DME: a full encryption, signature and KEM multivariate public key cryptosystem

Martín Avendaño, Pilar Coscojuela, Ignacio Luengo
Universidad Complutense de Madrid

PQCrypto 2023, College Park, MD
August 15-18 2023

Outline

1. Exponential maps
2. The old and new DME
3. DME setting
4. Public Key
5. Reduction of monomials
6. DME for KEM and Signature
7. Security of DME
8. Timings

Exponential maps

Given matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$ one can define an exponential map (called monomial in algebraic geometry) $F_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$ given by $F_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{1n}}, \ldots, x_1^{a_{n1}} \cdot \ldots \cdot x_n^{a_{nn}})$ and satisfying $F_B F_A = F_{B\cdot A}$

Proposition

If $A = (a_{ij})$ is invertible in $M_{n\times n}(\mathbb{Z}_{q-1})$ i.e. $\gcd(\det(A), q-1) = 1$, then F_A is invertible on $(\mathbb{F}_q \setminus \{0\})^n$ and the inverse of F_A is given by $F_{A^{-1}}$

Exponential maps

Given matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$ one can define
an exponential map (called monomial in algebraic geometry)
$F_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$ given by
$F_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{1n}}, \ldots, x_1^{a_{n1}} \cdot \ldots \cdot x_n^{a_{nn}})$ and
satisfying $F_B F_A = F_{B\cdot A}$

Proposition

If $A = (a_{ij})$ is invertible in $M_{n\times n}(\mathbb{Z}_{q-1})$ i.e. $\gcd(\det(A), q-1) = 1$, then F_A is invertible on $(\mathbb{F}_q \setminus \{0\})^n$ and the inverse of F_A is given by $F_{A^{-1}}$

DME (double matrix exponentiation)

- The public key of the original DME, is a map $F : \mathbb{F}_q^{2m} \to \mathbb{F}_q^{2m}$ obtained as composition of linear maps and two exponential maps over $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^m}$.
- DME was presented in 2017 to the KEM category (with $m = 3$) of the NIST call and was broken by Avendaño and Marco (Finite Fields and Their Appl. 71, 2021). Their attack only works for m odd.
- Beullens propose an decomposition attacks to the polynomials $\tilde{F}$ obtained by Weil's descent.

DME – NIST PQC 2023

The main new characteristics of the **new scheme DME** are:

- We use $r > 2$ exponentials over the same field $\mathbb{F}_{q^2}$.
- A procedure for the (drastic) reduction of the number of monomials
- The linear components can have translations. This fact may produce failure of decryption or invalid signatures.
- The entries of the exponent matrices are not public.

DME – NIST PQC 2023

The main new characteristics of the **new scheme DME** are:

- We use $r > 2$ exponentials over the same field $\mathbb{F}_{q^2}$.
- A procedure for the (drastic) reduction of the number of monomials
- The linear components can have translations. This fact may produce failure of decryption or invalid signatures.
- The entries of the exponent matrices are not public.

The public key of the new DME, is a map $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ obtained as composition of linear maps and r exponential maps over $\mathbb{F}_{q^2}$ with $q = 2^e$.

We denote the resulting scheme by $DME(r, n, q)$

The main new characteristics of the **new scheme DME** are:

- We use $r > 2$ exponentials over the same field $\mathbb{F}_{q^2}$.
- A procedure for the (drastic) reduction of the number of monomials
- The linear components can have translations. This fact may produce failure of decryption or invalid signatures.
- The entries of the exponent matrices are not public.

The public key of the new DME, is a map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ obtained as composition of linear maps and r exponential maps over $\mathbb{F}_{q^2}$ with $q = 2^e$.

