DME: a multivariate KEM scheme

Ignacio Luengo
(U. Complutense de Madrid)

Implemented by
Martín Avendaño, (CUD Zaragoza)
Miguel A. Marco, (U. Zaragoza)

NIST First PQC Standarization Conference
April 11-13, 2018
Fort Lauderdale, FL

Exponential maps (called monomial in algebraic geometry)

A matrix

$$A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$$

defines an exponential map

$$G_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$$

given by

$$G_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdot \ldots \cdot x_n^{a_{nn}})$$

and satisfying

$$((x_1, \ldots, x_n)^A)^B = (x_1, \ldots, x_n)^{A\cdot B}$$

Theorem : If $\gcd(\det(A), q-1) = 1$, then G_A is invertible on $(\mathbb{F}_q \setminus \{0\})^n$ and the inverse of G_A is given by $G_{A^{-1}}$

DME stands for double matrix exponentiation

The public key $F : \mathbb{F}_q^{nm} \to \mathbb{F}_q^{nm}$ is a map obtained as composition of five maps, $F = L_3 \circ G_2 \circ L_2 \circ G_1 \circ L_1$, and $q = 2^e$.

$$\underbrace{\mathbb{F}_q^{mn} \xrightarrow{L_1} (\mathbb{F}_{q^n})^m \xrightarrow{G_1} (\mathbb{F}_{q^n})^m \xrightarrow{L_2} (\mathbb{F}_{q^m})^n \xrightarrow{G_2} (\mathbb{F}_{q^m})^n \xrightarrow{L_3} \mathbb{F}_q^{mn}}_{F}$$

The map F is designed to verify,

- F is injective on $(\mathbb{F}_q^n \setminus \{0\})^m$
- $\forall x \in (\mathbb{F}_q^n \setminus \{0\})^m,\ F(x) \in (\mathbb{F}_q^m \setminus \{0\})^n$.

- The maps G_1 and G_2 are exponential maps given by **(public)** matrices with two non-zero entries (powers of 2).
- The maps L_1, L_2 and L_3 are $\mathbb{F}_q$-linear **(secret)** isomorphisms
- **NIST proposal:** $n = 2, m = 3, q = 2^{48}, (288 bits)$
- Each component of F has 64 monomials
- F^{-1} is polynomial and has at least 2^{100} monomials.
- A typical monomial of F looks like

$$x_{i_1}^{2^{\alpha_1}} \cdots x_{i_4}^{2^{\alpha_4}} = x_1^{8388608} x_3^{131072} x_4^{8589934592} x_6^{1048576}$$

DME features

	Key Gen.	Encr.	Decr.	SK	PK	CT	bytes
DME	445 M	2.11 M	1.08 M	288 B	2304 B	36 B	33 B

Pros:

- Very simple design
- Flexibility
- Constant time evaluation (timing side-channel attacks)
- Randomness: similar behavior as a block cypher : PRNG, Graph
- Immune to Grobner basis attack over $\mathbb{F}_{2^{48}}$

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem
- Estructural attacks to find the secret linear maps L_i

Cryptoanalisys: Weil descent over $\mathbb{F}_2$

- Over $\mathbb{F}_2$, F can be written as a system $\tilde{F}$ of quartic polynomials in 288 variables.
- Attack(Ward Buellens): use Fauguere-Perret decomposition algorithm (does not work for small fields)
- Degree of regularity of $\tilde{F}$

New proposed parameters for the second round:

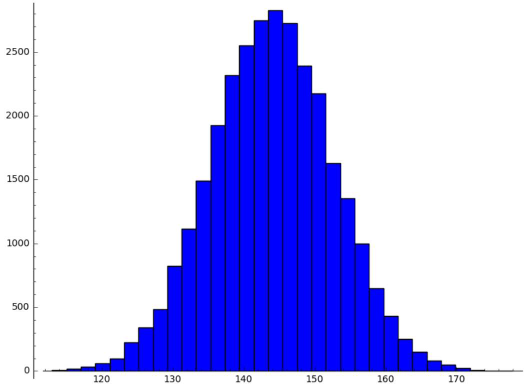
- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$
- $h(x_1, \ldots, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6, x_2 x_4 x_6, 0)$
  $F : (\mathbb{F}_q)^6 \to (\mathbb{F}_q)^8$
- ct$=$ 48 bytes, 32 monomials
- Typical monomials

$$x_1^{2^{\alpha_1}} x_2^{b_1} x_3^{2^{\alpha_3}} x_4^{b_4} x_5^{2^{\alpha_5}} x_6^{b_6}$$

- On $\mathbb{F}_2$ the PK, $\tilde{F}$ can have degree > 100 and more than 2^{256} monomials

Thank you for your attention!

Questions?



Back