DME: MULTIVARIATE SIGNATURE PUBLIC KEY SCHEME

IGNACIO LUENGO, MARTÍN AVENDAÑO

Departamento de Álgebra, Geometría y Topología, Facultad de Matemáticas, Universidad Complutense de Madrid. Plaza de Ciencias 3, 28040 Madrid, Spain.

1. Introduction

This document present the digital signature version the multivariate public key cryptosystem DME based on the composition of linear and exponential maps that produces a public key of very high degree. The main reference for the description of DME is ([4]), the core of the scheme is deterministic trapdoor permutation and allows to use as random padding OAEP for KEM and PSS00 for signature. In this paper the signature scheme DME-SIGN correspond to the DME-PSS00 of ([4]).

The main components of the DME are exponential maps $E_A : K^n \to K^n$ associated to matrices $A = (a_{ij}) \in \mathcal{M}_{n\times n}(\mathbb{Z})$, where K is a finite field given by the following formula:

$$E_A(x_1, \dots, x_n) = (x_1^{a_{11}} \cdot \dots \cdot x_n^{a_{1n}}, \dots, x_1^{a_{n1}} \cdot \dots \cdot x_n^{a_{nn}}). \tag{1}$$

The following two facts are extremely useful and also easy to verify:

a) If $A, B \in \mathcal{M}_{n\times n}(\mathbb{Z})$ and $C = B \cdot A$, then $F_C = F_B \circ F_A$.
b) If $\det(A) = \pm 1$, then the inverse matrix A^{-1} has integer entries, F_A is invertible on $(K \setminus \{0\})^n$, and its inverse is given by $F_{A^{-1}}$.

The of monomial maps that E_A are extensively used in Algebraic Geometry and produce birrational maps. In [2] these transformations are used to produce a multivariate public key cryptosystem. If $\det(A) \neq \pm 1$, the monomial map is not birrational and

Let $q = p^e$ be a prime power and $\mathbb{F}_q$ denote a finite field of q elements. It is not necessary to consider exponents greater than $q-2$ since $x^{q-1} = 1$ for all $x \in \mathbb{F}_q \setminus \{0\}$. We take $A \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q-1})$ and then we have:

Proposition 1.1. *Let $A \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q-1})$ and $G_A : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the corresponding monomial map. If $\gcd(\det(A), q-1) = 1$, and we set $b := \det(A)^{-1} \in \mathbb{Z}_{q-1}$ and $B := b\mathrm{Adj}(A)$, then $A^{-1} = B \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q-1})$ and $F_A : (\mathbb{F}_q \setminus \{0\})^n \to (\mathbb{F}_q \setminus \{0\})^n$ is bijective with inverse $F_{A^{-1}}$.*

For the proof see (([4]) thm1.2)

The exponential maps F_A can be used to build a quadratic multivariate PKC in the standard way by putting powers of q in the non-zero entries of the matrix A and 2 non zero entries $q^{a_{ij}}$ and 2 non zero in each row od A one gets a quadratic public key, if we allow 3 non zero entries, we get cubic polynomials, and so on. We made extensive computer tests leading to the conclusion that those systems are not safe against Gröbner basis attack for reasonable key size.

In order to make an scheme stronger against algebraic cryptanalysis we take $q = 2^e$ and allow the non-zero entries of A to be powers of 2 that are not powers of q. This choice produces final polynomials with degree up to $q-1$ in each variable. The kernel of the DME is a composition of r exponentials with n variables and $n+1$ linear maps, that we denote by DME-$(r, n, 2^e)$. We can get very efficient and safe DME-$(r, n, 2^e)$ schemes with $n = 6, 8$ and $3 \le r \le 6$. FIn order to simplify the notation, we take $r = 4$ and $n = 8$ in the following description of the DME.

2. Mathematical description of DME-$(4, 8, 2^e)$

The DME-$(4, 8, 2^e)$ cryptosystem works with plain texts and cypher texts in $\mathbb{F}_q^8$ with $q = 2^e$. Let $u^2 + au + b \in \mathbb{F}_q[u]$ be an irreducible polynomial, consider the field extension $\mathbb{F}_{q^2} = \mathbb{F}_q[u]/\langle u^2 + au + b\rangle$ of degree two over $\mathbb{F}_q$. Let $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ be the bijection defined by $(x, y) \mapsto x + y\bar{u}$ and let $\bar{\phi} : \mathbb{F}_q^8 \to (\mathbb{F}_{q^2})^4$ be the map $(x_1, \dots, x_8) \mapsto (\phi(x_1, x_2), \phi(x_3, x_4), \phi(x_5, x_6), \phi(x_7, x_8))$.**The values of e, a, b are fixed during the setup of the system.**

The DME-$(4, 8, 2^e)$ cryptosystem combines 5 linear+affine maps $L_0, \dots, L_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ with 4 exponential maps $E_1, \dots, E_4 : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$. More precisely, the encryption map

$$F = \Psi(L_0, \dots, L_r, E_1, \dots, E_r) : \mathbb{F}_q^8 \to \mathbb{F}_q^8$$

E-mail address: iluengo@ucm.es, mavend01@ucm.es.

is given by the composition

$$\begin{array}{l}
\mathbb{F}_q^8 \xrightarrow{L_0} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{E_1} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}} \\
\mathbb{F}_q^8 \xrightarrow{L_1} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{E_2} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}} \\
\mathbb{F}_q^8 \xrightarrow{L_2} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{E_3} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}} \\
\mathbb{F}_q^8 \xrightarrow{L_3} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{E_4} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}} \\
\mathbb{F}_q^8 \xrightarrow{L_4} \mathbb{F}_q^8
\end{array}$$

of the linear+affine and exponential maps interleaved with the bijections $\bar{\phi}$ and $\bar{\phi}^{-1}$.

Each linear+affine map L_i is made of four linear maps $L_{i1}, \ldots, L_{i4} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ and four translation vectors $a_{i1}, \ldots, a_{i4} \in \mathbb{F}_q^2$, so that

$$L_i(x_1, \ldots, x_8) = (L_{i1}(x_1, x_2) + a_{i1}, L_{i2}(x_3, x_4) + a_{i2}, L_{i3}(x_5, x_6) + a_{i3}, L_{i4}(x_7, x_8) + a_{i4}).$$

The matrices of the blocks $L_{i1}, \ldots, L_{i4}$ are $A_{i1}, \ldots, A_{i4} \in \mathbb{F}_q^{2\times 2}$, respectively.

An important setting for the security of DME is the number of steps with translation vectors. In [] Thm 5.2 we proof that there is not failure of decryption if we use translations only in one intermediate step with non zero $1 \le i_0 < 4$ and set $a_{ij} = 0$ for all $i \neq i_0$. We also proof in the same place that we will have failure of decryption if there are translations at more than one step

Setting: We set non zero translations the last 3 linear maps L_i, this setting will produce failure of decryption, but for signature use ** and that gives not signing or verifying errors.

The exponential maps $F_{E_i} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ are defined by he matrices 4×4 E_i with coefficients in $[0, q^2 - 1]$. It is not necessary to consider exponents greater than $q^2 - 1$ since $x^{q^2} = x$ for all $x \in \mathbb{F}_{q^2}$.

The linear+affine maps $L_i : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ are invertible if and only if each of the 2×2 blocks $L_{i1}, L_{i2}, L_{i3}, L_{i4}$ have non-zero determinant. In this case, the inverse of L_i is

$$L_i^{-1}(x_1, \ldots, x_8) = (L_{i1}^{-1}(x_1, x_2) - L_{i1}^{-1} a_{i1}, \ldots, L_{i4}^{-1}(x_7, x_8) - L_{i4}^{-1} a_{i4}),$$

i.e. L_i^{-1} is also a linear+affine map.

The exponential maps $E_i : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ are not invertible in general. However, their restrictions to the torus $\widehat{E}_i : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ are invertible if and only if

$$\gcd(\det(E_i), q^2 - 1) = 1.$$

The inverse of $\widehat{E}_i$ is also an exponential map $\widehat{E}_i^{-1} : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$, given by the inverse of the matrix E_i modulo $q^2 - 1$. This matrix has coefficients in $[0, q^2 - 2]$. Using the same matrix, we extend $\widehat{E}_i^{-1}$ to an exponential map $E_i^{-1} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$.

The private key consists of the coefficients of the linear+affine maps $L_0, \ldots, L_4$ and exponential maps $E_1, \ldots, E_4$, nevertheless the security of DME is based on the difficulty to find the linear maps $L_0, \ldots, L_4$ and the exponential can be made partially or totally public. The public key data are enough to apply all those maps in reverse, that is, to being able to decrypt or to signing.

The public key is the polynomial representation of the composition of the maps,

$$F(x_1, \ldots, x_8) = (F_{4,1}, F_{4,2}, F_{4,3}, F_{4,4}, F_{4,5}, F_{4,6}, F_{4,7}, F_{4,8})$$

.

3. Computation of the public key F

If $\underline{x} = (x_1, \ldots, x_8) \in \mathbb{F}_q^8$ are the initial coordinates, then the composition of all the maps allow us to compute the components of $F(\underline{x})$ as polynomials $F_{4,j} \in \mathbb{F}_q[x_1, \ldots, x_8]$. In order to keep the number of monomials small, we choose the matrices E_i with the following properties:

(1) The entries of E_i are powers of 2.
(2) Each row of E_i has one or two non zero entries.
(3) If $\det(E_i)$ is not a power of 2 we choose the entries of E_i such a way that $d_i = \frac{1}{\det(E_i)} \mod q^2 - 1$ has a fixed small binary weight.

The computation of $d_i = \frac{1}{\det(E_i)} \mod q^2 - 1$ is the most time consuming task of the inverse $F^{-1}(\underline{x})$ the condition (3) is essential to get speed up the signing procedure. The inverse map F^{-1} is also composition of 4 exponentials so if the number of monomials of F^{-1} is not very big, one can get the polynomial components of F^{-1} by interpolation, provided enough number of pairs $(\underline{x}, F(\underline{x}))$. To avoid this attack we take such that the last inverse d_4 has binary weight to ensure that the inverse E_i^{-4} has entries with big binary weight that will produce a big number of monomial of the inverse F^{-1} above a given security level for instance $q^2 = 2^{2e}$.

It is possible to get the monomials of the F_i without computing the composition of all the maps. It is easy to verify that after exponential E_i plus $\bar{\phi}^{-1}$ the 8 resulting polynomials

$$F_{i,1}, F_{i,2}, F_{i,3}, F_{i,4}, F_{i,5}, F_{i,6}, F_{i,7}, F_{i,8}$$

verify that $F_{i,2k-1}$, $F_{i,2k}$ and $F_{i,2k-1} + \bar{u}.F_{i,2k}$ share the same monomials M_{ik} unless some coefficient vanish and also the same happens after we apply L_i.

Let $M = [m_1, \dots m_s]$ a list of monomials and α a power of 2, we define $M^\alpha = [m_1^\alpha, \dots, m_s^\alpha]$. If $M = [m_1, \dots, m_s]$ and $N = [n_1, \dots, n_t]$ are lists of monomials, we define

$$M^\alpha \otimes N^\beta = [m_i^\alpha \otimes n_j^\beta, 1 \le i \le s, 1 \le j \le t],$$

that is, $M^\alpha \otimes N^\beta$ is the Kronecker tensor product of M^α and N^β as row matrices.

It is easy to verify that $M_{ij}^\alpha \otimes M_{ik}^\beta$ is the list of monomials of the polynomial

$$(F_{i,2j-1} + \bar{u}.F_{i,2j})^\alpha \cdot (F_{i,2k-1} + \bar{u}.F_{i,2k})^\beta$$

since the exponents α and β are powers of 2.

—bf Notation: We use the following convention for the entries of each matrix E_i, we call $\alpha_{i,2k-1}$ the first non zero entry of the row k and $\alpha_{i,2k}$ the second non zero entry. If there is only one non zero entry, we just set $\alpha_{i,2k} = 0$.

We reduce the list of monomials when some of them are repeated. Let us define an operation $Rm(M)$ on a list of monomials M that removes all duplicates, keeping only the first appearance of each monomial in the list and erasing the rest. The following algorithm, called MON, shows how to compute the lists of monomials of the F_{rj}.

Algorithm 3.1 MON, compute the monomials in the public-key polynomials.

Input: $(E_1, \dots, E_r)$
Output: $(M_{r1}, M_{r2}, M_{r3}, M_{r4})$

```
M_01 ← [x_1, x_2], M_02 ← [x_3, x_4], M_03 ← [x_5, x_6], M_04 ← [x_7, x_8]
C_01 ← A_01, ..., C_04 ← A_04
for i = 0 to r − 1 do
   for k = 1 to 4 do
      M_(i+1)k = M_ik1^(α_i,2k−1) ⊗ M_ik2^(α_i,2k), where M_ik2 = [1] if α_i,2k = 0
      M_(i+1)k = Rm(M_(i+1)k)
      if a_(i+1)k ≠ 0 then
         append 1 to the list M_(i+1)k
      end if
   end for
end for
```

The size of the lists M_{ri} can be up to double exponential on the number of rounds r for instance if all the rows of the E_i have two non zero entries then $card(M_{ri}) = 2^{2^r}$. We can reduce the size of the list of monomials by imposing some linear condition on the exponents $e_{i,j}$ of $\alpha_{i,j}$ ($\alpha_{i,j} = 2^{e_{i,j}}$), in such a way that some of the monomials become equal and the coefficient of the repeated monomial is a sum of several terms, which will give us some defense against the structural cryptanalysis because we need to take care of the following fact:

The final polynomials are obtained by computing

$$(F_{r-1,2j-1} + \bar{u}.F_{r-1,2j})^\alpha \cdot (F_{r-1,2k-1} + \bar{u}.F_{r-1,2k})^\beta$$

after the last exponential.

Let $(F_{r-1,2j-1} + \bar{u}.F_{r-1,2j})^\alpha = \sum B_i m_i$ and $F_{r-1,2k-1} + \bar{u}.F_{r-1,2k})^\beta = \sum C_j n_j$ where $B_i, C_k \in \mathbb{F}q^2$ and m_i, n_j are monomial in $\underline{x}$. Then,

$$(F_{(r-1)k_1}^{\alpha_{i,2k-1}} \cdot F_{(r-1)k_2}^{\alpha_{i,2k}} = \left(\sum B_i m_i\right) \cdot \left(\sum C_j n_j\right) = \sum B_i C_j m_i n_j = \sum H_{ij} m_i n_j.$$

Thus, we have $H_{ij} = B_i C_j$, and it is clear now that the coefficients $H_{ij} \in \mathbb{F}_{q^2}$ satisfy $H_{ij} H_{kl} = H_{il} H_{kj}$, which will be called quadratic relations (QR) from now on. Since the coefficients of final polynomials $F_1, \dots F_8$ are obtained applying $\bar{\phi}^{-1}$ and L_r, we can use the QR to compute equations for the coefficients of the components of inverse of L_r^{-1}. Given that the QR are homogeneous (of degree two), one can solve those equations to find L_r^{-1} and L_r up to a constant.

In order to eliminate the QR among the H_{ij}, the strategy is to force many coincidences among the final monomials, that is, if H_{ij} is a sum $= \sum B_k C_l$ it will by more difficult to get the quadratic relations or any polynomial relations among the H_{ij}. The implicit equations on the H_{ij} are obtained by computing the equations of the image of the map $Q = (Q_{ij})$, defined by $H_{ij} = Q_{ij}(B,C) = \sum B_k C_l$, that is by eliminating the B_1 and C_j from the system $\langle H_{ij} - \sum B_k C_l \rangle$

$$Q : \mathbb{F}_{q^2}[B_k, C_l] \longrightarrow \mathbb{F}_{q^2}[H_{ij}]$$

For instance, for the second component of example 1 there are no QR, the source has 24 variables and the target 48.

Assume that we are at the step i of the algorithm MON and we are computing the list $M_{(i+1)k}$. We can force a reduction of the monomials only if there are two non zero entries $2^{e_{i,2k-1}}$ and $2^{e_{i,2k}}$ in the corresponding row of the matrix E_i, so we'll have to compute $M_{(i+1)k} = M_{ik_1}^{\alpha_{i,2k-1}} \otimes M_{ik_2}^{\alpha_{i,2k}}$. Now, we take a variable that is in both lists with exponent a power of 2, which for simplicity we'll assume it is x_1. More precisely, the monomial $x_1^{2^{l_1}} \cdot m_1$, where $l_1 = l_1(e_{j,l} : 1 \le j \le i-1)$ is a linear form and m_1 is a monomial in the other variables would appear in M_{ik_1}, and $x_1^{2^{l_2}} \cdot m_2$ in the list M_{ik_2}. By the method that the lists are constructed (x_1 and x_2 play exactly the same role), we would also have the monomials $x_2^{2^{l_1}} \cdot m_1$ and $x_2^{2^{l_2}} \cdot m_2$ in the lists M_{ik_1} and M_{ik_2}, respectively.

Now, when we compute $M_{ik_1}^{\alpha_{i,2k-1}}$, the exponent of x_1 in the first monomial is $2^{l_1+e_{i,2k-1}}$ and in the other list is $2^{l_2+e_{i,2k}}$. We can force that $2^{l_1+e_{i,2k-1}} = 2^{l_2+e_{i,2k}}$ if we substitute $e_{i,2k}$ by $e_{i,2k-1}+l_1-l_2$ and then the monomials in both lists became

$$x_1^{2^{l_1+e_{i,2k-1}}} \cdot m_1^{2^{e_{i,2k-1}}}, \; x_2^{2^{l_1+e_{i,2k-1}}} \cdot m_1^{2^{e_{i,2k-1}}}$$

in the first list, and

$$x_1^{2^{l_1+e_{i,2k-1}}} \cdot m_2^{2^{e_{i,2k-1}+l_1-l_2}}, \; x_2^{2^{l_1+e_{i,2k-1}}} \cdot m_2^{2^{e_{i,2k-1}+l_1-l_2}}$$

in the second.