We denote the resulting scheme by $DME(r, n, q)$

DME setting

The setting for DME$(r, 8, 2^e)$ cryptosystem is:

Let $h(u) = u^2 + au + b \in \mathbb{F}_q[u]$ be a fixed irreducible polynomial, and $\mathbb{F}_{q^2} = \mathbb{F}_q[u]/\langle h(u) \rangle$ and $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ be the corresponding isomorphism. Let $\bar{\phi} : \mathbb{F}_q^8 \to (\mathbb{F}_{q^2})^4$ be the map

$$(x_1, \ldots, x_8) \mapsto (\phi(x_1, x_2), \phi(x_3, x_4), \phi(x_5, x_6), \phi(x_7, x_8))$$

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

The DME$(r, 8, 2^e)$ scheme combines $r + 1$ linear+affine maps $L_0, \ldots, L_r : \mathbb{F}_q^8 \to \mathbb{F}_q^8$ with r exponential maps $F_{E_1}, \ldots, F_{E_r} : (\mathbb{F}_{q^2})^4 \to (\mathbb{F}_{q^2})^4$ as follows:

$$\mathbb{F}_q^8 \xrightarrow{L_0} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{F_{E_1}} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}}$$

$$\mathbb{F}_q^8 \xrightarrow{L_1} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{F_{E_2}} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}}$$

$$\mathbb{F}_q^8 \xrightarrow{L_2} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{F_{E_3}} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}}$$

$$\mathbb{F}_q^8 \xrightarrow{L_3} \mathbb{F}_q^8 \xrightarrow{\bar{\phi}} (\mathbb{F}_{q^2})^4 \xrightarrow{F_{E_4}} (\mathbb{F}_{q^2})^4 \xrightarrow{\bar{\phi}^{-1}}$$

$$\mathbb{F}_q^8 \xrightarrow{L_4} \mathbb{F}_q^8$$

DME Public Key

The rows of the matrices E_i have 1 or 2 non zero entries that are powers of 2.

The number of monomials can be up to double exponential in the number of round r. For instance if each row of E_i has 2 non zero entries then each component has 2^{2^r} monomials.

The lists of monomials and the list of coefficients of the components F_{ri} can be computed very efficiently as follows:

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

Applying the mixed-product property of the Kronecker product :

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

DME Public Key

The rows of the matrices E_i have 1 or 2 non zero entries that are powers of 2.

The number of monomials can be up to double exponential in the number of round r. For instance if each row of E_i has 2 non zero entries then each component has 2^{2^r} monomials.

The lists of monomials and the list of coefficients of the components F_{ri} can be computed very efficiently as follows:

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

Applying the mixed-product property of the Kronecker product :

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

Reduction of monomials

For $i > 1$ the list of monomials $M_{(i+1)l} = (M_{ij}^{\alpha} \otimes M_{ik}^{\beta})$ can be reduced if M_{ij} and M_{ik} have a variable in common say x_1 and let $x_1^{2^{l_1}} \cdot m_1$ and $x_1^{2^{l_2}} \cdot m_2$ the monomials with x_1 in both lists.

Let $\alpha = 2^{l_1}$ and $\beta = 2^{l_2}$ then $M_{(i+1)l}$ has 2 monomials with terms $x_1^{e_1+l_1}$ and $x_1^{e_2+l_2}$.

Making $l_2 = e_1 + l_1 - e_2$ will produce 2 equal monomials.

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

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

The final lists (M_{31}, M_{32}, M_{33}) have size $(2^7, 2^7, 2^6)$ and applying the above procedure after the sizes are $(32, 36, 24)$.

For $i > 1$ the list of monomials $M_{(i+1)l} = (M_{ij}^{\alpha} \otimes M_{ik}^{\beta})$ can be reduced if M_{ij} and M_{ik} have a variable in common say x_1 and let $x_1^{2^{l_1}} \cdot m_1$ and $x_1^{2^{l_2}} \cdot m_2$ the monomials with x_1 in both lists.

Let $\alpha = 2^{l_1}$ and $\beta = 2^{l_2}$ then $M_{(i+1)l}$ has 2 monomials with terms $x_1^{e_1+l_1}$ and $x_1^{e_2+l_2}$.

Making $l_2 = e_1 + l_1 - e_2$ will produce 2 equal monomials.

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

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

The final lists (M_{31}, M_{32}, M_{33}) have size $(2^7, 2^7, 2^6)$ and applying the above procedure after the sizes are $(32, 36, 24)$.

DME as a permutation

Theorem

If the linear components L_i of F do not have affine translations then the public key map $F : (\mathbb{F}_{q^2} \setminus \{0\})^4 \to (\mathbb{F}_{q^2} \setminus \{0\})^4$ is a permutation.

