Practical Attack on All Parameters of the DME Signature Scheme

Pierre Briaud[1,2], joint work with Maxime Bros[3], Ray Perlner[3] and Daniel Smith-Tone[3,4]

Eurocrypt 2024, May 30

[1]Inria Paris
[2]Sorbonne Université
[3]NIST
[4]University of Louisville

DME ?

"New" signature candidate submitted to NIST

- Multivariate, ad hoc design
- Level I : sig size 32 B, pk size 1.5 kB + VERY efficient

DME ?

“New” signature candidate submitted to NIST

- Multivariate, ad hoc design
- Level I : sig size 32 B, pk size 1.5 kB + VERY efficient

This talk

A practical key recovery attack (< 1s for Level I, naive Magma script)

Description of DME

Multivariate signature scheme

Public key

$$P = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$$

Gives map $\mathbb{F}_q^n \to \mathbb{F}_q^m$

$$\boxed{\boldsymbol{\sigma} \in \mathbb{F}_q^n \text{ valid on message } \boldsymbol{m} \in \mathbb{F}_q^m \Leftrightarrow P(\boldsymbol{\sigma}) = \boldsymbol{m}}$$

Multivariate signature scheme

Public key

$$P = (p_1, \dots, p_m) \in \mathbb{F}_q[x_1, \dots, x_n]^m$$

Gives map $\mathbb{F}_q^n \to \mathbb{F}_q^m$

$$\boxed{\boldsymbol{\sigma} \in \mathbb{F}_q^n \text{ valid on message } \boldsymbol{m} \in \mathbb{F}_q^m \Leftrightarrow P(\boldsymbol{\sigma}) = \boldsymbol{m}}$$

~~Standard multivariate~~

- P has high degree (~~quadratic P~~)
- For λ-bit security, $m = n = 8$ and $q = 2^{\lambda/4}$ (~~$m, n = f(\lambda)$, constant q~~)

Multiple rounds

We have $P \stackrel{def}{=} R_3 \circ R_2 \circ R_1 \circ R_0$, where

$$R_i \stackrel{def}{=} C_i \circ L_i \circ F_{\boldsymbol{A}_i},$$

and

- $F_{\boldsymbol{A}_i}$: "exponential map"
- L_i : specific $\mathbb{F}_q$-linear map
- C_i : addition of constants

Sign : compute $P^{-1}(\boldsymbol{m})$ by inverting the rounds

Exponential map $F_{\mathbf{A}_i}$ (1)

Field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$, $U \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$

$$(x, y) \in \mathbb{F}_q^2 \leftrightarrow x + Uy \in \mathbb{F}_{q^2}$$

$$\phi(x_1, \ldots, x_8) \stackrel{def}{=} (x_1 + Ux_2, \ldots, x_7 + Ux_8) \in \mathbb{F}_{q^2}^4$$

Final map $\mathbb{F}_q^8 \to \mathbb{F}_q^8$

$$F_{\mathbf{A}} \stackrel{def}{=} \phi^{-1} \circ E_{\mathbf{A}} \circ \phi, \quad E_{\mathbf{A}} : \mathbb{F}_{q^2}^4 \to \mathbb{F}_{q^2}^4$$

Big-field map $E_{\mathbf{A}}$

Matrix $\boldsymbol{A} \stackrel{def}{=} (a_{ij}) \in \mathbb{Z}_{q^2-1}^{4\times 4}$ contains exponents

$$E_{\mathbf{A}}(X_1, \ldots, X_4) \stackrel{def}{=} (X_1^{a_{11}} X_2^{a_{12}} X_3^{a_{13}} X_4^{a_{14}}, \ldots, X_1^{a_{41}} X_2^{a_{42}} X_3^{a_{43}} X_4^{a_{44}})$$

Exponential map $F_{\mathbf{A_i}}$ (2)

$\forall \boldsymbol{A},\ \boldsymbol{A}' \in \mathbb{Z}_{q^2-1}^{4\times 4},\ F_{\mathbf{A}} \circ F_{\mathbf{A}'} = F_{\mathbf{AA}'}$

$\det(\boldsymbol{A})$ invertible $\Rightarrow F_{\mathbf{A}}|_{\phi^{-1}\left((\mathbb{F}_{q^2}\setminus\{0\})^4\right)}$ bijective

Exponential map $F_{\mathbf{A_i}}$ (2)

$\forall \boldsymbol{A},\ \boldsymbol{A}' \in \mathbb{Z}_{q^2-1}^{4\times 4},\ F_{\mathbf{A}} \circ F_{\mathbf{A}'} = F_{\mathbf{AA}'}$
det $(\boldsymbol{A})$ invertible $\Rightarrow F_{\mathbf{A}}|_{\phi^{-1}((\mathbb{F}_{q^2}\setminus\{0\})^4)}$ bijective

DME matrices

We have $\mathbf{A}_0 = \boldsymbol{I}_4$ and

$$\mathbf{A}_1 = \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix} \mathbf{A}_2 = \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix} \mathbf{A}_3 = \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix}$$