When the tensor product of both lists is computed, we get that two of the four monomials are equal:

$$x_1^{2^{l_1+e_{i,j2k-1}}} \cdot m_1^{2^{e_{i,j2k-1}}} \cdot x_2^{2^{e_{i,j2k-1}+l_1-l_2}} \cdot m_2^{2^{e_{i,j2k-1}+l_1-l_2}}$$
$$= x_2^{2^{l_1+e_{i,j2k-1}}} \cdot m_1^{2^{e_{i,2k-1j}}} \cdot x_1^{2^{l_1+e_{i,j2k-1}}} \cdot m_2^{2^{e_{i,j2k-1}+l_1-l_2}}.$$

If there are other variables repeated in both lists that have different exponents after the change $e_{i,2k} = e_{i,2k-1}+l_1-l_2$, we can repeat the same procedure of imposing a linear condition, but in this case the linear equations involves terms e_{jk} with $j \le i-1$. In general, each linear condition will produce the reduction of many monomials, but the actual number depends of the structure of the matrices E_i and it is not possible to give a general formula for the final number of monomials of F. we call this algorithm RED , the input is the set $\{E_i\}$. Next, we present an example of the procedure.

Example 1: For this example, we take $q = 2^e$, $n = 6$ and following matrices over $\mathbb{Z}_{q^2-1}$:

$$E_1 = \begin{pmatrix} \alpha_{1,1} & 0 & \alpha_{1,2} \\ \alpha_{1,3} & \alpha_{1,4} & 0 \\ 0 & 0 & \alpha_{1,5} \end{pmatrix}, \quad E_2 = \begin{pmatrix} \alpha_{2,1} & \alpha_{2,2} & 0 \\ 0 & \alpha_{2,3} & \alpha_{2,4} \\ \alpha_{2,5} & 0 & \alpha_{2,6} \end{pmatrix}, \quad E_3 = \begin{pmatrix} \alpha_{3,1} & 0 & \alpha_{3,2} \\ \alpha_{3,3} & \alpha_{3,4} & 0 \\ 0 & \alpha_{3,5} & \alpha_{3,6} \end{pmatrix}.$$

As usual, $\alpha_{i,j} = 2^{e_{i,j}}$ and $e_{i,j} \le e-1$. If the $e_{i,j}$ are generic, the lists of monomials after the first exponential (M_{11}, M_{12}, M_{13}) have size $(2^2, 2^2, 2)$, after the second exponential the lists (M_{21}, M_{22}, M_{23}) have size $(2^4, 2^3, 2^3)$, and after the third one the final lists (M_{31}, M_{32}, M_{33}) have size $(2^7, 2^7, 2^6)$. We can apply the method in this section and find 7 independent linear conditions on the $e_{i,j}$ as follows: after E_1, the lists (M_{11}, M_{12}, M_{13}) have size $(2^2, 2^2, 2)$, after E_2, we observe that the list M_{21} comes from tensoring M_{11} and M_{13}, which have x_1 and x_6 in common, so the linear condition $e_{2,2} = e_{1,1} + e_{2,1} - e_{1,3}$ reduces the number of monomials to 12. For M_{21} there are no common variables and for M_{23} we get the condition $e_{2,4} = -e_{2,5} + e_{2,6} - e_{1,1} + e_{1,3} + e_{2,3}$, that gives $(12, 2^3, 6)$ monomials. Finally, after E_3, the lists have size $(72, 96, 48)$. For the list M_{31} we get the condition $e_{3,2} = e_{3,1} + e_{2,1} - e_{2,5}$ that reduces the size of M_{31} to 32. For the list M_{32} we get the condition $e_{3,4} = e_{3,3} + e_{1,1} + e_{2,1} - e_{1,3} + e_{2,3}$ that reduces the size of M_{32} to 36. There is another independent linear equation $-e_{1,2} + e_{1,5} - e_{1,3} - e_{2,3} + e_{2,4}$ that reduce the size of M_{32} to 36. For the list M_{33} we get the condition $e_{3,6} = e_{3,5} - e_{1,1} + e_{1,3} - e_{2,5} + e_{2,3}$ that reduce the size of M_{33} to 24.

By making the above linear changes in the exponents of the E_i, new matrices E_i' and lists that have $(32, 36, 24)$ monomials appear, where one can verify that there are no quadratic relations among the coefficients H_{ij}. using a CAS system one can compute binomial relations of the type $\prod(H_{ij}) - \prod(H_{kl})$ up to some degree. In this example we check with Maple that there are no binomial relations up to degree 10 .

By checking the final lists of monomials, we can observe and interesting structure:
if we make the changes of variables in S_1, S_2 and S_3:

$$S_1 = \begin{bmatrix} x_1^{2^{e_{1,1}+e_{1,1}+e_{2,1}}} = y_{11}, x_2^{2^{e_{1,1}+e_{1,1}+e_{2,1}}} = y_{12}, x_3^{2^{e_{1,4}+e_{1,1}+e_{2,1}-e_{1,3}+e_{3,1}}} = y_{13}, \\ x_4^{2^{e_{1,4}+e_{1,1}+e_{2,1}-e_{1,3}+e_{3,1}}} = y_{14}, x_5^{2^{e_{1,2}+e_{2,1}+e_{3,1}}} = y_{15}, x_6^{2^{e_{1,2}+e_{2,1}+e_{3,1}}} = y_{16} \end{bmatrix}$$

$$S_2 = \begin{bmatrix} x_1^{2^{e_{1,1}+e_{2,1}+e_{3,3}}} = y_{21}, x_2^{2^{{}^{e}e_{1,1}+e_{2,1}+e_{3,3}}} = y_{22}, x_3^{2^{e_{1,4}+e_{1,1}+e_{2,1}-e_{1,3}+e_{3,3}}} = y_{23}, \\ x_4^{2^{e_{1,4}+e_{1,1}+e_{2,1}-e_{1,3}+e_{3,3}}} = y_{24}, x_5^{2^{e_{1,2}+e_{2,1}+e_{3,3}}} = y_{24}, x_6^{2^{e_{1,2}+e_{2,1}+e_{3,3}}} = y_{26} \end{bmatrix}$$

$$S_3 = \begin{bmatrix} x_1^{2^{e_{1,3}+e_{2,3}+e_{3,5}}} = y_{31}, x_2^{2^{e_{1,3}+e_{2,3}+e_{3,5}}} = y_{32}, x_3^{2^{e_{1,4}+e_{2,3}+e_{3,5}}} = y_{33}, \\ x_4^{2^{e_{1,4}+e_{2,3}+e_{3,5}}} = y_{34}, x_5^{2^{e_{1,2}-e_{1,1}+e_{1,3}+e_{2,3}+e_{3,5}}} = y_{35}, x_6^{2^{e_{1,2}-e_{1,1}+e_{1,3}+e_{2,3}+e_{3,5}}} = y_{36} \end{bmatrix}$$

we get polynomials $\overline{F_i} = F_i(y) \in \mathbb{F}_q[y_{11}, \dots y_{36}]$ of low degree 6 or 7. Therefore, using S_1, S_2, S_3 and $\overline{F_i}(y)$ instead of $F_i(x)$ as public key will make faster encryption for DME-KEM and faster signature verification for DME-SIGN.

4. Computing the coefficients of the public key F

Once the list of monomials of the $F_{r,j}$ is obtained, one gets the coefficient of each group of polynomials by evaluating the polynomials $F_{r,1}, ..., F_{r,8}$. The set of pairs $(\underline{c}, F_{r,j}(\underline{c}))$ should be big enough to guarantee that the corresponding linear equations are independent. That is, if $Q_k = [q_1...q_d]$ and $F_{r,j} = \sum_{i=1}^{d} f_{rji} q_i(x)$, we take vectors $\underline{c}_1, \dots, \underline{c}_R$ such that the linear equations on the coefficients f_{rij} in $F_k(c_e) = \sum f_{rji} q_i(c_e)$ are independent and can be solved to get the coefficients of the polynomials $F_{r,1}, \dots, F_{r,8}$.

To compute the polynomials $F_{r,k}$ faster we can use the same idea used to compute the lists of monomials of the polynomial $(F_{i,2j-1} + \bar{u}F_{i,2j})^\alpha (F_{i,2k-1} + \bar{u}F_{i,2k})^\beta$, i.e. $M_{ij}^\alpha \otimes M_{ik}^\beta$. Let s_{ij} be the size of the list M_{ij}. Now, regard M_{ij} as a $1 \times s_{ij}$ matrix, which by abuse of notation, we will still write it as M_{ij}. We denote by C_{ij} the $s_{ij} \times 2$ matrix of the coefficients of the polynomials $F_{i,2j-1}$ and $F_{i,2j}$ on the monomials of M_{ij}, as shown in the following formula:

$$C_{ij} = \begin{bmatrix} c_{11}^{ij} & c_{12}^{ij} \\ c_{21}^{ij} & c_{22}^{ij} \\ \vdots & \vdots \\ c_{s_{ij}1}^{ij} & c_{s_{ij}2}^{ij} \end{bmatrix}$$

Now we have that $F_{i,2j-1} + \bar{u}F_{i,2j} = M_{ij} \cdot C_{ij} \cdot (1, \bar{u})^t$.

If $\alpha = 2^b$, then $(F_{i,2j-1} + \bar{u}F_{i,2j})^\alpha = M_{ij}^\alpha \cdot C_{ij}^\alpha \cdot (1, \bar{u}^\alpha)^t$.

Applying the mixed-product property of the Kronecker product we get:

$$\begin{aligned} &(F_{i,2j-1} + \bar{u}F_{i,2j})^\alpha \cdot (F_{i,2k-1} + \bar{u}F_{i,2k})^\beta \\ &\qquad = (M_{ij}^\alpha \cdot C_{ij}^\alpha \cdot (1, \bar{u}^\alpha)^t) \otimes (M_{ik}^\beta \cdot C_{ik}^\beta \cdot (1, \bar{u}^\beta)^t) \\ &\qquad = (M_{ij}^\alpha \otimes M_{ik}^\beta) \cdot (C_{ij}^\alpha \otimes C_{ik}^\beta) \cdot (1, \bar{u}^\beta, \bar{u}^\alpha, \bar{u}^{\alpha+\beta})^t \end{aligned}$$

Let's call $U_{\alpha\beta}$ the 4×2 matrix defined by

$$(1, \bar{u}^\beta, \bar{u}^\alpha, \bar{u}^{\alpha+\beta})^t = U_{\alpha\beta} \cdot (1, \bar{u})^t.$$

Then, we have the following result:

Lemma 4.1. *The matrix of coefficients of $(F_{i,2j-1} + \bar{u}F_{i,2j})^\alpha \cdot (F_{i,2k-1} + \bar{u}F_{i,2k})^\beta$ with respect of the monomials $M_{ij}^\alpha \otimes M_{ik}^\beta$ is $(C_{ij}^\alpha \otimes C_{ik}^\beta) \cdot U_{\alpha\beta}$*

Now, we can compute the coefficients of the $F_{r,j}$ with algorithms similar to Rm and MON. Given the matrices of coefficients (M, C) of a component we define Rc(C) the matrix coefficient obtained by adding of the coefficient of a the same monomial in the case that is repeated in the monomial list M.

Algorithm 4.1 COE, compute the coefficients of the public-key polynomials.

Input: $(E_1, \dots, E_r, L_0 \dots L_r)$
Output: $(C_{r1}, C_{r2}, C_{r3}, C_{r4})$
$M_{01} \leftarrow [x_1, x_2]$, $M_{02} \leftarrow [x_3, x_4]$, $M_{03} \leftarrow [x_5, x_6]$, $M_{04} \leftarrow [x_7, x_8]$
$C_{01} \leftarrow A_{01}, \dots, C_{04} \leftarrow A_{04}$
for $i = 0$ **to** $r - 1$ **do**
  for $k = 1$ **to** 4 **do**
    if $\alpha_{i,2k} \neq 0$ **then**
      $C_{(i+1)k} = \left(C_{ik_1}^{\alpha_{i,2k-1}} \otimes C_{ik_2}^{\alpha_{i,2k}}\right) \cdot U_{\alpha_{i,2k-1},\alpha_{i,2k}}$
    else
      $C_{(i+1)k} = C_{ik_1}^{\alpha_{i,2k-1}} \cdot (1, \bar{u}^\alpha)$
    end if
    $C_{(i+1)k} = Rc(C_{(i+1)k})$
    $C_{(i+1)k} = L_{(i+1)k} \cdot C_{(i+1)k} + a_{(i+),k}$
  end for
end for

5. Signing procedure of DME-SIGN

Let's assume that the public key is

$$F = \Psi(L_0, \ldots, L_r, E_1, \ldots, E_r) : \mathbb{F}_q^8 \to \mathbb{F}_q^8.$$

By construction, F is a composition of bijections of $(\mathbb{F}_{q^2} \setminus \{0\})^4$ if there is no affine translations $a_{i,j} = 0$ for all i, that is:

Remark 5.1. *Let $\mathbb{U} = \bar{\phi}^{-1}((\mathbb{F}_{q^2} \setminus \{0\})^4) \subset \mathbb{F}_q^8$ then $F : \mathbb{U} \to \mathbb{U}$ is a bijection.*

If there are non zero affine translations then vector $\underline{y} \in \mathbb{U}$ may fall outside $\mathbb{U}$ after translation and this fact can produce a failure for decryption or signing. In ([LA]) we see that if we have translations at only one step the failure of encryption/decryption can be detect and corrected. If there are non zero affine translations in more than one step then can be failure of decryption even if $F(\underline{x}) \in \mathbb{U}$. In example 1, if we take $a_{11} \neq 0, a_{21} \neq 0, a_{22} \neq 0$ and the rest of the a_{ij} are zero, after L_1 we may have $(x_1^1, x_2^1) = (0, 0)$ and $E_1(y^0)$ can not be inverted but as $a_{21} \neq 0$ and $a_{22} \neq 0$ then we may have $\underline{x}^2 \in \mathbb{U}$ and $F(\underline{x}) \in \mathbb{U}$, but clearly F is not invertible at $F(\underline{x})$. One can check that if we take $a_{13} \neq 0$ and $a_{21} \neq 0$ then F has the property that if $F(\underline{x}) \in \mathbb{U}$ then $F^{-1}(F(\underline{x})) = \underline{x}$, but the converse of this statement is not true because the matrices E_i^{-1} have all the entries different from zero.

In the setting of DME-SIGN that we present here the number of rounds $r = 3or4$ and the we use affine translations in the last 3 linear maps. For instance if $r = 4$ then L_2, L_3, L_4. The signing procedure goes as follows. Let $\underline{z} = P(Men)$ the padding of the message Men , we compute $F^{-1}(\underline{z})$ starting with $\underline{z_1} = L_4^{-1}(\underline{z})$, if $\underline{z}_1 \notin \mathbb{U}$ we recompute $\underline{z} = P(Men)$ and start again. We do the same if $L_3^{-1}(\underline{z}_i)$ or $L_2^{-1}(\underline{z}_i)$ are not in $\mathbb{U}$

It vis clear that even with the translations F is a permutation in a set $\mathbb{V} \in (\mathbb{F}_{q^2} \setminus \{0\})^4$ and that the probability of $\underline{z}_i) \notin \mathbb{V}$ is approximately $1/q^2$ and we can work with F as a trapdoor one way permutation. For padding, we use the standards OAEP for PKE and KEM and PSS00 for probabilistic signature scheme, and we will denote by DME-KEM and DME-SIGN the corresponding schemes.

6. Setting of the DME-SIGN

The security of the DME depends on the chosen settings and parameters. We will describe first the setting of the the scheme $DME(r, n, 2^e)$:

6.1. **The configuration of matrices.** We define a **Configuration of Matrices** ($\mathcal{CM}$) as a list of r matrices for the exponentials where the non zero entries are substituted by 1. We denote such matrices by E_i^*. Let $\mathcal{CM} = [E_r^*, \ldots E_1^*]$ be a configuration. Then, it is easy to get the number of monomials of the each component of F from $\mathcal{CM}$ if there are no repeated monomials, just compute $E^* = E_r^* \cdots E_1^*$ and let t_k be the sum of the entries in the $k-th$ row of E^*, in which case the number of monomials of the components F_{2k-1}, F_{2k} is 2^{t_k}. In the example 1 we have

$$E^* = E_3^* \cdot E_2^* \cdot E_1^* = \begin{pmatrix} 3 & 1 & 3 \\ 3 & 2 & 2 \\ 2 & 1 & 3 \end{pmatrix}$$

and the corresponding number of monomials is $(2^7, 2^7, 2^6)$. The algorithm RED reduce number of monomials to $(32, 36, 24)$. Please notice that the output of algorithm RED depend only in the configuration $\mathcal{CM}$, we will denote it by RED($\mathcal{CM}$).If we consider possible attack of the DME by Weil descent, then t_k give also the degree of the components F_{2k-1}, F_{2k} when we express them as polynomials over $\mathbb{F}_2$. In fact one of the main reason to use $r = 4$ instead of$r = 4$ is to increase the values in the list (t_1, t_2, t_3, t_4).

