HMFEv - An Efficient Multivariate Signature Scheme

Albrecht Petzoldt, Ming-Shing Chen, Jintai Ding, Bo-Yin Yang

PQCrypto 2017

Utrecht, Netherlands

Outline

Multivariate Cryptography

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$

The security of multivariate schemes is based on the

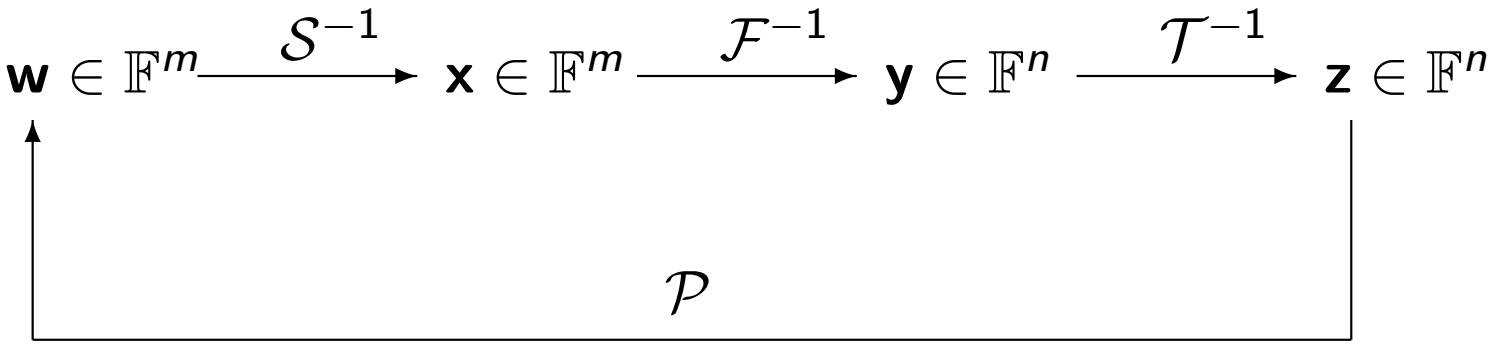
Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}),\ldots,p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\ldots,\bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Construction

- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible linear maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *Public key*: $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ supposed to look like a random system
- *Private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$ allows to invert the public key