In the current version we allow affine translations L_i that can produce failure of decryption or invalid signature with a probability of around $(1/q^2)$.

DME for KEM and Signature

We use the DME permutation to build an RSA like scheme using as random padding the standards OAEP for PKE and KEM and PSS00 for signature whose security is well understood.

DME-Sign

For the signature one has to compute $F^{-1}(pad(msg))$ and invalid signatures can be avoided as follows:
The translations in L_i^{-1} can produce at some step one 0 that and give vector outside of $(\mathbb{F}_{q^2} \setminus \{0\})^4$, if this happens we start again with a new PSS padding $pad(msg)$.

DME for KEM and Signature

We use the DME permutation to build an RSA like scheme using as random padding the standards OAEP for PKE and KEM and PSS00 for signature whose security is well understood.

DME-Sign

For the signature one has to compute $F^{-1}(pad(msg))$ and invalid signatures can be avoided as follows:
The translations in L_i^{-1} can produce at some step one 0 that and give vector outside of $(\mathbb{F}_{q^2} \setminus \{0\})^4$, if this happens we start again with a new PSS padding $pad(msg)$.

Security of DME

- Gröbner basis.
- Weil's descent
- Structural Cryptanalysis

Configuration Matrices ($\mathcal{CM}$) as a list of matrices for the exponentials where the non zero entries are substituted by 1. $\mathcal{CM} = [E_r^*, \dots E_1^*]$, $E^* = E_r^* \cdots E_1^*$. Let t_k be the sum of the entries in the k-th row of E^* then t_k is the degree of the components obtained by Weil's descent.

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

Security of DME

Security of DME

- Gröbner basis.
- Weil's descent
- Structural Cryptanalysis

Configuration Matrices ($\mathcal{CM}$) as a list of matrices for the exponentials where the non zero entries are substituted by 1. $\mathcal{CM} = [E_r^*, \ldots E_1^*]$, $E^* = E_r^* \cdots E_1^*$. Let t_k be the sum of the entries in the k-th row of E^* then t_k is the degree of the components obtained by Weil's descent.

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

Gröbner basis

If $F(\underline{x}) = \underline{y}$ we have to consider the ideal
$I = \langle f_1(\underline{x}) - y_1, \ldots, f_n(\underline{x}) - y_n, x_1^{2^e} - x_1, \ldots, x_n^{2^e} - x_n \rangle$

Let $sd(I)$ be the **solving degree of** I:

$$\binom{n + sd(I)}{n}^{\omega} \quad (*)$$

- $sd(I)$ is bounded below be degree of the initial basis I. Since $x_n^{2^e} - x_n \in I$, $sd(I)$ is bounded below by 2^e.
- For $n = 8$ and $q = 2^{64}$ (*) gives $O(2^{1024})$
- Limited experimental evidence: Magma with $512Gb$ of RAM can not solve I for $e > 4$

Gröbner basis

If $F(\underline{x}) = \underline{y}$ we have to consider the ideal
$I = \langle f_1(\underline{x}) - y_1, \ldots, f_n(\underline{x}) - y_n, x_1^{2^e} - x_1, \ldots, x_n^{2^e} - x_n \rangle$

Let $sd(I)$ be the **solving degree of** I:

$$\binom{n + sd(I)}{n}^{\omega} \quad (*)$$

- $sd(I)$ is bounded below be degree of the initial basis I. Since $x_n^{2^e} - x_n \in I$, $sd(I)$ is bounded below by 2^e.
- For $n = 8$ and $q = 2^{64}$ (*) gives $O(2^{1024})$
- Limited experimental evidence: Magma with $512Gb$ of RAM can not solve I for $e > 4$

Structural Cryptanalysis

On can try to get the components of F starting with the last linear component L_r as follows:
$F_{i+1,2l-1} + \bar{u}F_{i+1,2l} = (F_{i,2j-1} + \bar{u}F_{i,2j})^{\alpha} \cdot (F_{i,2k-1} + \bar{u}F_{i,2k})^{\beta}$
$= (\sum B_i m_i) \cdot (\sum C_j n_j) = \sum B_i C_j m_i n_j = \sum H_{ij} m_i n_j$

The relations $H_{ij} = Q_{ij}(B, C) = \sum B_k C_l$, can be used to get homogeneous implicit equations for the H_{ij} that will give us (homog.) equations for the unknown entries of the matrices L_{rk}^{-1} that can be solved up to a multiplicative constant $\lambda_k \in \mathbb{F}_q$, and given $(\lambda_1, \ldots, \lambda_4) \in \mathbb{F}_q \setminus \{0\}$

The reduction of monomials gives makes that the coefficients of m_i and n_j have many terms that make the computation of the implicit equation of the H_{ij} more complex.