6.2. **The configuration of matrices of DEM-SIGN.** For the parameters of DME-SIGN we propose $DME(r, n, 2^e)$ with $r = 3$ and non zero translations in the last 3 linear. For the configuration of matrices $\mathcal{CM}_2$ defined as follows:

$$E_1^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, E_2^* = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_3^* = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

$$E^* = E_3^* \cdot E_2^* \cdot E_1^* = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$$

By looking 2 E^* we see that $(t_1, t_2, t_3, t_4) = (5, 4, 4, 5)$. We have only to condition that reduce the number of monomials namely

$$e_{1,2} = e_{1,1} + e_{2,1} + e_{3,1} - e_{1,2} - e_{2,3},$$
$$e_{3,8} = e_{1,4} + e_{2,5} + e_{3,7} - e_{1,5} - e_{2,6}$$

With this reduction we pass from $(2^5, 2^4, 2^4, 2^5)$ monomials to $(24, 16, 26, 24)$ monomials and we will have many quadratic relations(QR). By putting translations in the linear components of $L_1, L2, L3$ we get by the algorithm MON

$(75, 25, 25, 75)$ and with the above two linear conditions the monomials are reduced to $(65, 25, 25, 65)$ and we get even more QR.

For the parameters of DME-SIGN we propose $DME(r, n, 2^e)$ with $r = 4$ and non zero translations in the last 3 linear. The configuration of matrices
$\mathcal{CM}_2$ is defined as follows:

$$E_1^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, E_2^* = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_3^* = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, E_4^* = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$E^* = E_4^* \cdot E_3^* \cdot E_2^* \cdot E_1^* = \begin{pmatrix} 3 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 \end{pmatrix}$$

By looking to E^* we see that $(t_1, t_2, t_3, t_4) = (7, 4, 4, 7)$. We have only 2 condition on E_3 and 2 condition on E_3 that reduce the number of monomials from $(2^7, 2^4, 2^4, 2^7)$ monomials to $(48, 16, 16, 48)$ monomials and there are not quadratic relations(QR) in the 48 monomials components. By putting translations in the linear components of $L_1, L2, L3$ we get by the algorithm MON $(185, 25, 25, 185)$ and with the above 4 mentioned linear conditions the monomials are reduced to $(94, 25, 25, 94)$ and there are not QR in the 94 monomials components.

We will see in sec** that both set of parameters for 3 and 4 gives the same security so we implemented only the 3 round one but keep the other setting in case that there is some concerns about future attacks in which the number of rounds matter. In order to have an approximate idea of the ratio of sizes and timing of the 3 and 4 version we can see the tables in ([4]) and compare the results for $\mathcal{CM}_1$ and $\mathcal{CM}_2$.

7. Implementation and timings of DME-SIGN

We have implemented the DME-SIGN cryptosystem with the same parameters, i.e. four linear maps with the last three of them having an affine component in each variable, interleaved with three exponential maps. The main difference between each version is the size of the finite field $\mathbb{F}_q$, which can be chosen as $q = 2^{32}$, $q = 2^{48}$ or $q = 2^{64}$. The signature is computed by applying a PSS padding (based of the SHA-3 hash function) prior our decryption function. Besides the reference implementation in C99, we provide a highly optimized version which benefits from the CLMUL instruction in modern x86_64 processors and a careful choice of the binary representation of the elements of $\mathbb{F}_q$.

	keygen	sign	open	skey	pkey	signature
$q = 2^{32}$, reference	2581 usec	321 usec	42 usec	369 bytes	1449 bytes	32 bytes
$q = 2^{32}$, optimized	121 usec	19 usec	9 usec	369 bytes	1449 bytes	32 bytes
$q = 2^{48}$, reference	7846 usec	1030 usec	100 usec	545 bytes	2169 bytes	48 bytes
$q = 2^{48}$, optimized	262 usec	35 usec	11 usec	545 bytes	2169 bytes	48 bytes
$q = 2^{64}$, reference	10911 usec	1456 usec	115 usec	721 bytes	2889 bytes	64 bytes
$q = 2^{64}$, optimized	251 usec	41 usec	12 usec	721 bytes	2889 bytes	64 bytes

Table 1: The timings correspond to a message size of 200 bytes on an Intel(R) Core(TM) i7-8565U CPU at 1.80GHz laptop running Linux Mint 21 x86_64.

8. Security of DME-SIGN

8.1. **Structural Cryptanalysis.** Given $\mathcal{CM}$, it is straightforward to use the algorithm RED($\mathcal{CM}$) to reduce the number of monomials of the F_i, in fact the linear relations depends only on $\mathcal{CM}$ and they are easy to compute. Remember that the algorithm produce some linear condition on the exponents of the matrices that allow us to eliminate some parameters and find new matrices with exponents in the remainder parameters.

An interesting point for the security of the DME is that the final exponents of the monomials depend on fewer parameters than the final matrices, this fact implies that given the monomials the public key F,we can get the values of the parameters involved in the public key and the rest of parameters are free will produce a big list of matrices with the same exponents as F. In configuration $\mathcal{CM}_1$ that we present here there are initially 20 parameters that reduce to 17 after the 2 conditions for the reduction of plus one other conditions for fixing the determinant inverse d_3. monomials. If we apply the methods ([MA, sec 6.2]) and examining the lists of exponents that appear in $(F, S1, S2, S3)$ we can verify that given the exponents matrices E_i depends of the known of F and other "free" 7 parameters. That is given the monomials of the public key there are $2^{7(\log_2(e)+1)}$ sets of matrices that produce the same monomials. This means that for $q = 2^{64}$, there are 2^{49} sets of matrices for a given public key. It is necessary to make further research to determine for instance equivalents keys with exponents that depends on less parameters.

For this reason we will estimate the security of each setting against the structural cryptoanalysis be computing the complexity of finding the linear components of the secret key starting with the last one L_3. As we explained in section 3, for each linear map L_{rk} we can use the the relations $H_{ij} = Q_{ij}(B, C) = \sum B_k C_l$, to get the quadratic relations $H_{ij} H_{kl} = H_{kj} H_{il}$ and more homogeneous implicit equations for the H_{ij} by eliminating B_i and C_j from those equations. This implicit equations will give us homogeneous equations for the unknown entries of the matrices L_{3k}^{-1} and the translations a_{3k} by using that

$$B_i = B_{i1} + \bar{u}B_{i2} = L_{3k}^{-1}(D_i) - (a_{3k1} + \bar{u}a_{3k2})$$

where $D_i = D_{i1} + \bar{u}D_{i2}$ are the known coefficients of the corresponding monomial of the public key.

As the implicit equations that we get are homogeneous, we would have a solution for the matrix of L_{3k}^{-1} and the a_{3k} that is defined up to a multiplicative constant $\lambda_k \in \mathbb{F}_q$, and given $(\lambda_1, \dots, \lambda_4) \in \mathbb{F}_q \setminus \{0\}$ we can find the inverse of the L_{3k} and a_{3k}. Once we compute the inverse of L_3 and F we are in the same situation and we will get the matrices L_{2k} up to 4 constants $(\mu_1, \dots, \mu_4) \in \mathbb{F}_q \setminus \{0\}$ thus setting the size of the field $q = 2^e$ we have to choose 8 values in $\mathbb{F}_q$ that gives 2_{8e} security margin or 2_{4e} if we take in account quantum Grover algorithm

This is one of the **main advantages** of the simple design of the DME-SIGN, namely we can change the security level by changing only the size of the base field q. For the NIST security level V we choose in the implementation $q = 2^{64}$ and the choice of the 8 constants gives us a complexity of 2^{512} or 2^{256} with Grover. For the NIST security level III we choose $q = 2^{48}$ and for the NIST level I we choose $q = 2^{32}$. We can see from the table in the next section that the sizes of the PK and SK are proportional to the size of q. The timings depends of the size of q and the way the arithmetic in $\mathbb{F}_q$ is implemented.

8.2. **Gröbner basis.** To determine the resistance of a $\mathcal{CM}$ to the Gröbner basis attack, we have to estimate the complexity of computing the Gröbner basis of the ideal

$$I = \langle f_1(\underline{x}) - y_1, \dots, f_n(\underline{x}) - y_n, x_1^{2^e} - x_1, \dots, x_n^{2^e} - x_n \rangle$$

where $F(\underline{x}) = \underline{y}$. Let $sd(I)$ be the **solving degree of** I, i.e. the the highest degree of polynomials involved in the computation of the Gröbner basis. The complexity of computing the Gröbner basis using a algorithm like F4/F5 is bounded from above by

$$O\left(\binom{n + sd(I)}{n}^{\omega}\right) \tag{2}$$

where ω is the exponent in the complexity of matrix multiplication. It is easy to see that this upper bound is well above $O(2^{256})$, since $sd(I)$ is bounded below be degree of the initial basis I , $x_n^{2^e} - x_n \in I$ and a typical monomial of F has from 4 to 8 variables we can force the degree of I to be bounded below by 2^e. Now if we take a $\mathcal{CM}$ with 8 variables (2) is bounded below by 2^{16e}. If we use $q = 2^{64}$ then the complexity is bounded by $O(2^{1024})$.

We can safely assume that $2^e \leq sd(I)$, the problem is that we do not know if the bound (2) is accurate or not for the Gröbner basis computation of this kind of ideals. In order to make an experimental testing of the above bound, we used Magma in a cluster with several fat nodes with 512 Gb of RAM each. After an extensive series of computations, Magma can find the Gröbner basis only for $q = 2^3$ and or $q = 2^4$. For $q = 2^5$ Magma exhausted the RAM before the end of the computation. Here are the conclusions that we get from our experiments.

- Given a $\mathcal{CM}$, the time of computing the Gröbner basis depends mainly on the exponents of F, but not of the actual matrices that give F.
- The initial basis I can be considered sparse because it has a low number of monomials by rapport to the degree but the intermediate computations of Magma show that the number of monomials can be very big.
- The upper bound (2) seems to be accurate, but further research is needed to confirm this fact.

Of course those conclusions can not be extrapolated for higher q. If any one can try to verify those conclusion for $e \geq 5$ we can provide them the basis for different $\mathcal{CM}$.

We can use the special form of the monomials that allow to substitute $F(\underline{x})$ by $F(y_{11}, \dots)$ as described in example 1, but this will give a greater complexity because we will have much more variables but the degree will not decrease much. Let's explain this in the example 1. We have now that $\bar{F}$ has 18 variables $\{y_{11}, \dots, y_{36}\}$. If we examine the relations among the x_i and the y_{jk} given by the lists S_1, S_2, S_3 we find, for instance, $x_1^{2^{e_{3,1}+e_{1,1}+e_{2,1}}} = y_{21}, x_1^{2^{e_{1,3}+e_{2,3}+e_{3,3}}} = y_{31}$, so we would get a relation $y_{31} = y_{21}^{2^a}$ for some $a \leq q$ and we would end with a basis $\bar{I}$ such that $sd(\bar{I}) \geq 2^e$ as before.

8.3. **Estimation of the number of monomials of the inverse.** As we mentioned earlier we set that $d_i = 1/det(A_i)modq$ has a fixed binary weight to get a number of monomials of the inverse big enough and to speed up the computation of $F{-}1(\underline{z})$. From the shape of the matrix A_3(or A_3) can see that the adjoint matrix $Adj(E_3)modq$ has on each row one entry that is a power of 2 with a minus sign so its binary weight is $2e - 1$ so if we started with the 8 coordinates of $\underline{z}$ then $E_3^{-1}(\underline{z})$ will have at least 2^{2e} monomials in each components and much more after the other 2 natrix exponentiations independent of the binary weight of d_3 In the implementation we fix d_3 with binary weight 9.

8.4. **Weil descent.** Taking a base of $\mathbb{F}_q$ over $\mathbb{F}_2$, namely $B = \{v_1, \dots, v_e\}$, we can express the polynomial of F as polynomials $\tilde{F}$ in $8e$ variables over $\mathbb{F}_2$. It is easy to verify that before the reduction of monomials, the degrees of the components of $\tilde{F}$ are $(t_1 \dots t_4)$. In fact the raise of the binary degree of the public key was one of the reasons to use more than two exponentials to defend DME against attacks like ([5])

The reduction of monomials can produce also a reduction of the degrees of $\tilde{F}$ and it is not possible to determine apriori the degrees of the $\tilde{F}$. One has to examine the list of monomials after the reduction and compute the degrees. For instance, in example 1 the degrees reduced from $(7, 7, 6)$ to $(5, 6, 6)$.

References

[1] J. Ding, D.r Schmidt: Solving degree and degree of regularity for polynomial systems over finite fields. Number theory and cryptography, pp. 34–49, Lecture Notes in Comput. Sci., 8260, Springer, Heidelberg, 2013.

[2] J. Ding, C. Wolf, B. Yang: l-Invertible Cycles for Multivariate Quadratic (MQ) Public Key Cryptography.

[3] I. Luengo: DME a public key, signature and KEM system based on double exponentiation with matrix exponents. Preprint 2017. `https://csrc.nist.gov/CSRC/media/Presentations/DME/images-media/dme-April2018.pdf`

[4] I. Luengo, M. Avendaño : DME: a full encryption, signature and KEM multivariate public key cryptosystem. IACR preprint 2022/1538.

[5] J.C. Faugère, L. Perret.:An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. Journal of Symbolic Computation 44 (2009) 1676–1689

Implementation of DME-3rnds-8vars-32bits-sign

Ignacio Luengo*[1], Martín Avendaño†[1], and Pilar Coscojuela‡[1]

[1]Universidad Complutense de Madrid

June 27, 2023

The `DME-3rnds-8vars-32bits-sign` is a signature scheme based on the composition of three different types of polynomial maps $\mathbb{F}_{2^{32}}^8 \to \mathbb{F}_{2^{32}}^8$ that are bijective almost everywhere: linear maps, affine shifts, and exponential maps. The individual maps form the secret key, and the composition of the maps, which is given by eight polynomials in $\mathbb{F}_{2^{32}}[x_1, \ldots, x_8]$ is the public key. The signature is obtained by mapping the message to $\mathbb{F}_{2^{32}}^8$ using a hash function (and a PSS padding with 64 random bits) and then applying the decryption map to get a signature of 256 bits (32 bytes).

1 Mathematical description of DME-3rnds-8vars-32bits-sign

Let $q = 2^{32}$ and let $\mathbb{F}_q$ be a finite field with q elements. Consider an irreducible monic polinomial $p(u) = u^2 + p_1 u + p_0 \in \mathbb{F}_q[u]$. The quotient ring $\mathbb{F}_q[u]/\langle p(u) \rangle$ defines a field of q^2 elements, which we denote $\mathbb{F}_{q^2}$. The map $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ given by

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto x + yu$$

is a bijection. This map can be extended naturally to a map $\overline{\phi} : \mathbb{F}_q^8 \to (\mathbb{F}_{q^2})^4$

$$\overline{\phi} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} \phi \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ \phi \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ \phi \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ \phi \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

which is also a bijection.

For any matrix $M \in \mathbb{Z}^{4\times 4}$, we define the exponential map $E_M : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ given by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \begin{bmatrix} x_1^{m_{11}} x_2^{m_{12}} x_3^{m_{13}} x_4^{m_{14}} \\ x_1^{m_{21}} x_2^{m_{22}} x_3^{m_{23}} x_4^{m_{24}} \\ x_1^{m_{31}} x_2^{m_{32}} x_3^{m_{33}} x_4^{m_{34}} \\ x_1^{m_{41}} x_2^{m_{42}} x_3^{m_{43}} x_4^{m_{44}} \end{bmatrix}.$$

The following result summarizes the properties of the exponential maps that are needed for the `DME-3rnds-8vars-32bits-sign` cryptosystem.

*iluengo@ucm.es
†mavend01@ucm.es
‡picoscoj@ucm.es

Lemma 1.1. *Let $M_1, M_2 \in \mathbb{Z}^{4\times 4}$. Then:*

1. $E_{M_1} \circ E_{M_2} = E_{M_1 \cdot M_2}$.
2. $M_1 \equiv M_2 \pmod{q^2-1} \Rightarrow E_{M_1} = E_{M_2}$.
3. $M_1 \cdot M_2 \equiv \mathrm{Id} \pmod{q^2-1} \Rightarrow E_{M_1} \circ E_{M_2} = \mathrm{Id}$.
4. $\gcd(\det(M_1), q^2-1) = 1 \Rightarrow E_{M_1}$ *is invertible.*

If no entry of the matrix M is negative, then E_M can be extended to a map $\overline{E_M} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ with the same formula and setting $0^0 = 1$. It should be noted that the extended maps $\overline{E_M}$ fail in general to be bijections, even if $\gcd(\det(M), q^2-1) = 1$.

In `DME-3rnds-8vars-32bits-sign`, we have three exponential maps E_1, E_2 and E_3, whose matrices are

$$M_1 = \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix},$$

respectively, with $a_0, \ldots, a_5, b_0, \ldots, b_5, c_0, \ldots, c_7 \in [0, 63]$ such that

$$\begin{aligned} c_1 &\equiv a_0 + b_0 + c_0 - a_1 - b_2 \pmod{64}, \\ c_7 &\equiv a_3 + b_4 + c_6 - a_4 - b_5 \pmod{64}, \\ c_4 &\equiv c_2 + c_5 - c_3 + 57 \pmod{64}. \end{aligned}$$

It is easy to verify that the three matrices M_1, M_2 and M_3 satisfy condition 4 of lemma 1.1.

In `DME-3rnds-8vars-32bits-sign`, we also needs four invertible linear maps $L_1, L_2, L_3, L_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$, each of which has a four 2×2 block structure

$$L_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} L_{i1} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ L_{i2} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ L_{i3} \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ L_{i4} \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

with $L_{ij} \in \mathbb{F}_q^{2\times 2}$ and $\det(L_{ij}) \neq 0$.