Linear map L_i

Direct sum of 4 maps $\mathbb{F}_q^2 \to \mathbb{F}_q^2$

$$L_i(x_1, \ldots, x_8) \overset{def}{=} (L_{i1}(x_1, x_2), \ldots, L_{i4}(x_7, x_8)),$$

where $L_{ij} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ linear, $\det(L_{ij}) \neq 0$

Also contributes to efficiency

Rest of the talk

Equivalent key recovery

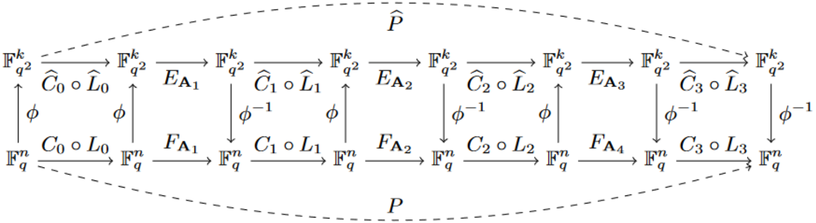
$$\text{Find } \widetilde{R_3} \circ \widetilde{R_2} \circ \widetilde{R_1} \circ \widetilde{R_0} = P, \; \widetilde{R_i} \neq R_i$$

Unpeel rounds one by one, start from $\widetilde{R_3}$

Main ideas

Lift to extension field

$$\widehat{P} \overset{def}{=} \phi \circ P \circ \phi^{-1} \in \left(\mathbb{F}_{q^2}[X_1, \ldots, X_4]/\langle X_\ell^{q^2} - X_\ell,\ \ell \in \{1..4\}\rangle\right)^4$$



We can write $\widehat{P} = \widehat{R_3} \circ \widehat{R_2} \circ \widehat{R_1} \circ \widehat{R_0}$,

$$\widehat{R_i} \overset{def}{=} (\phi \circ C_i \circ \phi^{-1}) \circ (\phi \circ L_i \circ \phi^{-1}) \circ (\phi \circ \phi^{-1} \circ E_{\mathbf{A}_i} \circ \phi \circ \phi^{-1}) \overset{def}{=} \widehat{C_i} \circ \widehat{L_i} \circ E_{\mathbf{A}_i}$$

New linear maps

Recall that $L_i(x_1, \ldots, x_8) = (L_{i1}(x_1, x_2), \ldots)$ and $\phi(x_1, x_2, \ldots) = (x_1 + Ux_2, \ldots)$

$\Rightarrow \widehat{L_i} = \phi \circ L_i \circ \phi^{-1} = (\widehat{L_{i1}}, \ldots, \widehat{L_{i4}})$, where $\widehat{L_{ij}} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is $\mathbb{F}_q$-linear

Expression of $\widehat{L_{ij}}$

$X \mapsto A_{ij}X + B_{ij}X^q$, where $A_{ij},\ B_{ij} \in \mathbb{F}_{q^2}$ (q-polynomial)

New linear maps

Recall that $L_i(x_1, \dots, x_8) = (L_{i1}(x_1, x_2), \dots)$ and $\phi(x_1, x_2, \dots) = (x_1 + Ux_2, \dots)$

$\Rightarrow \widehat{L_i} = \phi \circ L_i \circ \phi^{-1} = (\widehat{L_{i1}}, \dots, \widehat{L_{i4}})$, where $\widehat{L_{ij}} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is $\mathbb{F}_q$-linear

Expression of $\widehat{L_{ij}}$

$X \mapsto A_{ij}X + B_{ij}X^q$, where $A_{ij},\ B_{ij} \in \mathbb{F}_{q^2}$ (q-polynomial)

- Components only mixed within exponential maps $E_{\mathbf{A_i}}$

Monomials in intermediate states (1)

State after applying $\widehat{R_i}$: $(G_1^{(i)}, \ldots, G_4^{(i)})$

Monomials in intermediate states (1)

State after applying $\widehat{R_i}$: $(G_1^{(i)}, \ldots, G_4^{(i)})$

Orbit of $\mu \in \mathbb{F}_{q^2}[X_1, \ldots, X_4]/\langle X_\ell^{q^2} - X_\ell,\ \ell \in \{1..4\}\rangle$

All monomials obtained from μ by raising one or several variables to the power q

For $\mu = X_1 X_3^5 \to \{X_1^q X_3^5,\ X_1 X_3^{5q},\ X_1^q X_3^{5q},\ X_1 X_3^5\}$

Lemma

For all i, j, the set of monomials present in $G_j^{(i)}$ is a union of orbits

Proof: true after $\widehat{R_0} = \widehat{C_0} \circ \widehat{L_0}$ on $(X_1, \ldots, X_4)$. Then preserved by $+$, $\times$, $X \mapsto X^{2^a}$ □

Monomials in intermediate states (2)

Orbits are unknown

For $x \in \mathbb{Z}_{q^2-1}$, $\bar{x}$ rep. $\in \{0..q^2-2\}$

$$\mu = X_1^{\alpha} X_2^{\beta} X_3^{\gamma} X_4^{\delta} \to (\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$$