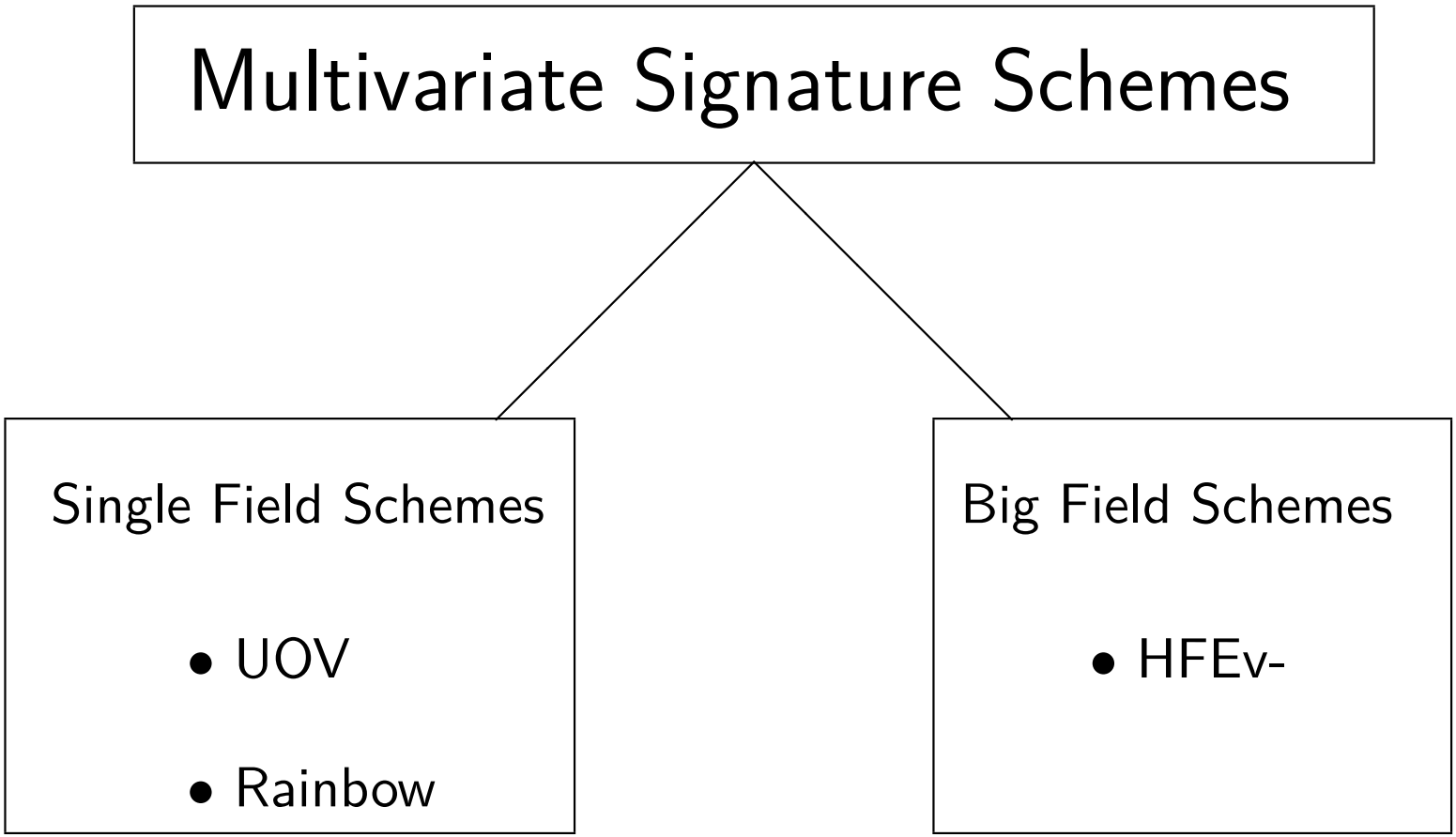
Workflow

Decryption / Signature Generation

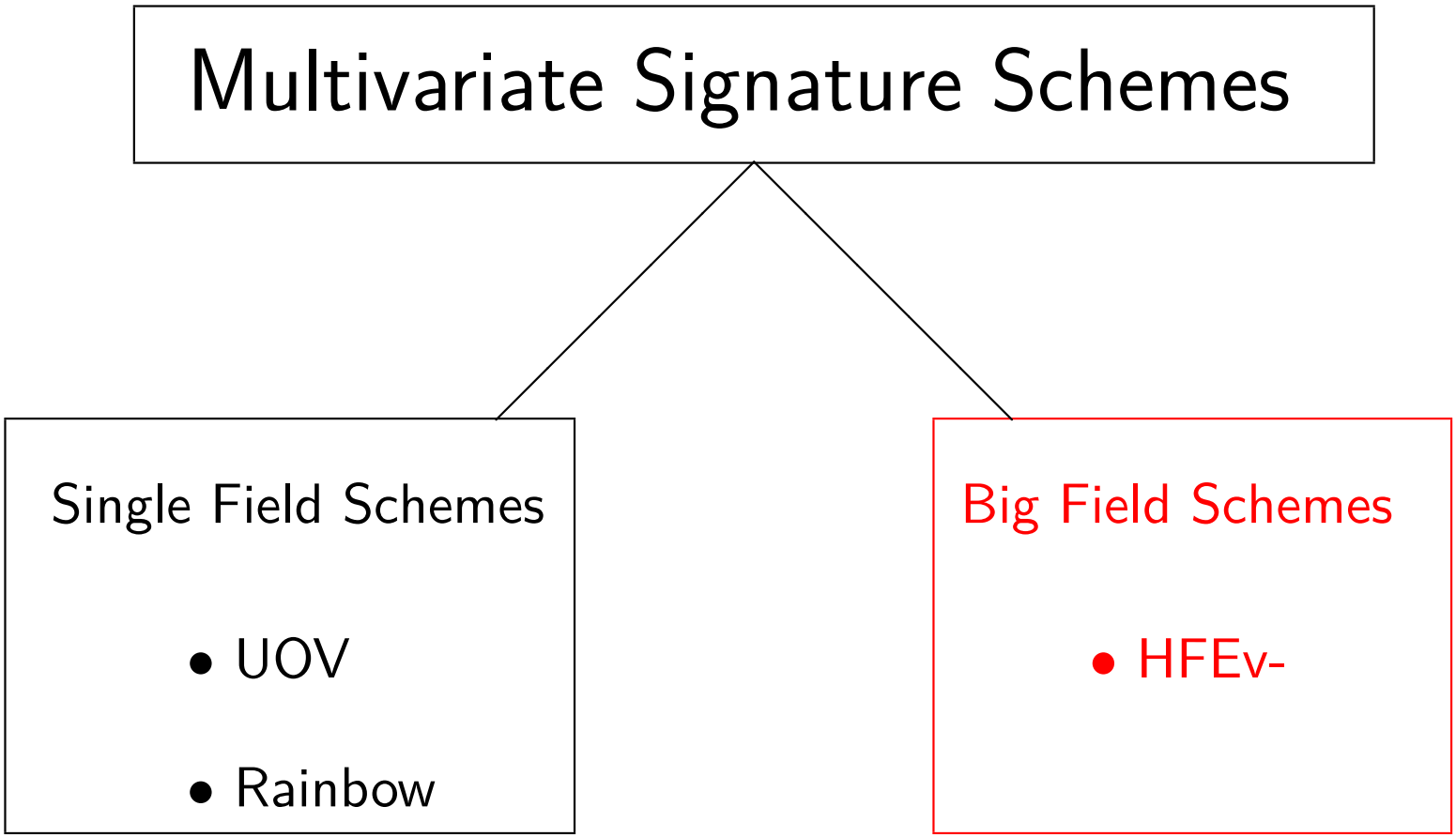


Encryption / Signature Verification

Multivariate Signature Schemes



Multivariate Signature Schemes



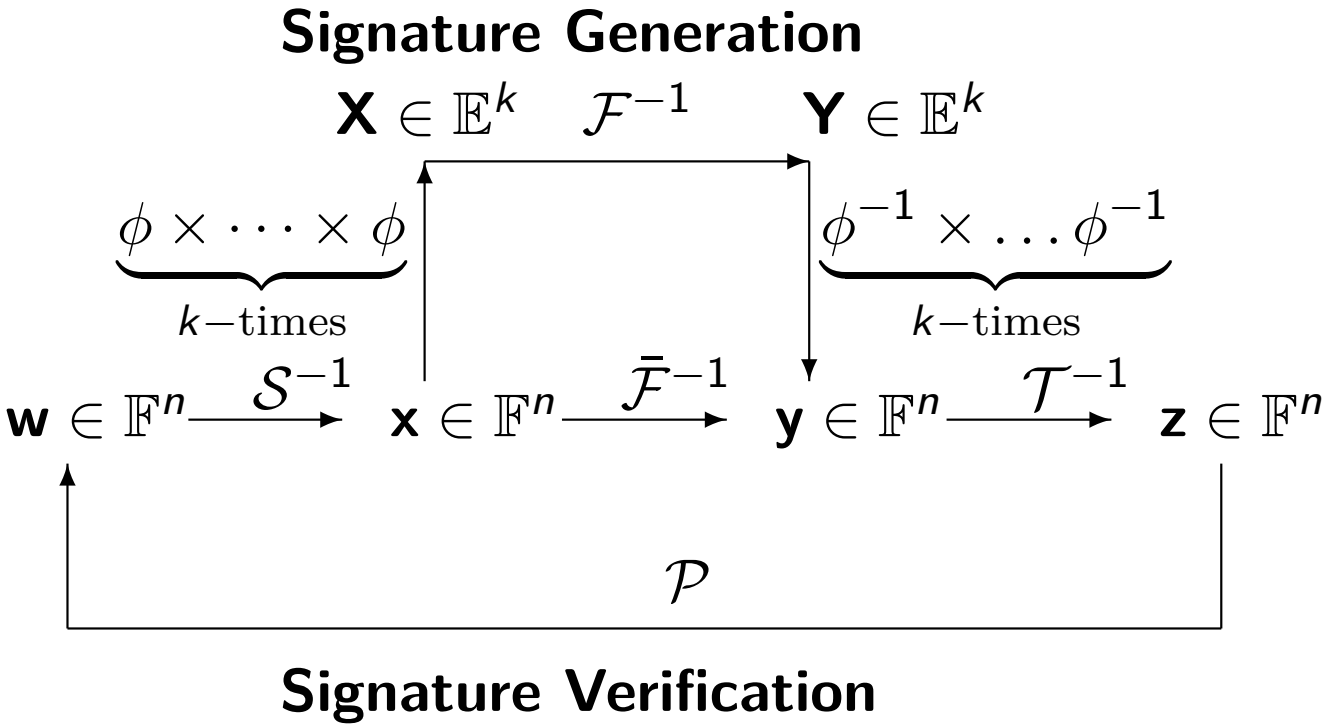
HFEv-

- uses HFE polynomial $\mathcal{F}$ of degree D
- signature generation: invert $\mathcal{F}$ by Berlekamps algorithm (complexity $\sim D^3$)

Efficiency: Use small D
Security: $r = \lfloor \log_q(D-1) \rfloor + 1$ should not be too small
$\Rightarrow$ Use HFEv- over small fields, e.g. $\mathbb{F}$=GF(2)
$\Rightarrow$ many equations and variables required to defend against (quantum) brute force attacks
$\Rightarrow$ large key sizes, hard to scale to higher security levels