In addition to the linear maps, we have three affine shifts $A_2, A_3, A_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ given by

$$A_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} x_1 + A_{i1} \\ x_2 + A_{i2} \\ x_3 + A_{i3} \\ x_4 + A_{i4} \\ x_5 + A_{i5} \\ x_6 + A_{i6} \\ x_7 + A_{i7} \\ x_8 + A_{i8} \end{bmatrix}$$

with $A_{ij} \in \mathbb{F}_q$.

The secret key consists of the four linear maps L_1, L_2, L_3, L_4, the three affine shifts A_2, A_3, A_4 and the three exponential maps E_1, E_2, E_3. The following composition

$$A_4 \circ L_4 \circ \overline{\phi}^{-1} \circ \overline{E_3} \circ \overline{\phi} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1$$

defines a map `dme-enc` : $\mathbb{F}_q^8 \to \mathbb{F}_q^8$.

Let $D \subseteq \mathbb{F}_q^8$ be the set of $x \in \mathbb{F}_q^8$ such that

$$\begin{aligned}
&(\overline{\phi}^{-1} \circ L_1)(x),\\
&(\overline{\phi}^{-1} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x),\\
&(\overline{\phi}^{-1} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x)
\end{aligned}$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry. Let $E = \texttt{dme-enc}(D) \subseteq \mathbb{F}_q^8$. By construction, the restriction `dme-enc` : $D \to E$ is a bijection.

Lemma 1.2. $|D| \geq 3(q^2-1)^4 - 2q^8 \geq q^8 - 12q^6$. *In particular, the probability that a randomly chosen $x \in \mathbb{F}_q^8$ (with a uniform distribution) does not belong to D is at most $12q^{-2} < 2^{-60}$.*

The main property of the map `dme-enc` is that it can be given by polynomials (this fact can be proven by following the sequence of maps that define `dme-enc`, starting with 8 variables $x_1, \ldots, x_8$). More precisely, there exists $p_1, \ldots, p_8 \in \mathbb{F}_q[x_1, \ldots, x_8]$ such that

$$\texttt{dme-enc}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} p_1(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_2(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_3(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_4(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_5(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_6(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_7(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_8(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \end{bmatrix}$$

where p_1, p_2, p_7, p_8 having 65 monomials each and p_3, p_4, p_5, p_6 having 25 monomials each.

Define the integers $f_0, \ldots, f_{15} \in [0, 31]$ as

$$\begin{aligned}
f_0 &= a_0 + b_0 + c_0 \bmod 32\\
f_1 &= a_1 + b_2 + c_2 \bmod 32\\
f_2 &= a_1 + b_2 + c_4 \bmod 32\\
f_3 &= a_1 + b_2 + c_6 \bmod 32\\
f_4 &= a_2 + a_0 + b_0 - a_1 + c_0 \bmod 32\\
f_5 &= a_2 + b_2 + c_2 \bmod 32\\
f_6 &= a_2 + b_2 + c_4 \bmod 32\\
f_7 &= a_2 + b_2 + c_6 \bmod 32\\
f_8 &= a_4 + b_5 + c_1 \bmod 32\\
f_9 &= a_4 + b_5 + c_3 \bmod 32\\
f_{10} &= a_4 + b_5 + c_5 \bmod 32\\
f_{11} &= a_3 + b_3 + c_7 \bmod 32\\
f_{12} &= a_5 + b_5 + c_1 \bmod 32\\
f_{13} &= a_5 + b_5 + c_3 \bmod 32\\
f_{14} &= a_5 + b_5 + c_5 \bmod 32\\
f_{15} &= a_5 + a_3 + b_3 - a_4 + c_7 \bmod 32
\end{aligned}$$

and consider the expressions

$$\begin{array}{llll}
z_0 = x_1^{2^{f_0}} & z_1 = x_1^{2^{f_1}} & z_2 = x_1^{2^{f_2}} & z_3 = x_1^{2^{f_3}} \\
z_4 = x_2^{2^{f_0}} & z_5 = x_2^{2^{f_1}} & z_6 = x_2^{2^{f_2}} & z_7 = x_1^{2^{f_3}} \\
z_8 = x_3^{2^{f_4}} & z_9 = x_3^{2^{f_5}} & z_{10} = x_3^{2^{f_6}} & z_{11} = x_3^{2^{f_7}} \\
z_{12} = x_4^{2^{f_4}} & z_{13} = x_4^{2^{f_5}} & z_{14} = x_4^{2^{f_6}} & z_{15} = x_4^{2^{f_7}} \\
z_{16} = x_5^{2^{f_8}} & z_{17} = x_5^{2^{f_9}} & z_{18} = x_5^{2^{f_{10}}} & z_{19} = x_5^{2^{f_{11}}} \\
z_{20} = x_6^{2^{f_8}} & z_{21} = x_6^{2^{f_9}} & z_{22} = x_6^{2^{f_{10}}} & z_{23} = x_6^{2^{f_{11}}} \\
z_{24} = x_7^{2^{f_{12}}} & z_{25} = x_7^{2^{f_{13}}} & z_{26} = x_7^{2^{f_{14}}} & z_{27} = x_7^{2^{f_{15}}} \\
z_{28} = x_8^{2^{f_{12}}} & z_{29} = x_8^{2^{f_{13}}} & z_{30} = x_8^{2^{f_{14}}} & z_{31} = x_8^{2^{f_{15}}}
\end{array}$$

A careful study of p_1 and p_2 show that the 65 monomials are exactly

$$\begin{array}{lll}
m_{1,1} = z_{24}z_{16}z_8z_0^2 & m_{1,2} = z_{28}z_{16}z_8z_0^2 & m_{1,3} = z_{24}z_{20}z_8z_0^2 \\
m_{1,4} = z_{28}z_{20}z_8z_0^2 & m_{1,5} = z_8z_0^2 & m_{1,6} = z_{24}z_{16}z_{12}z_0^2 \\
m_{1,7} = z_{28}z_{16}z_{12}z_0^2 & m_{1,8} = z_{24}z_{20}z_{12}z_0^2 & m_{1,9} = z_{28}z_{20}z_{12}z_0^2 \\
m_{1,10} = z_{12}z_0^2 & m_{1,11} = z_{24}z_{16}z_8z_4z_0 & m_{1,12} = z_{28}z_{16}z_8z_4z_0 \\
m_{1,13} = z_{24}z_{20}z_8z_4z_0 & m_{1,14} = z_{28}z_{20}z_8z_4z_0 & m_{1,15} = z_8z_4z_0 \\
m_{1,16} = z_{24}z_{16}z_{12}z_4z_0 & m_{1,17} = z_{28}z_{16}z_{12}z_4z_0 & m_{1,18} = z_{24}z_{20}z_{12}z_4z_0 \\
m_{1,19} = z_{28}z_{20}z_{12}z_4z_0 & m_{1,20} = z_{12}z_4z_0 & m_{1,21} = z_{24}z_{16}z_0 \\
m_{1,22} = z_{28}z_{16}z_0 & m_{1,23} = z_{24}z_{20}z_0 & m_{1,24} = z_{28}z_{20}z_0 \\
m_{1,25} = z_0 & m_{1,26} = z_{24}z_{16}z_8z_4^2 & m_{1,27} = z_{28}z_{16}z_8z_4^2 \\
m_{1,28} = z_{24}z_{20}z_8z_4^2 & m_{1,29} = z_{28}z_{20}z_8z_4^2 & m_{1,30} = z_8z_4^2 \\
m_{1,31} = z_{24}z_{16}z_{12}z_4^2 & m_{1,32} = z_{28}z_{16}z_{12}z_4^2 & m_{1,33} = z_{24}z_{20}z_{12}z_4^2 \\
m_{1,34} = z_{28}z_{20}z_{12}z_4^2 & m_{1,35} = z_{12}z_4^2 & m_{1,36} = z_{24}z_{16}z_4 \\
m_{1,37} = z_{28}z_{16}z_4 & m_{1,38} = z_{24}z_{20}z_4 & m_{1,39} = z_{28}z_{20}z_4 \\
m_{1,40} = z_4 & m_{1,41} = z_{24}z_{16}z_8z_0 & m_{1,42} = z_{28}z_{16}z_8z_0 \\
m_{1,43} = z_{24}z_{20}z_8z_0 & m_{1,44} = z_{28}z_{20}z_8z_0 & m_{1,45} = z_8z_0 \\
m_{1,46} = z_{24}z_{16}z_{12}z_0 & m_{1,47} = z_{28}z_{16}z_{12}z_0 & m_{1,48} = z_{24}z_{20}z_{12}z_0 \\
m_{1,49} = z_{28}z_{20}z_{12}z_0 & m_{1,50} = z_{12}z_0 & m_{1,51} = z_{24}z_{16}z_8z_4 \\
m_{1,52} = z_{28}z_{16}z_8z_4 & m_{1,53} = z_{24}z_{20}z_8z_4 & m_{1,54} = z_{28}z_{20}z_8z_4 \\
m_{1,55} = z_8z_4 & m_{1,56} = z_{24}z_{16}z_{12}z_4 & m_{1,57} = z_{28}z_{16}z_{12}z_4 \\
m_{1,58} = z_{24}z_{20}z_{12}z_4 & m_{1,59} = z_{28}z_{20}z_{12}z_4 & m_{1,60} = z_{12}z_4 \\
m_{1,61} = z_{24}z_{16} & m_{1,62} = z_{28}z_{16} & m_{1,63} = z_{24}z_{20} \\
m_{1,64} = z_{28}z_{20} & m_{1,65} = 1 &
\end{array}$$

Similarly, the 25 monomials that appear in p_3 and p_4 are

$$\begin{array}{lll}
m_{2,1} = z_{25}z_{17}z_9z_1 & m_{2,2} = z_{29}z_{17}z_9z_1 & m_{2,3} = z_{25}z_{21}z_9z_1 \\
m_{2,4} = z_{29}z_{21}z_9z_1 & m_{2,5} = z_9z_1 & m_{2,6} = z_{25}z_{17}z_{13}z_1 \\
m_{2,7} = z_{29}z_{17}z_{13}z_1 & m_{2,8} = z_{25}z_{21}z_{13}z_1 & m_{2,9} = z_{29}z_{21}z_{13}z_1 \\
m_{2,10} = z_{13}z_1 & m_{2,11} = z_{25}z_{17}z_9z_5 & m_{2,12} = z_{29}z_{17}z_9z_5 \\
m_{2,13} = z_{25}z_{21}z_9z_5 & m_{2,14} = z_{29}z_{21}z_9z_5 & m_{2,15} = z_9z_5 \\
m_{2,16} = z_{25}z_{17}z_{13}z_5 & m_{2,17} = z_{29}z_{17}z_{13}z_5 & m_{2,18} = z_{25}z_{21}z_{13}z_5 \\
m_{2,19} = z_{29}z_{21}z_{13}z_5 & m_{2,20} = z_{13}z_5 & m_{2,21} = z_{25}z_{17} \\
m_{2,22} = z_{29}z_{17} & m_{2,23} = z_{25}z_{21} & m_{2,24} = z_{29}z_{21} \\
m_{2,25} = 1 & &
\end{array}$$

the 25 monomials that appear in p_5 and p_6 are

$$\begin{array}{lll}
m_{3,1} = z_{26}z_{18}z_{10}z_2 & m_{3,2} = z_{30}z_{18}z_{10}z_2 & m_{3,3} = z_{26}z_{22}z_{10}z_2 \\
m_{3,4} = z_{30}z_{22}z_{10}z_2 & m_{3,5} = z_{10}z_2 & m_{3,6} = z_{26}z_{18}z_{14}z_2 \\
m_{3,7} = z_{30}z_{18}z_{14}z_2 & m_{3,8} = z_{26}z_{22}z_{14}z_2 & m_{3,9} = z_{30}z_{22}z_{14}z_2 \\
m_{3,10} = z_{14}z_2 & m_{3,11} = z_{26}z_{18}z_{10}z_6 & m_{3,12} = z_{30}z_{18}z_{10}z_6 \\
m_{3,13} = z_{26}z_{22}z_{10}z_6 & m_{3,14} = z_{30}z_{22}z_{10}z_6 & m_{3,15} = z_{10}z_6 \\
m_{3,16} = z_{26}z_{18}z_{14}z_6 & m_{3,17} = z_{30}z_{18}z_{14}z_6 & m_{3,18} = z_{26}z_{22}z_{14}z_6 \\
m_{3,19} = z_{30}z_{22}z_{14}z_6 & m_{3,20} = z_{14}z_6 & m_{3,21} = z_{26}z_{18} \\
m_{3,22} = z_{30}z_{18} & m_{3,23} = z_{26}z_{22} & m_{3,24} = z_{30}z_{22} \\
m_{3,25} = 1 & &
\end{array}$$

and the 65 monomials that appear in p_7 and p_8 are

$$\begin{array}{lll}
m_{4,1} = z_{27}z_{19^2}z_{11}z_3 & m_{4,2} = z_{31}z_{19^2}z_{11}z_3 & m_{4,3} = z_{27}z_{23}z_{19}z_{11}z_3 \\
m_{4,4} = z_{31}z_{23}z_{19}z_{11}z_3 & m_{4,5} = z_{19}z_{11}z_3 & m_{4,6} = z_{27}z_{23^2}z_{11}z_3 \\
m_{4,7} = z_{31}z_{23^2}z_{11}z_3 & m_{4,8} = z_{23}z_{11}z_3 & m_{4,9} = z_{27}z_{19}z_{11}z_3 \\
m_{4,10} = z_{31}z_{19}z_{11}z_3 & m_{4,11} = z_{27}z_{23}z_{11}z_3 & m_{4,12} = z_{31}z_{23}z_{11}z_3 \\
m_{4,13} = z_{11}z_3 & m_{4,14} = z_{27}z_{19^2}z_{15}z_3 & m_{4,15} = z_{31}z_{19^2}z_{15}z_3 \\
m_{4,16} = z_{27}z_{23}z_{19}z_{15}z_3 & m_{4,17} = z_{31}z_{23}z_{19}z_{15}z_3 & m_{4,18} = z_{19}z_{15}z_3 \\
m_{4,19} = z_{27}z_{23^2}z_{15}z_3 & m_{4,20} = z_{31}z_{23^2}z_{15}z_3 & m_{4,21} = z_{23}z_{15}z_3 \\
m_{4,22} = z_{27}z_{19}z_{15}z_3 & m_{4,23} = z_{31}z_{19}z_{15}z_3 & m_{4,24} = z_{27}z_{23}z_{15}z_3 \\
m_{4,25} = z_{31}z_{23}z_{15}z_3 & m_{4,26} = z_{15}z_3 & m_{4,27} = z_{27}z_{19^2}z_{11}z_7 \\
m_{4,28} = z_{31}z_{19^2}z_{11}z_7 & m_{4,29} = z_{27}z_{23}z_{19}z_{11}z_7 & m_{4,30} = z_{31}z_{23}z_{19}z_{11}z_7 \\
m_{4,31} = z_{19}z_{11}z_7 & m_{4,32} = z_{27}z_{23^2}z_{11}z_7 & m_{4,33} = z_{31}z_{23^2}z_{11}z_7 \\
m_{4,34} = z_{23}z_{11}z_7 & m_{4,35} = z_{27}z_{19}z_{11}z_7 & m_{4,36} = z_{31}z_{19}z_{11}z_7 \\
m_{4,37} = z_{27}z_{23}z_{11}z_7 & m_{4,38} = z_{31}z_{23}z_{11}z_7 & m_{4,39} = z_{11}z_7 \\
m_{4,40} = z_{27}z_{19^2}z_{15}z_7 & m_{4,41} = z_{31}z_{19^2}z_{15}z_7 & m_{4,42} = z_{27}z_{23}z_{19}z_{15}z_7 \\
m_{4,43} = z_{31}z_{23}z_{19}z_{15}z_7 & m_{4,44} = z_{19}z_{15}z_7 & m_{4,45} = z_{27}z_{23^2}z_{15}z_7 \\
m_{4,46} = z_{31}z_{23^2}z_{15}z_7 & m_{4,47} = z_{23}z_{15}z_7 & m_{4,48} = z_{27}z_{19}z_{15}z_7 \\
m_{4,49} = z_{31}z_{19}z_{15}z_7 & m_{4,50} = z_{27}z_{23}z_{15}z_7 & m_{4,51} = z_{31}z_{23}z_{15}z_7 \\
m_{4,52} = z_{15}z_7 & m_{4,53} = z_{27}z_{19^2} & m_{4,54} = z_{31}z_{19^2} \\
m_{4,55} = z_{27}z_{23}z_{19} & m_{4,56} = z_{31}z_{23}z_{19} & m_{4,57} = z_{19} \\
m_{4,58} = z_{27}z_{23^2} & m_{4,59} = z_{31}z_{23^2} & m_{4,60} = z_{23} \\
m_{4,61} = z_{27}z_{19} & m_{4,62} = z_{31}z_{19} & m_{4,63} = z_{27}z_{23} \\
m_{4,64} = z_{31}z_{23} & m_{4,65} = 1 &
\end{array}$$

Using the notation above, the polynomials $p_1, \ldots, p_8$ can be written as

$$\begin{array}{ll}
p_1 = \sum_{i=1}^{65} p_{1,i}m_{1,i} & p_2 = \sum_{i=1}^{65} p_{2,i}m_{1,i} \\
p_3 = \sum_{i=1}^{25} p_{3,i}m_{2,i} & p_4 = \sum_{i=1}^{25} p_{4,i}m_{2,i} \\
p_5 = \sum_{i=1}^{25} p_{5,i}m_{3,i} & p_6 = \sum_{i=1}^{25} p_{6,i}m_{3,i} \\
p_7 = \sum_{i=1}^{65} p_{7,i}m_{4,i} & p_8 = \sum_{i=1}^{65} p_{8,i}m_{4,i}
\end{array}$$

and the public key is just these eight polynomials (which are encoded by the list of 360 coefficients and the values $f_0, \ldots, f_{15}$).

