q^2}^n & & \end{array}$$

In this section, we see how to recover the entries of L_3 (and then, trivially we get L_2 assuming only that we know the total composition map, and the entries of F.

Now, denote by $\zeta_1, \zeta_2, \zeta_3$ the columns of L_{21}, interpreted as elements of $\mathbb{F}_{q^3}$, and by $\zeta_4, \zeta_5, \zeta_6$ the columns of L_{22}. Analogously, the columns of L_{31}^{-1} and L_{32}^{-1} will be denoted as $\vartheta_1, \vartheta_2, \vartheta_3$ and $\vartheta_4, \vartheta_5, \vartheta_6$ respectively. Note that, by the same kind of arguments used in Section 3, we can assume that $\vartheta_3 = \vartheta_6 = 1$.

If we apply L_2 to the vector $(1, 0, 0, 1, 0, 0)$ we get a column vector of the form

$$\begin{pmatrix} \zeta_1 \\ \zeta 4 \end{pmatrix}$$

where ζ_1 and ζ_4 are considered now as a vector with three coordinates.

Its image by F is

$$\begin{pmatrix} \zeta_1^{F_{11}} \zeta_4^{F_{12}} \\ \zeta_1^{F_{21}} \zeta 4^{F_{22}} \end{pmatrix}$$

And the final application of L_3 gives a vector $(z_1^{14}, \ldots, z_6^{14})$, that is known (since it is just the result of the full map to the starting vector). Applying the inverse of L_3, we get that

$$\begin{aligned} \zeta_1^{F_{11}} \zeta_4^{F_{12}} &= z_1^{14} \vartheta_1 + z_2^{14} \vartheta_2 + z_3^{14} \\ \zeta_1^{F_{21}} \zeta_4^{F_{22}} &= z_4^{14} \vartheta_4 + z_5^{14} \vartheta_5 + z_6^{14} \end{aligned}$$

Analogously, if we start with the vectors $(1, 0, 0, 0, 1, 0)$, $(1, 0, 0, 0, 0, 1)$, $(0, 1, 0, 1, 0, 0)$, $(0, 1, 0, 0, 1, 0)$, $(0, 0, 1, 1, 0, 0)$, $(0, 0, 1, 0, 1, 0)$ and $(0, 0, 1, 0, 0, 1)$ and apply the same reasoning, we get the equations:

$$\begin{aligned} \zeta_1^{F_{11}} \zeta_5^{F_{12}} &= z_1^{15} \vartheta_1 + z_2^{15} \vartheta_2 + z_3^{15} \\ \zeta_1^{F_{21}} \zeta_5^{F_{22}} &= z_4^{15} \vartheta_4 + z_5^{15} \vartheta_5 + z_6^{15} \\ \zeta_1^{F_{11}} \zeta_6^{F_{12}} &= z_1^{16} \vartheta_1 + z_2^{16} \vartheta_2 + z_3^{16} \\ \zeta_1^{F_{21}} \zeta_6^{F_{22}} &= z_4^{16} \vartheta_4 + z_5^{16} \vartheta_5 + z_6^{16} \\ \zeta_2^{F_{11}} \zeta_4^{F_{12}} &= z_1^{24} \vartheta_1 + z_2^{24} \vartheta_2 + z_3^{24} \\ \zeta_2^{F_{21}} \zeta_4^{F_{22}} &= z_4^{24} \vartheta_4 + z_5^{24} \vartheta_5 + z_6^{24} \\ \zeta_2^{F_{11}} \zeta_5^{F_{12}} &= z_1^{25} \vartheta_1 + z_2^{25} \vartheta_2 + z_3^{25} \\ \zeta_2^{F_{21}} \zeta_5^{F_{22}} &= z_4^{25} \vartheta_4 + z_5^{25} \vartheta_5 + z_6^{25} \\ \zeta_2^{F_{11}} \zeta_6^{F_{12}} &= z_1^{26} \vartheta_1 + z_2^{26} \vartheta_2 + z_3^{26} \\ \zeta_2^{F_{21}} \zeta_6^{F_{22}} &= z_4^{26} \vartheta_4 + z_5^{26} \vartheta_5 + z_6^{26} \\ \zeta_3^{F_{11}} \zeta_4^{F_{12}} &= z_1^{34} \vartheta_1 + z_2^{34} \vartheta_2 + z_3^{34} \\ \zeta_3^{F_{21}} \zeta_4^{F_{22}} &= z_4^{34} \vartheta_4 + z_5^{34} \vartheta_5 + z_6^{34} \\ \zeta_3^{F_{11}} \zeta_5^{F_{12}} &= z_1^{35} \vartheta_1 + z_2^{35} \vartheta_2 + z_3^{35} \\ \zeta_3^{F_{21}} \zeta_5^{F_{22}} &= z_4^{35} \vartheta_4 + z_5^{35} \vartheta_5 + z_6^{35} \\ \zeta_3^{F_{11}} \zeta_6^{F_{12}} &= z_1^{36} \vartheta_1 + z_2^{36} \vartheta_2 + z_3^{36} \\ \zeta_3^{F_{21}} \zeta_6^{F_{22}} &= z_4^{36} \vartheta_4 + z_5^{36} \vartheta_5 + z_6^{36} \end{aligned}$$

