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

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

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.