Let M_1^{-1}, M_2^{-1}, and M_3^{-1} be the inverses of M_1, M_2, and M_3 modulo $q^2 - 1$, respectively, with their entries reduced to the interval $[0, q^2 - 1)$. Let $E_1^{-1}, E_2^{-1}, E_3^{-1} : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ the corresponding exponential maps and $\overline{E_1^{-1}}, \overline{E_2^{-1}}, \overline{E_3^{-1}} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ their extensions. The following composition

$$L_1^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_1^{-1}} \circ \overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1}$$

defines a map $\texttt{dme-dec} : \mathbb{F}_q^8 \to \mathbb{F}_q^8$. By construction, we have that `dme-dec` maps E to D and, restricted to those sets, is the inverse of `dme-enc`. It is easy to verify that E is exactly the set of $y \in \mathbb{F}_q^8$ such

that

$$(\overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y)$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry.

The cryptographic assumption in `DME-3rnds-8vars-32bits-sign` is that, for any $y \in E$, the system of eight polynomial equations in eight unknowns

$$\begin{aligned}
p_1(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_1 \\
p_2(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_2 \\
p_3(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_3 \\
p_4(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_4 \\
p_5(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_5 \\
p_6(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_6 \\
p_7(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_7 \\
p_8(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_8
\end{aligned}$$

is hard to solve. In particular, this implies that it is not feasible to compute a secret key corresponding to a given public key.

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{256}$ map of the `DME-3rnds-8vars-32bits-sign` scheme, as required by the API, returns (m, s) where m is the original message and the signature s is obtained by first applying a PSS-SHA3 padding (with 64 random bits), then reading the 256 bit sequence as a vector in $\mathbb{F}_q^8$, applying `dme-dec`, and lastly, interpreting the resulting vector as a 256 bit sequence. The `dme-open` $: \{0,1\}^* \times \{0,1\}^{256} \to \{0,1\}^* \cup \{error\}$ reverses the procedure above using `dme-enc` and checks that the signature is legitimate. The details of these algorithms are given in the next section.

2 Implementation details of DME-3rnds-8vars-32bits-sign

The field of $q = 2^{32}$ is implemented as the quotient ring

$$\mathbb{F}_q = \mathbb{F}_2[t]/\langle t^{32} + t^{11} + t^4 + t + 1\rangle,$$

and the monic irreducible polynomial $p(u) \in \mathbb{F}_q[u]$ that defines $\mathbb{F}_{q^2}$ is $p(u) = u^2 + tu + 1$, so we have

$$\mathbb{F}_{q^2} = \mathbb{F}_q[u]/\langle u^2 + tu + 1\rangle.$$

An element $\alpha = \alpha_{31}t^{31} + \cdots + \alpha_1 t + \alpha_0 \in \mathbb{F}_q$ can be interpreted as the 32 bits unsigned integer $\texttt{int}(\alpha) = \alpha_{31}2^{31} + \cdots + \alpha_1 2 + \alpha_0 \in [0, 2^{64} - 1]$. In C99, these fit perfectly in the `uint32_t` type of the standard library. When serialized into bytes, the little-endian convention is used for all integer types. In particular, the element α above, correspond with the sequence of 4 bytes

$$\left(\left\lfloor \frac{\texttt{int}(\alpha)}{2^{8i}} \right\rfloor \bmod 2^8 \right)$$

for $i = 0, 1, \ldots, 3$ in exactly this order. An element $\beta = \beta_0 + \beta_1 u \in \mathbb{F}_{q^2}$ is serialized as the 8 byte sequence obtained by serializing first β_0 and then β_1. Similarly, a matrix $\gamma \in \mathbb{F}_q^{2\times 2}$ is serialized as the 16 bytes sequence obtained by serializing γ_{11}, γ_{12}, γ_{21}, γ_{22} in that order.

The private key is $369 = 16 \cdot 16 + 24 \cdot 4 + 6 + 6 + 5$ bytes long, which correspond to the serialization of the the 16 matrices $L_{11}^{-1}, L_{12}^{-1}, \ldots, L_{44}^{-1}$, then the serialization of the 24 affine shifts $A_{21}, A_{22}, A_{31}, A_{32}, A_{41}, A_{42}, A_{23}, A_{24}, \ldots, A_{47}, A_{48} \in \mathbb{F}_q$, followed by a single byte for each $a_0, \ldots, a_5$,

$b_0, \ldots, b_5, c_0, c_2, c_3, c_5, c_6$. The coefficients c_1, c_4 and c_7 are not serialized since they can be recovered from the other values.

The public key is $1449 = 360 \cdot 8 + 9$ bytes long, which correspond to the serialization of the coefficients of $p_1, p_2, \ldots, p_8$ followed by a single byte for each $f_0, f_1, f_3, f_5, f_8, f_9, f_{10}, f_{11}, f_{12}$. The values of $f_2, f_4, f_6, f_7, f_{13}, f_{14}, f_{15}$ are not serialized since they can be computed from the other values by

$$\begin{aligned}
f_2 &= (f_1 + f_{10} - f_9 + 57) \bmod 32 \\
f_4 &= (f_0 + f_5 - f_1) \bmod 32 \\
f_6 &= (f_5 + f_2 - f_1) \bmod 32 \\
f_7 &= (f_5 + f_3 - f_1) \bmod 32 \\
f_{13} &= (f_{12} + f_9 - f_8) \bmod 32 \\
f_{14} &= (f_{12} + f_{10} - f_8) \bmod 32 \\
f_{15} &= (f_{11} + f_{12} - f_8) \bmod 32
\end{aligned}$$

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{256}$ map (the secret key is implicit here) is computed by the following procedure:

1. let $msg \in \{0,1\}^*$ be the input message,
2. choose $r \in \{0,1\}^{64}$ at random,
3. compute $w = \texttt{SHA3}(msg||r) \in \{0,1\}^{128}$,
4. compute $g = \texttt{SHA3}(w) \oplus (r||0) \in \{0,1\}^{128}$,
5. compute $s = \texttt{dme-dec}(w||g) \in \mathbb{F}_q^8 \simeq \{0,1\}^{256}$,
6. return (msg, s).

This function is implemented in C99 as `crypto_sign`, with the only difference that the return value is $msg||s$ instead of (msg, s).

The `dme-open` $: \{0,1\}^* \times \{0,1\}^{256} \to \{0,1\}^* \cup \{error\}$ map (the public key is implicit here) is computed as follows:

1. let $(msg, s) \in \{0,1\}^* \times \{0,1\}^{256}$ be the input message and its corresponding signature,
2. compute $w \in \{0,1\}^{128}$ and $g \in \{0,1\}^{128}$ as $w||g = \texttt{dme-enc}(s)$,
3. compute $r \in \{0,1\}^{64}$ as the first 64 bits of $\texttt{SHA3}(w) \oplus g$,
4. if $w \neq \texttt{SHA3}(msg||r)$, return $error$,
5. otherwise, return the original message msg.

This function is implemented in C99 as `crypto_sign_open`, but the two separate arguments for the message msg and the signature s, the function takes only one with the concatenation of both $msg||s$.

The function `dme-keypair`, which corresponds in the C99 implementation with `crypto_sign_keypair` creates 16 random matrices in $\mathbb{F}_q^{2\times 2}$, 4 random shifts in $\mathbb{F}_q^8$ and random values for $a_0, \ldots, c_7 \in [0, 127]$ satisfying the restrictions explained in the previous section (for instance, the matrices have to be invertible). With the secret key already chosen, the public key is computed by operating with 8 (symbolic) polynomials until $p_1, \ldots, p_8 \in \mathbb{F}_q[x_1, \ldots, x_8]$ is obtained. Then both keys are serialized and returned.

3 Timings

On a laptop with a Intel(R) Core(TM) i7-8565U CPU at 1.80GHz, with 8 Gb of RAM, running a Linux Mint 21 x86_64 operating system, the performance of the API primitives (for message of 200 bytes) is given in the following table:

`dme-keypair`	121 usec
`dme-sign`	19 usec
`dme-open`	9 usec

The length of the private key is 369 bytes and the length of the public key is 1449 bytes.

Implementation of DME-3rnds-8vars-48bits-sign

Ignacio Luengo*[1], Martín Avendaño†[1], and Pilar Coscojuela‡[1]

[1]Universidad Complutense de Madrid

June 27, 2023

The `DME-3rnds-8vars-48bits-sign` is a signature scheme based on the composition of three different types of polynomial maps $\mathbb{F}_{2^{48}}^8 \to \mathbb{F}_{2^{48}}^8$ that are bijective almost everywhere: linear maps, affine shifts, and exponential maps. The individual maps form the secret key, and the composition of the maps, which is given by eight polynomials in $\mathbb{F}_{2^{48}}[x_1, \ldots, x_8]$ is the public key. The signature is obtained by mapping the message to $\mathbb{F}_{2^{48}}^8$ using a hash function (and a PSS padding with 96 random bits) and then applying the decryption map to get a signature of 384 bits (48 bytes).

1 Mathematical description of DME-3rnds-8vars-48bits-sign

Let $q = 2^{48}$ and let $\mathbb{F}_q$ be a finite field with q elements. Consider an irreducible monic polinomial $p(u) = u^2 + p_1 u + p_0 \in \mathbb{F}_q[u]$. The quotient ring $\mathbb{F}_q[u]/\langle p(u) \rangle$ defines a field of q^2 elements, which we denote $\mathbb{F}_{q^2}$. The map $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ given by

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto x + yu$$

is a bijection. This map can be extended naturally to a map $\overline{\phi} : \mathbb{F}_q^8 \to (\mathbb{F}_{q^2})^4$

$$\overline{\phi} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} \phi \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ \phi \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ \phi \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ \phi \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

which is also a bijection.

For any matrix $M \in \mathbb{Z}^{4\times 4}$, we define the exponential map $E_M : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ given by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \begin{bmatrix} x_1^{m_{11}} x_2^{m_{12}} x_3^{m_{13}} x_4^{m_{14}} \\ x_1^{m_{21}} x_2^{m_{22}} x_3^{m_{23}} x_4^{m_{24}} \\ x_1^{m_{31}} x_2^{m_{32}} x_3^{m_{33}} x_4^{m_{34}} \\ x_1^{m_{41}} x_2^{m_{42}} x_3^{m_{43}} x_4^{m_{44}} \end{bmatrix}.$$

The following result summarizes the properties of the exponential maps that are needed for the `DME-3rnds-8vars-48bits-sign` cryptosystem.

*iluengo@ucm.es

†mavend01@ucm.es

‡picoscoj@ucm.es

Lemma 1.1. *Let $M_1, M_2 \in \mathbb{Z}^{4\times 4}$. Then:*

1. $E_{M_1} \circ E_{M_2} = E_{M_1 \cdot M_2}$.
2. $M_1 \equiv M_2 \pmod{q^2-1} \Rightarrow E_{M_1} = E_{M_2}$.
3. $M_1 \cdot M_2 \equiv \mathrm{Id} \pmod{q^2-1} \Rightarrow E_{M_1} \circ E_{M_2} = \mathrm{Id}$.
4. $\gcd(\det(M_1), q^2-1) = 1 \Rightarrow E_{M_1}$ *is invertible.*

If no entry of the matrix M is negative, then E_M can be extended to a map $\overline{E_M} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ with the same formula and setting $0^0 = 1$. It should be noted that the extended maps $\overline{E_M}$ fail in general to be bijections, even if $\gcd(\det(M), q^2-1) = 1$.

In `DME-3rnds-8vars-48bits-sign`, we have three exponential maps E_1, E_2 and E_3, whose matrices are

$$M_1 = \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix},$$

respectively, with $a_0, \ldots, a_5, b_0, \ldots, b_5, c_0, \ldots, c_7 \in [0, 95]$ such that

$$\begin{aligned} c_1 &\equiv a_0 + b_0 + c_0 - a_1 - b_2 \pmod{96}, \\ c_7 &\equiv a_3 + b_4 + c_6 - a_4 - b_5 \pmod{96}, \\ c_4 &\equiv c_2 + c_5 - c_3 + 17 \pmod{96}. \end{aligned}$$

It is easy to verify that the three matrices M_1, M_2 and M_3 satisfy condition 4 of lemma 1.1.

In `DME-3rnds-8vars-48bits-sign`, we also needs four invertible linear maps $L_1, L_2, L_3, L_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$, each of which has a four 2×2 block structure

$$L_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} L_{i1} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ L_{i2} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ L_{i3} \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ L_{i4} \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

with $L_{ij} \in \mathbb{F}_q^{2\times 2}$ and $\det(L_{ij}) \neq 0$.

In addition to the linear maps, we have three affine shifts $A_2, A_3, A_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ given by

$$A_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} x_1 + A_{i1} \\ x_2 + A_{i2} \\ x_3 + A_{i3} \\ x_4 + A_{i4} \\ x_5 + A_{i5} \\ x_6 + A_{i6} \\ x_7 + A_{i7} \\ x_8 + A_{i8} \end{bmatrix}$$

with $A_{ij} \in \mathbb{F}_q$.

The secret key consists of the four linear maps L_1, L_2, L_3, L_4, the three affine shifts A_2, A_3, A_4 and the three exponential maps E_1, E_2, E_3. The following composition

$$A_4 \circ L_4 \circ \overline{\phi}^{-1} \circ \overline{E_3} \circ \overline{\phi} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1$$

defines a map `dme-enc` $: \mathbb{F}_q^8 \to \mathbb{F}_q^8$.

Let $D \subseteq \mathbb{F}_q^8$ be the set of $x \in \mathbb{F}_q^8$ such that

$$\begin{aligned}
&(\overline{\phi}^{-1} \circ L_1)(x), \\
&(\overline{\phi}^{-1} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x), \\
&(\overline{\phi}^{-1} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x)
\end{aligned}$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry. Let $E =$ `dme-enc`$(D) \subseteq \mathbb{F}_q^8$. By construction, the restriction `dme-enc` $: D \to E$ is a bijection.

Lemma 1.2. $|D| \geq 3(q^2-1)^4 - 2q^8 \geq q^8 - 12q^6$. *In particular, the probability that a randomly chosen* $x \in \mathbb{F}_q^8$ *(with a uniform distribution) does not belong to* D *is at most* $12q^{-2} < 2^{-92}$.

The main property of the map `dme-enc` is that it can be given by polynomials (this fact can be proven by following the sequence of maps that define `dme-enc`, starting with 8 variables $x_1, \dots, x_8$). More precisely, there exists $p_1, \dots, p_8 \in \mathbb{F}_q[x_1, \dots, x_8]$ such that

$$\texttt{dme-enc} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} p_1(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_2(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_3(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_4(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_5(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_6(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_7(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_8(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \end{bmatrix}$$

where p_1, p_2, p_7, p_8 having 65 monomials each and p_3, p_4, p_5, p_6 having 25 monomials each.