Monomials in intermediate states (2)

Orbits are unknown

For $x \in \mathbb{Z}_{q^2-1}$, $\bar{x}$ rep. $\in \{0..q^2-2\}$

$$\mu = X_1^{\alpha} X_2^{\beta} X_3^{\gamma} X_4^{\delta} \to (\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$$

Hamming weights of binary decompositions

$$\mathrm{HW}(\mathrm{BinDec}(\bar{\alpha})), \mathrm{HW}(\mathrm{BinDec}(\bar{\beta})), \mathrm{HW}(\mathrm{BinDec}(\bar{\gamma})), \mathrm{HW}(\mathrm{BinDec}(\bar{\delta}))$$

(constant within one orbit)

$$\mathbf{A}_1 = \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix} \quad \mathbf{A}_2 = \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix} \quad \mathbf{A}_3 = \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix}$$

How we invert $\widehat{R_3}$

From $\widehat{P} = (G_1^{(3)}, \ldots, G_4^{(3)})$ and known Hamming weights

- deduce monomials in $(G_1^{(2)}, \ldots, G_4^{(2)})$ + some info on $E_{\mathbf{A}_3}$ (exponent differences)
- coefficients in $(G_1^{(2)}, \ldots, G_4^{(2)})$ are still unknown

How we invert $\widehat{R}_3$

From $\widehat{P} = (G_1^{(3)}, \ldots, G_4^{(3)})$ and known Hamming weights

- deduce monomials in $(G_1^{(2)}, \ldots, G_4^{(2)})$ + some info on $E_{\mathbf{A}_3}$ (exponent differences)
- coefficients in $(G_1^{(2)}, \ldots, G_4^{(2)})$ are still unknown

To find them, we solve polynomial systems (1 bilinear and 2 linear)

- variables : unknown coefficients
- scalars : known monomials

Bilinear system

Starting point

For $j \in \{1..4\}$, let $G_j = G_j^{(2)}$ (secret linear form)

$$\widehat{R_3}(G_1, G_2, G_3, G_4) = \widehat{P}$$

$$\Updownarrow$$

$$E_{\mathbf{A}_3}(G_1, G_2, G_3, G_4) = \widehat{L_3}^{-1} \circ \widehat{C_3}^{-1}(P_1, P_2, P_3, P_4)$$

Recall that

$$\mathbf{A}_3 = \begin{bmatrix} * & * & 0 & 0 \\ 0 & 2^{\alpha} & 0 & 2^{\beta} \\ 0 & 2^{\gamma} & 0 & 2^{\delta} \\ 0 & 0 & * & * \end{bmatrix}$$

Exploit common pattern in rows 2 and 3

Components 2 and 3

We obtain

$$G_2^{2^\alpha} \times G_4^{2^\beta} = A_2 P_2 + B_2 P_2^q + D_2$$
$$G_2^{2^\gamma} \times G_4^{2^\delta} = A_3 P_3 + B_3 P_3^q + D_3$$

(G_2, G_4 linear forms) ($A_i, B_i, D_i \in \mathbb{F}_{q^2}$)

From partial information on $E_{\mathbf{A}_3}$

We can assume $G_4^{2^\beta} = G_4^{2^\delta}$

With $\overline{F} \overset{def}{=} G_2^{2^\alpha}$, $\overline{H} \overset{def}{=} G_2^{2^\gamma}$, $\overline{G} \overset{def}{=} G_4^{2^\beta} = G_4^{2^\delta}$, we get

$$\overline{F} \times \overline{G} = A_2 P_2 + B_2 P_2^q + D_2$$
$$\overline{H} \times \overline{G} = A_3 P_3 + B_3 P_3^q + D_3$$

Bilinear equations

For each monomial, match the 2 secret coefficients

- bilinear equations (on the left, product of linear forms)
- the system is overdefined (common $\overline{G}$ factor)

Level I

We have $\#\text{eqs} = 2 \times (25 - 1) = 48$ and $\#\text{vars} = \underbrace{5}_{\overline{F}} + \underbrace{5}_{\overline{G}} + \underbrace{5}_{\overline{H}} + 2 = 17$

Trivially solved by Gröbner bases

Bilinear equations

For each monomial, match the 2 secret coefficients

- bilinear equations (on the left, product of linear forms)
- the system is overdefined (common $\overline{G}$ factor)

Level I

We have $\#\text{eqs} = 2 \times (25 - 1) = 48$ and $\#\text{vars} = \underbrace{5}_{\overline{F}} + \underbrace{5}_{\overline{G}} + \underbrace{5}_{\overline{H}} + 2 = 17$

Trivially solved by Gröbner bases

Components 1 and 4 (+ solutions) $\rightarrow$ 2 linear systems

Conclusion

- Same procedure applies for the previous rounds
- Attack not a lot more costly on the other levels (also $m = n = 8$)

In theory, DME can still be patched !