where the $z_k^{(ij)}$ are known values of $\mathbb{F}_q$, and the ζ_i and ϑ_j are unknown elements of $\mathbb{F}_{q^3}$. The same system of equations could be obtained by following track of the coefficients in the polynomial expression, instead of evaluating in particular values (both results would be equivalent).

What we need to do now is to solve this system of equations, for which we know that some solution exists. Moreover, we know that $(\zeta_1, \zeta_2, \zeta_3)$ are $\mathbb{F}_q$-lineally independent, and so are $(\zeta_4, \zeta_5, \zeta_6)$, $(\vartheta_1, \vartheta_2, \vartheta_3)$ and $(\vartheta_4, \vartheta_5, \vartheta_6)$. In particular, none of those elements is zero.

Doing some basic elimination of the ζ_i variables, we get some simpler subsystems of equations, for example,

$$\begin{aligned}
&(z_1^{14}\vartheta_1 + z_2^{14}\vartheta_2 + z_3^{14})(z_1^{25}\vartheta_1 + z_2^{25}\vartheta_2 + z_3^{25}) \\
&\quad = (z_1^{15}\vartheta_1 + z_2^{15}\vartheta_2 + z_3^{15})(z_1^{24}\vartheta_1 + z_2^{24}\vartheta_2 + z_3^{24}) \\
&(z_1^{14}\vartheta_1 + z_2^{14}\vartheta_2 + z_3^{14})(z_1^{26}\vartheta_1 + z_2^{26}\vartheta_2 + z_3^{26}) \\
&\quad = (z_1^{16}\vartheta_1 + z_2^{16}\vartheta_2 + z_3^{16})(z_1^{24}\vartheta_1 + z_2^{24}\vartheta_2 + z_3^{24})
\end{aligned}$$

which is a system of two quadratic equations in the variables ϑ_1, ϑ_2. It can be easily solved by taking a resultant (which is a degree 4 polynomial in just one variable) and then factoring it over $\mathbb{F}_{q^3}$. We will get at least one solution (since we know that one solution must exist) and at most four possible ones.

Note that there are more possible systems of two quadratic equations on the same variables, so the whole system is overdetermined. We can use that to discard some of the four possible solutions.

Analogously, we can solve for ϑ_4, ϑ_5. Then, solving for $\zeta_1, \ldots \zeta_6$ can be done just by applying the inverse of F.

Once we get all the values ϑ_i and ζ_j, we have effectively recovered the private key.

7. Conclusion

We have presented a structural attack to the DME cryptosystem with parameters $(3, 2, q)$, that is able to recover the full private key from the public key and two extra elements of $\mathbb{F}_q$ that depend on the private key. An exhaustive search gives an upper bound of q^2 to the security level. In particular, for the DME $(3, 2, 2^{48})$ version submitted to the NIST, this bound gives at most 96 bits of security, far less than the required 256 bits.

The attack only uses a very small fraction of the information contained in the public key. So we suspect that a deeper analysis could provide a better method than the exhaustive search for the full recovery of the private key.

Further research would be needed to determine if other choices of parameters are vulnerable to similar attacks.

References

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions. (Accessed 25 February 2020).
[2] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/DME-official-comment.pdf. (Accessed 25 February 2020).
[3] https://groups.google.com/a/list.nist.gov/forum/#!searchin/pqc-forum/dme|sort:date/pqc-forum/pR-O1CjHBtY/dkPKlJWrBwAJ. (Accessed 25 February 2020).
[4] https://docs.google.com/viewer?a=v&pid=forums&srcid=MDMyODM2NjQwOTk0MTgyNTI4NzgBMTI1OTE5ODU2NjgwODA3MTI1MzQBZGtQS2xKV3JCd0FKATAuMgFsaXN0Lm5pc3QuZ292AXYy&authuser=0. (Accessed 25 February 2020).