Define the integers $f_0, \dots, f_{15} \in [0, 47]$ as

$$\begin{aligned}
f_0 &= a_0 + b_0 + c_0 \bmod 48 \\
f_1 &= a_1 + b_2 + c_2 \bmod 48 \\
f_2 &= a_1 + b_2 + c_4 \bmod 48 \\
f_3 &= a_1 + b_2 + c_6 \bmod 48 \\
f_4 &= a_2 + a_0 + b_0 - a_1 + c_0 \bmod 48 \\
f_5 &= a_2 + b_2 + c_2 \bmod 48 \\
f_6 &= a_2 + b_2 + c_4 \bmod 48 \\
f_7 &= a_2 + b_2 + c_6 \bmod 48 \\
f_8 &= a_4 + b_5 + c_1 \bmod 48 \\
f_9 &= a_4 + b_5 + c_3 \bmod 48 \\
f_{10} &= a_4 + b_5 + c_5 \bmod 48 \\
f_{11} &= a_3 + b_3 + c_7 \bmod 48 \\
f_{12} &= a_5 + b_5 + c_1 \bmod 48 \\
f_{13} &= a_5 + b_5 + c_3 \bmod 48 \\
f_{14} &= a_5 + b_5 + c_5 \bmod 48 \\
f_{15} &= a_5 + a_3 + b_3 - a_4 + c_7 \bmod 48
\end{aligned}$$

and consider the expressions

$$\begin{array}{llll}
z_0 = x_1^{2^{f_0}} & z_1 = x_1^{2^{f_1}} & z_2 = x_1^{2^{f_2}} & z_3 = x_1^{2^{f_3}} \\
z_4 = x_2^{2^{f_0}} & z_5 = x_2^{2^{f_1}} & z_6 = x_2^{2^{f_2}} & z_7 = x_1^{2^{f_3}} \\
z_8 = x_3^{2^{f_4}} & z_9 = x_3^{2^{f_5}} & z_{10} = x_3^{2^{f_6}} & z_{11} = x_3^{2^{f_7}} \\
z_{12} = x_4^{2^{f_4}} & z_{13} = x_4^{2^{f_5}} & z_{14} = x_4^{2^{f_6}} & z_{15} = x_4^{2^{f_7}} \\
z_{16} = x_5^{2^{f_8}} & z_{17} = x_5^{2^{f_9}} & z_{18} = x_5^{2^{f_{10}}} & z_{19} = x_5^{2^{f_{11}}} \\
z_{20} = x_6^{2^{f_8}} & z_{21} = x_6^{2^{f_9}} & z_{22} = x_6^{2^{f_{10}}} & z_{23} = x_6^{2^{f_{11}}} \\
z_{24} = x_7^{2^{f_{12}}} & z_{25} = x_7^{2^{f_{13}}} & z_{26} = x_7^{2^{f_{14}}} & z_{27} = x_7^{2^{f_{15}}} \\
z_{28} = x_8^{2^{f_{12}}} & z_{29} = x_8^{2^{f_{13}}} & z_{30} = x_8^{2^{f_{14}}} & z_{31} = x_8^{2^{f_{15}}}
\end{array}$$

A careful study of p_1 and p_2 show that the 65 monomials are exactly

$$\begin{array}{lll}
m_{1,1} = z_{24}z_{16}z_8z_0^2 & m_{1,2} = z_{28}z_{16}z_8z_0^2 & m_{1,3} = z_{24}z_{20}z_8z_0^2 \\
m_{1,4} = z_{28}z_{20}z_8z_0^2 & m_{1,5} = z_8z_0^2 & m_{1,6} = z_{24}z_{16}z_{12}z_0^2 \\
m_{1,7} = z_{28}z_{16}z_{12}z_0^2 & m_{1,8} = z_{24}z_{20}z_{12}z_0^2 & m_{1,9} = z_{28}z_{20}z_{12}z_0^2 \\
m_{1,10} = z_{12}z_0^2 & m_{1,11} = z_{24}z_{16}z_8z_4z_0 & m_{1,12} = z_{28}z_{16}z_8z_4z_0 \\
m_{1,13} = z_{24}z_{20}z_8z_4z_0 & m_{1,14} = z_{28}z_{20}z_8z_4z_0 & m_{1,15} = z_8z_4z_0 \\
m_{1,16} = z_{24}z_{16}z_{12}z_4z_0 & m_{1,17} = z_{28}z_{16}z_{12}z_4z_0 & m_{1,18} = z_{24}z_{20}z_{12}z_4z_0 \\
m_{1,19} = z_{28}z_{20}z_{12}z_4z_0 & m_{1,20} = z_{12}z_4z_0 & m_{1,21} = z_{24}z_{16}z_0 \\
m_{1,22} = z_{28}z_{16}z_0 & m_{1,23} = z_{24}z_{20}z_0 & m_{1,24} = z_{28}z_{20}z_0 \\
m_{1,25} = z_0 & m_{1,26} = z_{24}z_{16}z_8z_4^2 & m_{1,27} = z_{28}z_{16}z_8z_4^2 \\
m_{1,28} = z_{24}z_{20}z_8z_4^2 & m_{1,29} = z_{28}z_{20}z_8z_4^2 & m_{1,30} = z_8z_4^2 \\
m_{1,31} = z_{24}z_{16}z_{12}z_4^2 & m_{1,32} = z_{28}z_{16}z_{12}z_4^2 & m_{1,33} = z_{24}z_{20}z_{12}z_4^2 \\
m_{1,34} = z_{28}z_{20}z_{12}z_4^2 & m_{1,35} = z_{12}z_4^2 & m_{1,36} = z_{24}z_{16}z_4 \\
m_{1,37} = z_{28}z_{16}z_4 & m_{1,38} = z_{24}z_{20}z_4 & m_{1,39} = z_{28}z_{20}z_4 \\
m_{1,40} = z_4 & m_{1,41} = z_{24}z_{16}z_8z_0 & m_{1,42} = z_{28}z_{16}z_8z_0 \\
m_{1,43} = z_{24}z_{20}z_8z_0 & m_{1,44} = z_{28}z_{20}z_8z_0 & m_{1,45} = z_8z_0 \\
m_{1,46} = z_{24}z_{16}z_{12}z_0 & m_{1,47} = z_{28}z_{16}z_{12}z_0 & m_{1,48} = z_{24}z_{20}z_{12}z_0 \\
m_{1,49} = z_{28}z_{20}z_{12}z_0 & m_{1,50} = z_{12}z_0 & m_{1,51} = z_{24}z_{16}z_8z_4 \\
m_{1,52} = z_{28}z_{16}z_8z_4 & m_{1,53} = z_{24}z_{20}z_8z_4 & m_{1,54} = z_{28}z_{20}z_8z_4 \\
m_{1,55} = z_8z_4 & m_{1,56} = z_{24}z_{16}z_{12}z_4 & m_{1,57} = z_{28}z_{16}z_{12}z_4 \\
m_{1,58} = z_{24}z_{20}z_{12}z_4 & m_{1,59} = z_{28}z_{20}z_{12}z_4 & m_{1,60} = z_{12}z_4 \\
m_{1,61} = z_{24}z_{16} & m_{1,62} = z_{28}z_{16} & m_{1,63} = z_{24}z_{20} \\
m_{1,64} = z_{28}z_{20} & m_{1,65} = 1 &
\end{array}$$

Similarly, the 25 monomials that appear in p_3 and p_4 are

$$\begin{array}{lll}
m_{2,1} = z_{25}z_{17}z_9z_1 & m_{2,2} = z_{29}z_{17}z_9z_1 & m_{2,3} = z_{25}z_{21}z_9z_1 \\
m_{2,4} = z_{29}z_{21}z_9z_1 & m_{2,5} = z_9z_1 & m_{2,6} = z_{25}z_{17}z_{13}z_1 \\
m_{2,7} = z_{29}z_{17}z_{13}z_1 & m_{2,8} = z_{25}z_{21}z_{13}z_1 & m_{2,9} = z_{29}z_{21}z_{13}z_1 \\
m_{2,10} = z_{13}z_1 & m_{2,11} = z_{25}z_{17}z_9z_5 & m_{2,12} = z_{29}z_{17}z_9z_5 \\
m_{2,13} = z_{25}z_{21}z_9z_5 & m_{2,14} = z_{29}z_{21}z_9z_5 & m_{2,15} = z_9z_5 \\
m_{2,16} = z_{25}z_{17}z_{13}z_5 & m_{2,17} = z_{29}z_{17}z_{13}z_5 & m_{2,18} = z_{25}z_{21}z_{13}z_5 \\
m_{2,19} = z_{29}z_{21}z_{13}z_5 & m_{2,20} = z_{13}z_5 & m_{2,21} = z_{25}z_{17} \\
m_{2,22} = z_{29}z_{17} & m_{2,23} = z_{25}z_{21} & m_{2,24} = z_{29}z_{21} \\
m_{2,25} = 1 & &
\end{array}$$

the 25 monomials that appear in p_5 and p_6 are

$$
\begin{array}{lll}
m_{3,1} = z_{26}z_{18}z_{10}z_2 & m_{3,2} = z_{30}z_{18}z_{10}z_2 & m_{3,3} = z_{26}z_{22}z_{10}z_2 \\
m_{3,4} = z_{30}z_{22}z_{10}z_2 & m_{3,5} = z_{10}z_2 & m_{3,6} = z_{26}z_{18}z_{14}z_2 \\
m_{3,7} = z_{30}z_{18}z_{14}z_2 & m_{3,8} = z_{26}z_{22}z_{14}z_2 & m_{3,9} = z_{30}z_{22}z_{14}z_2 \\
m_{3,10} = z_{14}z_2 & m_{3,11} = z_{26}z_{18}z_{10}z_6 & m_{3,12} = z_{30}z_{18}z_{10}z_6 \\
m_{3,13} = z_{26}z_{22}z_{10}z_6 & m_{3,14} = z_{30}z_{22}z_{10}z_6 & m_{3,15} = z_{10}z_6 \\
m_{3,16} = z_{26}z_{18}z_{14}z_6 & m_{3,17} = z_{30}z_{18}z_{14}z_6 & m_{3,18} = z_{26}z_{22}z_{14}z_6 \\
m_{3,19} = z_{30}z_{22}z_{14}z_6 & m_{3,20} = z_{14}z_6 & m_{3,21} = z_{26}z_{18} \\
m_{3,22} = z_{30}z_{18} & m_{3,23} = z_{26}z_{22} & m_{3,24} = z_{30}z_{22} \\
m_{3,25} = 1 & &
\end{array}
$$

and the 65 monomials that appear in p_7 and p_8 are

$$
\begin{array}{lll}
m_{4,1} = z_{27}z_{19^2}z_{11}z_3 & m_{4,2} = z_{31}z_{19^2}z_{11}z_3 & m_{4,3} = z_{27}z_{23}z_{19}z_{11}z_3 \\
m_{4,4} = z_{31}z_{23}z_{19}z_{11}z_3 & m_{4,5} = z_{19}z_{11}z_3 & m_{4,6} = z_{27}z_{23^2}z_{11}z_3 \\
m_{4,7} = z_{31}z_{23^2}z_{11}z_3 & m_{4,8} = z_{23}z_{11}z_3 & m_{4,9} = z_{27}z_{19}z_{11}z_3 \\
m_{4,10} = z_{31}z_{19}z_{11}z_3 & m_{4,11} = z_{27}z_{23}z_{11}z_3 & m_{4,12} = z_{31}z_{23}z_{11}z_3 \\
m_{4,13} = z_{11}z_3 & m_{4,14} = z_{27}z_{19^2}z_{15}z_3 & m_{4,15} = z_{31}z_{19^2}z_{15}z_3 \\
m_{4,16} = z_{27}z_{23}z_{19}z_{15}z_3 & m_{4,17} = z_{31}z_{23}z_{19}z_{15}z_3 & m_{4,18} = z_{19}z_{15}z_3 \\
m_{4,19} = z_{27}z_{23^2}z_{15}z_3 & m_{4,20} = z_{31}z_{23^2}z_{15}z_3 & m_{4,21} = z_{23}z_{15}z_3 \\
m_{4,22} = z_{27}z_{19}z_{15}z_3 & m_{4,23} = z_{31}z_{19}z_{15}z_3 & m_{4,24} = z_{27}z_{23}z_{15}z_3 \\
m_{4,25} = z_{31}z_{23}z_{15}z_3 & m_{4,26} = z_{15}z_3 & m_{4,27} = z_{27}z_{19^2}z_{11}z_7 \\
m_{4,28} = z_{31}z_{19^2}z_{11}z_7 & m_{4,29} = z_{27}z_{23}z_{19}z_{11}z_7 & m_{4,30} = z_{31}z_{23}z_{19}z_{11}z_7 \\
m_{4,31} = z_{19}z_{11}z_7 & m_{4,32} = z_{27}z_{23^2}z_{11}z_7 & m_{4,33} = z_{31}z_{23^2}z_{11}z_7 \\
m_{4,34} = z_{23}z_{11}z_7 & m_{4,35} = z_{27}z_{19}z_{11}z_7 & m_{4,36} = z_{31}z_{19}z_{11}z_7 \\
m_{4,37} = z_{27}z_{23}z_{11}z_7 & m_{4,38} = z_{31}z_{23}z_{11}z_7 & m_{4,39} = z_{11}z_7 \\
m_{4,40} = z_{27}z_{19^2}z_{15}z_7 & m_{4,41} = z_{31}z_{19^2}z_{15}z_7 & m_{4,42} = z_{27}z_{23}z_{19}z_{15}z_7 \\
m_{4,43} = z_{31}z_{23}z_{19}z_{15}z_7 & m_{4,44} = z_{19}z_{15}z_7 & m_{4,45} = z_{27}z_{23^2}z_{15}z_7 \\
m_{4,46} = z_{31}z_{23^2}z_{15}z_7 & m_{4,47} = z_{23}z_{15}z_7 & m_{4,48} = z_{27}z_{19}z_{15}z_7 \\
m_{4,49} = z_{31}z_{19}z_{15}z_7 & m_{4,50} = z_{27}z_{23}z_{15}z_7 & m_{4,51} = z_{31}z_{23}z_{15}z_7 \\
m_{4,52} = z_{15}z_7 & m_{4,53} = z_{27}z_{19^2} & m_{4,54} = z_{31}z_{19^2} \\
m_{4,55} = z_{27}z_{23}z_{19} & m_{4,56} = z_{31}z_{23}z_{19} & m_{4,57} = z_{19} \\
m_{4,58} = z_{27}z_{23^2} & m_{4,59} = z_{31}z_{23^2} & m_{4,60} = z_{23} \\
m_{4,61} = z_{27}z_{19} & m_{4,62} = z_{31}z_{19} & m_{4,63} = z_{27}z_{23} \\
m_{4,64} = z_{31}z_{23} & m_{4,65} = 1 &
\end{array}
$$

Using the notation above, the polynomials $p_1, \dots, p_8$ can be written as

$$
\begin{array}{ll}
p_1 = \sum_{i=1}^{65} p_{1,i}m_{1,i} & p_2 = \sum_{i=1}^{65} p_{2,i}m_{1,i} \\
p_3 = \sum_{i=1}^{25} p_{3,i}m_{2,i} & p_4 = \sum_{i=1}^{25} p_{4,i}m_{2,i} \\
p_5 = \sum_{i=1}^{25} p_{5,i}m_{3,i} & p_6 = \sum_{i=1}^{25} p_{6,i}m_{3,i} \\
p_7 = \sum_{i=1}^{65} p_{7,i}m_{4,i} & p_8 = \sum_{i=1}^{65} p_{8,i}m_{4,i}
\end{array}
$$

and the public key is just these eight polynomials (which are encoded by the list of 360 coefficients and the values $f_0, \dots, f_{15}$).

Let M_1^{-1}, M_2^{-1}, and M_3^{-1} be the inverses of M_1, M_2, and M_3 modulo q^2-1, respectively, with their entries reduced to the interval $[0, q^2-1)$. Let $E_1^{-1}, E_2^{-1}, E_3^{-1} : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ the corresponding exponential maps and $\overline{E_1^{-1}}, \overline{E_2^{-1}}, \overline{E_3^{-1}} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ their extensions. The following composition

$$
L_1^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_1^{-1}} \circ \overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1}
$$

defines a map `dme-dec` $: \mathbb{F}_q^8 \to \mathbb{F}_q^8$. By construction, we have that `dme-dec` maps E to D and, restricted to those sets, is the inverse of `dme-enc`. It is easy to verify that E is exactly the set of $y \in \mathbb{F}_q^8$ such

that

$$(\overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y)$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry.

The cryptographic assumption in `DME-3rnds-8vars-48bits-sign` is that, for any $y \in E$, the system of eight polynomial equations in eight unknowns

$$\begin{aligned}
p_1(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_1 \\
p_2(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_2 \\
p_3(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_3 \\
p_4(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_4 \\
p_5(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_5 \\
p_6(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_6 \\
p_7(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_7 \\
p_8(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_8
\end{aligned}$$

is hard to solve. In particular, this implies that it is not feasible to compute a secret key corresponding to a given public key.

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{384}$ map of the `DME-3rnds-8vars-48bits-sign` scheme, as required by the API, returns (m, s) where m is the original message and the signature s is obtained by first applying a PSS-SHA3 padding (with 96 random bits), then reading the 384 bit sequence as a vector in $\mathbb{F}_q^8$, applying `dme-dec`, and lastly, interpreting the resulting vector as a 384 bit sequence. The `dme-open` $: \{0,1\}^* \times \{0,1\}^{384} \to \{0,1\}^* \cup \{error\}$ reverses the procedure above using `dme-enc` and checks that the signature is legitimate. The details of these algorithms are given in the next section.

2 Implementation details of DME-3rnds-8vars-48bits-sign

The field of $q = 2^{48}$ is implemented as the quotient ring

$$\mathbb{F}_q = \mathbb{F}_2[t]/\langle t^{48} + t^{17} + t^2 + t + 1\rangle,$$

and the monic irreducible polynomial $p(u) \in \mathbb{F}_q[u]$ that defines $\mathbb{F}_{q^2}$ is $p(u) = u^2 + tu + 1$, so we have

$$\mathbb{F}_{q^2} = \mathbb{F}_q[u]/\langle u^2 + tu + 1\rangle.$$

An element $\alpha = \alpha_{47}t^{47} + \cdots + \alpha_1 t + \alpha_0 \in \mathbb{F}_q$ can be interpreted as the 48 bits unsigned integer $\texttt{int}(\alpha) = \alpha_{47}2^{47} + \cdots + \alpha_1 2 + \alpha_0 \in [0, 2^{48} - 1]$. In C99, these fit comfortably in the `uint64_t` type of the standard library. When serialized into bytes, the little-endian convention is used for all integer types. In particular, the element α above, correspond with the sequence of 6 bytes

$$\left(\left\lfloor \frac{\texttt{int}(\alpha)}{2^{8i}} \right\rfloor \bmod 2^8 \right)$$

for $i = 0, 1, \ldots, 5$ in exactly this order. An element $\beta = \beta_0 + \beta_1 u \in \mathbb{F}_{q^2}$ is serialized as the 12 byte sequence obtained by serializing first β_0 and then β_1. Similarly, a matrix $\gamma \in \mathbb{F}_q^{2\times 2}$ is serialized as the 24 bytes sequence obtained by serializing γ_{11}, γ_{12}, γ_{21}, γ_{22} in that order.

The private key is $545 = 16 \cdot 24 + 24 \cdot 6 + 6 + 6 + 5$ bytes long, which correspond to the serialization of the the 16 matrices $L_{11}^{-1}, L_{12}^{-1}, \ldots, L_{44}^{-1}$, then the serialization of the 24 affine shifts $A_{21}, A_{22}, A_{31}, A_{32}, A_{41}, A_{42}, A_{23}, A_{24}, \ldots, A_{47}, A_{48} \in \mathbb{F}_q$, followed by a single byte for each $a_0, \ldots, a_5$,

$b_0, \ldots, b_5, c_0, c_2, c_3, c_5, c_6$. The coefficients c_1, c_4 and c_7 are not serialized since they can be recovered from the other values.