Structural Cryptanalysis

On can try to get the components of F starting with the last linear component L_r as follows:

$$F_{i+1,2l-1} + \bar{u}F_{i+1,2l} = (F_{i,2j-1} + \bar{u}F_{i,2j})^{\alpha} \cdot (F_{i,2k-1} + \bar{u}F_{i,2k})^{\beta}$$
$$= (\sum B_i m_i) \cdot (\sum C_j n_j) = \sum B_i C_j m_i n_j = \sum H_{ij} m_i n_j$$

The relations $H_{ij} = Q_{ij}(B, C) = \sum B_k C_l$, can be used to get homogeneous implicit equations for the H_{ij} that will give us (homog.) equations for the unknown entries of the matrices L_{rk}^{-1} that can be solved up to a multiplicative constant $\lambda_k \in \mathbb{F}_q$, and given $(\lambda_1, \ldots, \lambda_4) \in \mathbb{F}_q \setminus \{0\}$

The reduction of monomials gives makes that the coefficients of m_i and n_j have many terms that make the computation of the implicit equation of the H_{ij} more complex.

Weil's descent

Weil's descent: The polynomial of F can be converted in polynomials $\tilde{F}$ in *ne* variables over $\mathbb{F}_2$.

W. Beullens proposed in 2018 to apply the decomposition algorithm of Fauguere-Perret for original DME. In that case $\tilde{F}$is the composition of two quadratic polynomials but the algorithm works only for generic polynomials.

We decide to add more rounds to DME in order increase the degree of $\tilde{F}$. In the example with 3 rounds the degree of the components before the reduction of monomials are $(7, 7, 6)$ and after reduction is $(5, 6, 5)$.

Timings for DME-Sign

	NSL	KeyGen	Sign	Verify	PKey	Skey	Signature
dme-4r-8v-64b-pss	5	4609827	222307	55484	4843	675	64
dme-3r-8v-64b-pss	5	1953078	182009	40197	2793	542	64
dilithium2	2	169935	238597	147235	1312	2544	2420
dilithium5	5	319828	617804	337222	2492	4880	4595
falcon1024dyn	5	78644060	2080846	310257	1793	2305	1330
sphincsf256shake256robust	5	23130618	530274683	25373313	64	128	49216

Figure: Average CPU cycles for SIGN as measured by SuperCop on an Intel(R) Core(TM) i7-1165G7 @ 2.80GHz (message length = 93 bytes)

Timings for different finite fields

finite field	2^{32}	2^{48}	2^{64}
dme-keypair	121 usec	262 usec	251 usec
dme-sign	19 usec	35 usec	41 usec
dme-open	9 usec	11 usec	12 usec
private key	369 bytes	545 bytes	721 bytes
public key	1449 bytes	2169 bytes	2889 bytes

Figure: Timings and key sizes for the DME signature scheme with 3 rounds and 8 variables. The message length is 100 bytes.

more security?

- Gröbner basis: increase the size of the field $\mathbb{F}_q$.
- Weil's descent: increase the number of rounds r.

more security?

- Gröbner basis: increase the size of the field $\mathbb{F}_q$.
- Weil's descent: increase the number of rounds r.
- Structural Cryptanalysis: take out component of the public key. i.e.

$$F : \mathbb{F}_q^8 \to \mathbb{F}_q^7$$

.

more security?

- Gröbner basis: increase the size of the field $\mathbb{F}_q$.
- Weil's descent: increase the number of rounds r.
- Structural Cryptanalysis: take out component of the public key. i.e.

$$F : \mathbb{F}_q^8 \to \mathbb{F}_q^7$$

.

Thank you!

Questions?

Thank you!

Questions?