The public key is $2169 = 360 \cdot 6 + 9$ bytes long, which correspond to the serialization of the coefficients of $p_1, p_2, \ldots, p_8$ followed by a single byte for each $f_0, f_1, f_3, f_5, f_8, f_9, f_{10}, f_{11}, f_{12}$. The values of $f_2, f_4, f_6, f_7, f_{13}, f_{14}, f_{15}$ are not serialized since they can be computed from the other values by

$$\begin{aligned}
f_2 &= (f_1 + f_{10} - f_9 + 17) \bmod 48 \\
f_4 &= (f_0 + f_5 - f_1) \bmod 48 \\
f_6 &= (f_5 + f_2 - f_1) \bmod 48 \\
f_7 &= (f_5 + f_3 - f_1) \bmod 48 \\
f_{13} &= (f_{12} + f_9 - f_8) \bmod 48 \\
f_{14} &= (f_{12} + f_{10} - f_8) \bmod 48 \\
f_{15} &= (f_{11} + f_{12} - f_8) \bmod 48
\end{aligned}$$

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{384}$ map (the secret key is implicit here) is computed by the following procedure:

1. let $msg \in \{0,1\}^*$ be the input message,
2. choose $r \in \{0,1\}^{96}$ at random,
3. compute $w = \mathtt{SHA3}(msg||r) \in \{0,1\}^{192}$,
4. compute $g = \mathtt{SHA3}(w) \oplus (r||0) \in \{0,1\}^{192}$,
5. compute $s = \mathtt{dme\text{-}dec}(w||g) \in \mathbb{F}_q^8 \simeq \{0,1\}^{384}$,
6. return (msg, s).

This function is implemented in C99 as `crypto_sign`, with the only difference that the return value is $msg||s$ instead of (msg, s).

The `dme-open` $: \{0,1\}^* \times \{0,1\}^{384} \to \{0,1\}^* \cup \{error\}$ map (the public key is implicit here) is computed as follows:

1. let $(msg, s) \in \{0,1\}^* \times \{0,1\}^{384}$ be the input message and its corresponding signature,
2. compute $w \in \{0,1\}^{192}$ and $g \in \{0,1\}^{192}$ as $w||g = \mathtt{dme\text{-}enc}(s)$,
3. compute $r \in \{0,1\}^{96}$ as the first 96 bits of $\mathtt{SHA3}(w) \oplus g$,
4. if $w \neq \mathtt{SHA3}(msg||r)$, return $error$,
5. otherwise, return the original message msg.

This function is implemented in C99 as `crypto_sign_open`, but the two separate arguments for the message msg and the signature s, the function takes only one with the concatenation of both $msg||s$.

The function `dme-keypair`, which corresponds in the C99 implementation with `crypto_sign_keypair` creates 16 random matrices in $\mathbb{F}_q^{2\times 2}$, 4 random shifts in $\mathbb{F}_q^8$ and random values for $a_0, \ldots, c_7 \in [0, 95]$ satisfying the restrictions explained in the previous section (for instance, the matrices have to be invertible). With the secret key already chosen, the public key is computed by operating with 8 (symbolic) polynomials until $p_1, \ldots, p_8 \in \mathbb{F}_q[x_1, \ldots, x_8]$ is obtained. Then both keys are serialized and returned.

3 Timings

On a laptop with a Intel(R) Core(TM) i7-8565U CPU at 1.80GHz, with 8 Gb of RAM, running a Linux Mint 21 x86_64 operating system, the performance of the API primitives (for message of 200 bytes) is given in the following table:

`dme-keypair`	262 usec
`dme-sign`	35 usec
`dme-open`	11 usec

The length of the private key is 545 bytes and the length of the public key is 2169 bytes.

Implementation of DME-3rnds-8vars-64bits-sign

Ignacio Luengo*[1], Martín Avendaño†[1], and Pilar Coscojuela‡[1]

[1]Universidad Complutense de Madrid

June 23, 2023

The `DME-3rnds-8vars-64bits-sign` is a signature scheme based on the composition of three different types of polynomial maps $\mathbb{F}_{2^{64}}^8 \to \mathbb{F}_{2^{64}}^8$ that are bijective almost everywhere: linear maps, affine shifts, and exponential maps. The individual maps form the secret key, and the composition of the maps, which is given by eight polynomials in $\mathbb{F}_{2^{64}}[x_1, \ldots, x_8]$ is the public key. The signature is obtained by mapping the message to $\mathbb{F}_{2^{64}}^8$ using a hash function (and a PSS padding with 256 random bits) and then applying the decryption map to get a signature of 512 bits (64 bytes).

1 Mathematical description of DME-3rnds-8vars-64bits-sign

Let $q = 2^{64}$ and let $\mathbb{F}_q$ be a finite field with q elements. Consider an irreducible monic polinomial $p(u) = u^2 + p_1 u + p_0 \in \mathbb{F}_q[u]$. The quotient ring $\mathbb{F}_q[u]/\langle p(u)\rangle$ defines a field of q^2 elements, which we denote $\mathbb{F}_{q^2}$. The map $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ given by

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto x + yu$$

is a bijection. This map can be extended naturally to a map $\overline{\phi} : \mathbb{F}_q^8 \to (\mathbb{F}_{q^2})^4$

$$\overline{\phi} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} \phi \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ \phi \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ \phi \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ \phi \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

which is also a bijection.

For any matrix $M \in \mathbb{Z}^{4\times 4}$, we define the exponential map $E_M : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ given by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \begin{bmatrix} x_1^{m_{11}} x_2^{m_{12}} x_3^{m_{13}} x_4^{m_{14}} \\ x_1^{m_{21}} x_2^{m_{22}} x_3^{m_{23}} x_4^{m_{24}} \\ x_1^{m_{31}} x_2^{m_{32}} x_3^{m_{33}} x_4^{m_{34}} \\ x_1^{m_{41}} x_2^{m_{42}} x_3^{m_{43}} x_4^{m_{44}} \end{bmatrix}.$$

The following result summarizes the properties of the exponential maps that are needed for the `DME-3rnds-8vars-64bits-sign` cryptosystem.

*iluengo@ucm.es
†mavend01@ucm.es
‡picoscoj@ucm.es

Lemma 1.1. *Let $M_1, M_2 \in \mathbb{Z}^{4\times 4}$. Then:*

1. $E_{M_1} \circ E_{M_2} = E_{M_1 \cdot M_2}$.
2. $M_1 \equiv M_2 \pmod{q^2-1} \Rightarrow E_{M_1} = E_{M_2}$.
3. $M_1 \cdot M_2 \equiv \mathrm{Id} \pmod{q^2-1} \Rightarrow E_{M_1} \circ E_{M_2} = \mathrm{Id}$.
4. $\gcd(\det(M_1), q^2-1) = 1 \Rightarrow E_{M_1}$ *is invertible.*

If no entry of the matrix M is negative, then E_M can be extended to a map $\overline{E_M} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ with the same formula and setting $0^0 = 1$. It should be noted that the extended maps $\overline{E_M}$ fail in general to be bijections, even if $\gcd(\det(M), q^2-1) = 1$.

In `DME-3rnds-8vars-64bits-sign`, we have three exponential maps E_1, E_2 and E_3, whose matrices are

$$M_1 = \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix},$$

respectively, with $a_0, \ldots, a_5, b_0, \ldots, b_5, c_0, \ldots, c_7 \in [0, 127]$ such that

$$\begin{aligned} c_1 &\equiv a_0 + b_0 + c_0 - a_1 - b_2 \pmod{128}, \\ c_7 &\equiv a_3 + b_4 + c_6 - a_4 - b_5 \pmod{128}, \\ c_4 &\equiv c_2 + c_5 - c_3 + 57 \pmod{128}. \end{aligned}$$

It is easy to verify that the three matrices M_1, M_2 and M_3 satisfy condition 4 of lemma 1.1.

In `DME-3rnds-8vars-64bits-sign`, we also needs four invertible linear maps $L_1, L_2, L_3, L_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$, each of which has a four 2×2 block structure

$$L_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} L_{i1} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ L_{i2} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \\ L_{i3} \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \\ L_{i4} \begin{bmatrix} x_7 \\ x_8 \end{bmatrix} \end{bmatrix}$$

with $L_{ij} \in \mathbb{F}_q^{2\times 2}$ and $\det(L_{ij}) \neq 0$.

In addition to the linear maps, we have three affine shifts $A_2, A_3, A_4 : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ given by

$$A_i \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} x_1 + A_{i1} \\ x_2 + A_{i2} \\ x_3 + A_{i3} \\ x_4 + A_{i4} \\ x_5 + A_{i5} \\ x_6 + A_{i6} \\ x_7 + A_{i7} \\ x_8 + A_{i8} \end{bmatrix}$$

with $A_{ij} \in \mathbb{F}_q$.

The secret key consists of the four linear maps L_1, L_2, L_3, L_4, the three affine shifts A_2, A_3, A_4 and the three exponential maps E_1, E_2, E_3. The following composition

$$A_4 \circ L_4 \circ \overline{\phi}^{-1} \circ \overline{E_3} \circ \overline{\phi} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1$$

defines a map $\texttt{dme-enc} : \mathbb{F}_q^8 \to \mathbb{F}_q^8$.

Let $D \subseteq \mathbb{F}_q^8$ be the set of $x \in \mathbb{F}_q^8$ such that

$$\begin{aligned}
&(\overline{\phi}^{-1} \circ L_1)(x), \\
&(\overline{\phi}^{-1} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x), \\
&(\overline{\phi}^{-1} \circ A_3 \circ L_3 \circ \overline{\phi}^{-1} \circ \overline{E_2} \circ \overline{\phi} \circ A_2 \circ L_2 \circ \overline{\phi}^{-1} \circ \overline{E_1} \circ \overline{\phi} \circ L_1)(x)
\end{aligned}$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry. Let $E = \texttt{dme-enc}(D) \subseteq \mathbb{F}_q^8$. By construction, the restriction $\texttt{dme-enc} : D \to E$ is a bijection.

Lemma 1.2. $|D| \geq 3(q^2-1)^4 - 2q^8 \geq q^8 - 12q^6$. *In particular, the probability that a randomly chosen* $x \in \mathbb{F}_q^8$ *(with a uniform distribution) does not belong to* D *is at most* $12q^{-2} < 2^{-124}$.

The main property of the map `dme-enc` is that it can be given by polynomials (this fact can be proven by following the sequence of maps that define `dme-enc`, starting with 8 variables $x_1, \ldots, x_8$). More precisely, there exists $p_1, \ldots, p_8 \in \mathbb{F}_q[x_1, \ldots, x_8]$ such that

$$\texttt{dme-enc} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} p_1(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_2(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_3(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_4(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_5(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_6(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_7(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \\ p_8(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \end{bmatrix}$$

where p_1, p_2, p_7, p_8 having 65 monomials each and p_3, p_4, p_5, p_6 having 25 monomials each.

Define the integers $f_0, \ldots, f_{15} \in [0, 63]$ as

$$\begin{aligned}
f_0 &= a_0 + b_0 + c_0 \bmod 64 \\
f_1 &= a_1 + b_2 + c_2 \bmod 64 \\
f_2 &= a_1 + b_2 + c_4 \bmod 64 \\
f_3 &= a_1 + b_2 + c_6 \bmod 64 \\
f_4 &= a_2 + a_0 + b_0 - a_1 + c_0 \bmod 64 \\
f_5 &= a_2 + b_2 + c_2 \bmod 64 \\
f_6 &= a_2 + b_2 + c_4 \bmod 64 \\
f_7 &= a_2 + b_2 + c_6 \bmod 64 \\
f_8 &= a_4 + b_5 + c_1 \bmod 64 \\
f_9 &= a_4 + b_5 + c_3 \bmod 64 \\
f_{10} &= a_4 + b_5 + c_5 \bmod 64 \\
f_{11} &= a_3 + b_3 + c_7 \bmod 64 \\
f_{12} &= a_5 + b_5 + c_1 \bmod 64 \\
f_{13} &= a_5 + b_5 + c_3 \bmod 64 \\
f_{14} &= a_5 + b_5 + c_5 \bmod 64 \\
f_{15} &= a_5 + a_3 + b_3 - a_4 + c_7 \bmod 64
\end{aligned}$$

and consider the expressions

$$\begin{array}{llll}
z_0 = x_1^{2^{f_0}} & z_1 = x_1^{2^{f_1}} & z_2 = x_1^{2^{f_2}} & z_3 = x_1^{2^{f_3}} \\
z_4 = x_2^{2^{f_0}} & z_5 = x_2^{2^{f_1}} & z_6 = x_2^{2^{f_2}} & z_7 = x_1^{2^{f_3}} \\
z_8 = x_3^{2^{f_4}} & z_9 = x_3^{2^{f_5}} & z_{10} = x_3^{2^{f_6}} & z_{11} = x_3^{2^{f_7}} \\
z_{12} = x_4^{2^{f_4}} & z_{13} = x_4^{2^{f_5}} & z_{14} = x_4^{2^{f_6}} & z_{15} = x_4^{2^{f_7}} \\
z_{16} = x_5^{2^{f_8}} & z_{17} = x_5^{2^{f_9}} & z_{18} = x_5^{2^{f_{10}}} & z_{19} = x_5^{2^{f_{11}}} \\
z_{20} = x_6^{2^{f_8}} & z_{21} = x_6^{2^{f_9}} & z_{22} = x_6^{2^{f_{10}}} & z_{23} = x_6^{2^{f_{11}}} \\
z_{24} = x_7^{2^{f_{12}}} & z_{25} = x_7^{2^{f_{13}}} & z_{26} = x_7^{2^{f_{14}}} & z_{27} = x_7^{2^{f_{15}}} \\
z_{28} = x_8^{2^{f_{12}}} & z_{29} = x_8^{2^{f_{13}}} & z_{30} = x_8^{2^{f_{14}}} & z_{31} = x_8^{2^{f_{15}}}
\end{array}$$

A careful study of p_1 and p_2 show that the 65 monomials are exactly

$$\begin{array}{lll}
m_{1,1} = z_{24}z_{16}z_8z_0^2 & m_{1,2} = z_{28}z_{16}z_8z_0^2 & m_{1,3} = z_{24}z_{20}z_8z_0^2 \\
m_{1,4} = z_{28}z_{20}z_8z_0^2 & m_{1,5} = z_8z_0^2 & m_{1,6} = z_{24}z_{16}z_{12}z_0^2 \\
m_{1,7} = z_{28}z_{16}z_{12}z_0^2 & m_{1,8} = z_{24}z_{20}z_{12}z_0^2 & m_{1,9} = z_{28}z_{20}z_{12}z_0^2 \\
m_{1,10} = z_{12}z_0^2 & m_{1,11} = z_{24}z_{16}z_8z_4z_0 & m_{1,12} = z_{28}z_{16}z_8z_4z_0 \\
m_{1,13} = z_{24}z_{20}z_8z_4z_0 & m_{1,14} = z_{28}z_{20}z_8z_4z_0 & m_{1,15} = z_8z_4z_0 \\
m_{1,16} = z_{24}z_{16}z_{12}z_4z_0 & m_{1,17} = z_{28}z_{16}z_{12}z_4z_0 & m_{1,18} = z_{24}z_{20}z_{12}z_4z_0 \\
m_{1,19} = z_{28}z_{20}z_{12}z_4z_0 & m_{1,20} = z_{12}z_4z_0 & m_{1,21} = z_{24}z_{16}z_0 \\
m_{1,22} = z_{28}z_{16}z_0 & m_{1,23} = z_{24}z_{20}z_0 & m_{1,24} = z_{28}z_{20}z_0 \\
m_{1,25} = z_0 & m_{1,26} = z_{24}z_{16}z_8z_4^2 & m_{1,27} = z_{28}z_{16}z_8z_4^2 \\
m_{1,28} = z_{24}z_{20}z_8z_4^2 & m_{1,29} = z_{28}z_{20}z_8z_4^2 & m_{1,30} = z_8z_4^2 \\
m_{1,31} = z_{24}z_{16}z_{12}z_4^2 & m_{1,32} = z_{28}z_{16}z_{12}z_4^2 & m_{1,33} = z_{24}z_{20}z_{12}z_4^2 \\
m_{1,34} = z_{28}z_{20}z_{12}z_4^2 & m_{1,35} = z_{12}z_4^2 & m_{1,36} = z_{24}z_{16}z_4 \\
m_{1,37} = z_{28}z_{16}z_4 & m_{1,38} = z_{24}z_{20}z_4 & m_{1,39} = z_{28}z_{20}z_4 \\
m_{1,40} = z_4 & m_{1,41} = z_{24}z_{16}z_8z_0 & m_{1,42} = z_{28}z_{16}z_8z_0 \\
m_{1,43} = z_{24}z_{20}z_8z_0 & m_{1,44} = z_{28}z_{20}z_8z_0 & m_{1,45} = z_8z_0 \\
m_{1,46} = z_{24}z_{16}z_{12}z_0 & m_{1,47} = z_{28}z_{16}z_{12}z_0 & m_{1,48} = z_{24}z_{20}z_{12}z_0 \\
m_{1,49} = z_{28}z_{20}z_{12}z_0 & m_{1,50} = z_{12}z_0 & m_{1,51} = z_{24}z_{16}z_8z_4 \\
m_{1,52} = z_{28}z_{16}z_8z_4 & m_{1,53} = z_{24}z_{20}z_8z_4 & m_{1,54} = z_{28}z_{20}z_8z_4 \\
m_{1,55} = z_8z_4 & m_{1,56} = z_{24}z_{16}z_{12}z_4 & m_{1,57} = z_{28}z_{16}z_{12}z_4 \\
m_{1,58} = z_{24}z_{20}z_{12}z_4 & m_{1,59} = z_{28}z_{20}z_{12}z_4 & m_{1,60} = z_{12}z_4 \\
m_{1,61} = z_{24}z_{16} & m_{1,62} = z_{28}z_{16} & m_{1,63} = z_{24}z_{20} \\
m_{1,64} = z_{28}z_{20} & m_{1,65} = 1 &
\end{array}$$

Similarly, the 25 monomials that appear in p_3 and p_4 are

$$\begin{array}{lll}
m_{2,1} = z_{25}z_{17}z_9z_1 & m_{2,2} = z_{29}z_{17}z_9z_1 & m_{2,3} = z_{25}z_{21}z_9z_1 \\
m_{2,4} = z_{29}z_{21}z_9z_1 & m_{2,5} = z_9z_1 & m_{2,6} = z_{25}z_{17}z_{13}z_1 \\
m_{2,7} = z_{29}z_{17}z_{13}z_1 & m_{2,8} = z_{25}z_{21}z_{13}z_1 & m_{2,9} = z_{29}z_{21}z_{13}z_1 \\
m_{2,10} = z_{13}z_1 & m_{2,11} = z_{25}z_{17}z_9z_5 & m_{2,12} = z_{29}z_{17}z_9z_5 \\
m_{2,13} = z_{25}z_{21}z_9z_5 & m_{2,14} = z_{29}z_{21}z_9z_5 & m_{2,15} = z_9z_5 \\
m_{2,16} = z_{25}z_{17}z_{13}z_5 & m_{2,17} = z_{29}z_{17}z_{13}z_5 & m_{2,18} = z_{25}z_{21}z_{13}z_5 \\
m_{2,19} = z_{29}z_{21}z_{13}z_5 & m_{2,20} = z_{13}z_5 & m_{2,21} = z_{25}z_{17} \\
m_{2,22} = z_{29}z_{17} & m_{2,23} = z_{25}z_{21} & m_{2,24} = z_{29}z_{21} \\
m_{2,25} = 1 & &
\end{array}$$

the 25 monomials that appear in p_5 and p_6 are

$$\begin{array}{lll}
m_{3,1} = z_{26}z_{18}z_{10}z_2 & m_{3,2} = z_{30}z_{18}z_{10}z_2 & m_{3,3} = z_{26}z_{22}z_{10}z_2 \\
m_{3,4} = z_{30}z_{22}z_{10}z_2 & m_{3,5} = z_{10}z_2 & m_{3,6} = z_{26}z_{18}z_{14}z_2 \\
m_{3,7} = z_{30}z_{18}z_{14}z_2 & m_{3,8} = z_{26}z_{22}z_{14}z_2 & m_{3,9} = z_{30}z_{22}z_{14}z_2 \\
m_{3,10} = z_{14}z_2 & m_{3,11} = z_{26}z_{18}z_{10}z_6 & m_{3,12} = z_{30}z_{18}z_{10}z_6 \\
m_{3,13} = z_{26}z_{22}z_{10}z_6 & m_{3,14} = z_{30}z_{22}z_{10}z_6 & m_{3,15} = z_{10}z_6 \\
m_{3,16} = z_{26}z_{18}z_{14}z_6 & m_{3,17} = z_{30}z_{18}z_{14}z_6 & m_{3,18} = z_{26}z_{22}z_{14}z_6 \\
m_{3,19} = z_{30}z_{22}z_{14}z_6 & m_{3,20} = z_{14}z_6 & m_{3,21} = z_{26}z_{18} \\
m_{3,22} = z_{30}z_{18} & m_{3,23} = z_{26}z_{22} & m_{3,24} = z_{30}z_{22} \\
m_{3,25} = 1 & &
\end{array}$$

and the 65 monomials that appear in p_7 and p_8 are

$$\begin{array}{lll}
m_{4,1} = z_{27}z_{19^2}z_{11}z_3 & m_{4,2} = z_{31}z_{19^2}z_{11}z_3 & m_{4,3} = z_{27}z_{23}z_{19}z_{11}z_3 \\
m_{4,4} = z_{31}z_{23}z_{19}z_{11}z_3 & m_{4,5} = z_{19}z_{11}z_3 & m_{4,6} = z_{27}z_{23^2}z_{11}z_3 \\
m_{4,7} = z_{31}z_{23^2}z_{11}z_3 & m_{4,8} = z_{23}z_{11}z_3 & m_{4,9} = z_{27}z_{19}z_{11}z_3 \\
m_{4,10} = z_{31}z_{19}z_{11}z_3 & m_{4,11} = z_{27}z_{23}z_{11}z_3 & m_{4,12} = z_{31}z_{23}z_{11}z_3 \\
m_{4,13} = z_{11}z_3 & m_{4,14} = z_{27}z_{19^2}z_{15}z_3 & m_{4,15} = z_{31}z_{19^2}z_{15}z_3 \\
m_{4,16} = z_{27}z_{23}z_{19}z_{15}z_3 & m_{4,17} = z_{31}z_{23}z_{19}z_{15}z_3 & m_{4,18} = z_{19}z_{15}z_3 \\
m_{4,19} = z_{27}z_{23^2}z_{15}z_3 & m_{4,20} = z_{31}z_{23^2}z_{15}z_3 & m_{4,21} = z_{23}z_{15}z_3 \\
m_{4,22} = z_{27}z_{19}z_{15}z_3 & m_{4,23} = z_{31}z_{19}z_{15}z_3 & m_{4,24} = z_{27}z_{23}z_{15}z_3 \\
m_{4,25} = z_{31}z_{23}z_{15}z_3 & m_{4,26} = z_{15}z_3 & m_{4,27} = z_{27}z_{19^2}z_{11}z_7 \\
m_{4,28} = z_{31}z_{19^2}z_{11}z_7 & m_{4,29} = z_{27}z_{23}z_{19}z_{11}z_7 & m_{4,30} = z_{31}z_{23}z_{19}z_{11}z_7 \\
m_{4,31} = z_{19}z_{11}z_7 & m_{4,32} = z_{27}z_{23^2}z_{11}z_7 & m_{4,33} = z_{31}z_{23^2}z_{11}z_7 \\
m_{4,34} = z_{23}z_{11}z_7 & m_{4,35} = z_{27}z_{19}z_{11}z_7 & m_{4,36} = z_{31}z_{19}z_{11}z_7 \\
m_{4,37} = z_{27}z_{23}z_{11}z_7 & m_{4,38} = z_{31}z_{23}z_{11}z_7 & m_{4,39} = z_{11}z_7 \\
m_{4,40} = z_{27}z_{19^2}z_{15}z_7 & m_{4,41} = z_{31}z_{19^2}z_{15}z_7 & m_{4,42} = z_{27}z_{23}z_{19}z_{15}z_7 \\
m_{4,43} = z_{31}z_{23}z_{19}z_{15}z_7 & m_{4,44} = z_{19}z_{15}z_7 & m_{4,45} = z_{27}z_{23^2}z_{15}z_7 \\
m_{4,46} = z_{31}z_{23^2}z_{15}z_7 & m_{4,47} = z_{23}z_{15}z_7 & m_{4,48} = z_{27}z_{19}z_{15}z_7 \\
m_{4,49} = z_{31}z_{19}z_{15}z_7 & m_{4,50} = z_{27}z_{23}z_{15}z_7 & m_{4,51} = z_{31}z_{23}z_{15}z_7 \\
m_{4,52} = z_{15}z_7 & m_{4,53} = z_{27}z_{19^2} & m_{4,54} = z_{31}z_{19^2} \\
m_{4,55} = z_{27}z_{23}z_{19} & m_{4,56} = z_{31}z_{23}z_{19} & m_{4,57} = z_{19} \\
m_{4,58} = z_{27}z_{23^2} & m_{4,59} = z_{31}z_{23^2} & m_{4,60} = z_{23} \\
m_{4,61} = z_{27}z_{19} & m_{4,62} = z_{31}z_{19} & m_{4,63} = z_{27}z_{23} \\
m_{4,64} = z_{31}z_{23} & m_{4,65} = 1 &
\end{array}$$

Using the notation above, the polynomials $p_1, \ldots, p_8$ can be written as

$$\begin{array}{ll}
p_1 = \sum_{i=1}^{65} p_{1,i}m_{1,i} & p_2 = \sum_{i=1}^{65} p_{2,i}m_{1,i} \\
p_3 = \sum_{i=1}^{25} p_{3,i}m_{2,i} & p_4 = \sum_{i=1}^{25} p_{4,i}m_{2,i} \\
p_5 = \sum_{i=1}^{25} p_{5,i}m_{3,i} & p_6 = \sum_{i=1}^{25} p_{6,i}m_{3,i} \\
p_7 = \sum_{i=1}^{65} p_{7,i}m_{4,i} & p_8 = \sum_{i=1}^{65} p_{8,i}m_{4,i}
\end{array}$$

and the public key is just these eight polynomials (which are encoded by the list of 360 coefficients and the values $f_0, \ldots, f_{15}$).

Let M_1^{-1}, M_2^{-1}, and M_3^{-1} be the inverses of M_1, M_2, and M_3 modulo $q^2 - 1$, respectively, with their entries reduced to the interval $[0, q^2 - 1)$. Let $E_1^{-1}, E_2^{-1}, E_3^{-1} : (\mathbb{F}_{q^2}^*)^4 \to (\mathbb{F}_{q^2}^*)^4$ the corresponding exponential maps and $\overline{E_1^{-1}}, \overline{E_2^{-1}}, \overline{E_3^{-1}} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ their extensions. The following composition

$$L_1^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_1^{-1}} \circ \overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1}$$

defines a map `dme-dec` $: \mathbb{F}_q^8 \to \mathbb{F}_q^8$. By construction, we have that `dme-dec` maps E to D and, restricted to those sets, is the inverse of `dme-enc`. It is easy to verify that E is exactly the set of $y \in \mathbb{F}_q^8$ such

that

$$(\overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y),$$
$$(\overline{\phi} \circ L_2^{-1} \circ A_2^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_2^{-1}} \circ \overline{\phi} \circ L_3^{-1} \circ A_3^{-1} \circ \overline{\phi}^{-1} \circ \overline{E_3^{-1}} \circ \overline{\phi} \circ L_4^{-1} \circ A_4^{-1})(y)$$

belong to $(\mathbb{F}_{q^2}^*)^4$, i.e. do not have a zero entry.

The cryptographic assumption in `DME-3rnds-8vars-64bits-sign` is that, for any $y \in E$, the system of eight polynomial equations in eight unknowns

$$\begin{aligned}
p_1(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_1 \\
p_2(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_2 \\
p_3(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_3 \\
p_4(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_4 \\
p_5(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_5 \\
p_6(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_6 \\
p_7(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_7 \\
p_8(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) &= y_8
\end{aligned}$$

is hard to solve. In particular, this implies that it is not feasible to compute a secret key corresponding to a given public key.

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{512}$ map of the `DME-3rnds-8vars-64bits-sign` scheme, as required by the API, returns (m, s) where m is the original message and the signature s is obtained by first applying a PSS-SHA3 padding (with 256 random bits), then reading the 512 bit sequence as a vector in $\mathbb{F}_q^8$, applying `dme-dec`, and lastly, interpreting the resulting vector as a 512 bit sequence. The `dme-open` $: \{0,1\}^* \times \{0,1\}^{512} \to \{0,1\}^* \cup \{error\}$ reverses the procedure above using `dme-enc` and checks that the signature is legitimate. The details of these algorithms are given in the next section.

2 Implementation details of DME-3rnds-8vars-64bits-sign

The field of $q = 2^{64}$ is implemented as the quotient ring

$$\mathbb{F}_q = \mathbb{F}_2[t]/\langle t^{64} + t^{11} + t^2 + t + 1\rangle,$$

and the monic irreducible polynomial $p(u) \in \mathbb{F}_q[u]$ that defines $\mathbb{F}_{q^2}$ is $p(u) = u^2 + tu + 1$, so we have

$$\mathbb{F}_{q^2} = \mathbb{F}_q[u]/\langle u^2 + tu + 1\rangle.$$

An element $\alpha = \alpha_{63}t^{63} + \cdots + \alpha_1 t + \alpha_0 \in \mathbb{F}_q$ can be interpreted as the 64 bits unsigned integer $\texttt{int}(\alpha) = \alpha_{63}2^{63} + \cdots + \alpha_1 2 + \alpha_0 \in [0, 2^{64} - 1]$. In C99, these fit perfectly in the `uint64_t` type of the standard library. When serialized into bytes, the little-endian convention is used for all integer types. In particular, the element α above, correspond with the sequence of 8 bytes

$$\left(\left\lfloor \frac{\texttt{int}(\alpha)}{2^{8i}} \right\rfloor \bmod 2^8 \right)$$

for $i = 0, 1, \ldots, 7$ in exactly this order. An element $\beta = \beta_0 + \beta_1 u \in \mathbb{F}_{q^2}$ is serialized as the 16 byte sequence obtained by serializing first β_0 and then β_1. Similarly, a matrix $\gamma \in \mathbb{F}_q^{2\times 2}$ is serialized as the 32 bytes sequence obtained by serializing γ_{11}, γ_{12}, γ_{21}, γ_{22} in that order.

The private key is $721 = 16 \cdot 32 + 24 \cdot 8 + 6 + 6 + 5$ bytes long, which correspond to the serialization of the the 16 matrices $L_{11}^{-1}, L_{12}^{-1}, \ldots, L_{44}^{-1}$, then the serialization of the 24 affine shifts $A_{21}, A_{22}, A_{31}, A_{32}, A_{41}, A_{42}, A_{23}, A_{24}, \ldots, A_{47}, A_{48} \in \mathbb{F}_q$, followed by a single byte for each $a_0, \ldots, a_5$,

$b_0, \ldots, b_5, c_0, c_2, c_3, c_5, c_6$. The coefficients c_1, c_4 and c_7 are not serialized since they can be recovered from the other values.

The public key is $2889 = 360 \cdot 8 + 9$ bytes long, which correspond to the serialization of the coefficients of $p_1, p_2, \ldots, p_8$ followed by a single byte for each $f_0, f_1, f_3, f_5, f_8, f_9, f_{10}, f_{11}, f_{12}$. The values of $f_2, f_4, f_6, f_7, f_{13}, f_{14}, f_{15}$ are not serialized since they can be computed from the other values by

$$\begin{aligned}
f_2 &= (f_1 + f_{10} - f_9 + 57) \bmod 64 \\
f_4 &= (f_0 + f_5 - f_1) \bmod 64 \\
f_6 &= (f_5 + f_2 - f_1) \bmod 64 \\
f_7 &= (f_5 + f_3 - f_1) \bmod 64 \\
f_{13} &= (f_{12} + f_9 - f_8) \bmod 64 \\
f_{14} &= (f_{12} + f_{10} - f_8) \bmod 64 \\
f_{15} &= (f_{11} + f_{12} - f_8) \bmod 64
\end{aligned}$$

The `dme-sign` $: \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^{512}$ map (the secret key is implicit here) is computed by the following procedure:

1. let $msg \in \{0,1\}^*$ be the input message,
2. choose $r \in \{0,1\}^{128}$ at random,
3. compute $w = \mathtt{SHA3}(msg||r) \in \{0,1\}^{256}$,
4. compute $g = \mathtt{SHA3}(w) \oplus (r||0) \in \{0,1\}^{256}$,
5. compute $s = \mathtt{dme\text{-}dec}(w||g) \in \mathbb{F}_q^8 \simeq \{0,1\}^{512}$,
6. return (msg, s).

This function is implemented in C99 as `crypto_sign`, with the only difference that the return value is $msg||s$ instead of (msg, s).

The `dme-open` $: \{0,1\}^* \times \{0,1\}^{512} \to \{0,1\}^* \cup \{error\}$ map (the public key is implicit here) is computed as follows:

1. let $(msg, s) \in \{0,1\}^* \times \{0,1\}^{512}$ be the input message and its corresponding signature,
2. compute $w \in \{0,1\}^{256}$ and $g \in \{0,1\}^{256}$ as $w||g = \mathtt{dme\text{-}enc}(s)$,
3. compute $r \in \{0,1\}^{128}$ as the first 128 bits of $\mathtt{SHA3}(w) \oplus g$,
4. if $w \neq \mathtt{SHA3}(msg||r)$, return $error$,
5. otherwise, return the original message msg.

This function is implemented in C99 as `crypto_sign_open`, but the two separate arguments for the message msg and the signature s, the function takes only one with the concatenation of both $msg||s$.

The function `dme-keypair`, which corresponds in the C99 implementation with `crypto_sign_keypair` creates 16 random matrices in $\mathbb{F}_q^{2\times 2}$, 4 random shifts in $\mathbb{F}_q^8$ and random values for $a_0, \ldots, c_7 \in [0, 127]$ satisfying the restrictions explained in the previous section (for instance, the matrices have to be invertible). With the secret key already chosen, the public key is computed by operating with 8 (symbolic) polynomials until $p_1, \ldots, p_8 \in \mathbb{F}_q[x_1, \ldots, x_8]$ is obtained. Then both keys are serialized and returned.

3 Timings

On a laptop with a Intel(R) Core(TM) i7-8565U CPU at 1.80GHz, with 8 Gb of RAM, running a Linux Mint 21 x86_64 operating system, the performance of the API primitives (for message of 200 bytes) is given in the following table:

`dme-keypair`	251 usec
`dme-sign`	41 usec
`dme-open`	12 usec

The length of the private key is 721 bytes and the length of the public key is 2889 bytes.