$\Rightarrow$ Can we create HFEv- like schemes over large fields?

Medium Field Signature Schemes



HMFEv - Key Generation

- finite field $\mathbb{F}$, integers k, ℓ, v, extension field $\mathbb{E}$ of degree ℓ, isomorphism $\phi : \mathbb{F}^\ell \to \mathbb{E}$, $m = k \cdot \ell$, $n = m + v$
- central map $\mathcal{F}$: k components $f^{(1)}, \ldots, f^{(k)} : \mathbb{E}^k \times \mathbb{F}^v \to \mathbb{E}$,

$$f^{(i)}(X_1, \ldots, X_k) = \sum_{r,s=1}^{k} \alpha_{r,s}^{(i)} X_r X_s + \sum_{r=1}^{k} \beta_r^{(i)}(v_1, \ldots, v_v) \cdot X_r + \gamma^{(i)}(v_1, \ldots, v_v)$$

  with $\beta_r^{(i)} : \mathbb{F}^v \to \mathbb{E}$ linear, $\gamma^{(i)} : \mathbb{F}^v \to \mathbb{E}$ quadratic
  $\Rightarrow \bar{\mathcal{F}} = (\phi^{-1} \times \cdots \times \phi^{-1}) \circ \mathcal{F} \circ (\phi \times \cdots \times \phi \times \mathrm{id}_v) : \mathbb{F}^n \to \mathbb{F}^m$ quadratic
- two invertible affine transformations $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$, $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$
- *private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

Signature Generation

Given: document d

1. use hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}^m$ to compute $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$
2. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m$ and $\mathbf{X}_i = \phi(x_{(i-1)\cdot\ell+1}, \ldots, x_{i\cdot\ell}) \in \mathbb{E}$ $(i = 1, \ldots, k)$.
3. Choose random values for the vinegar variables $v_1, \ldots, v_v$
   Solve the multivariate quadratic system $f^{(i)}_{v_1,\ldots,v_v}(Y_1, \ldots, Y_k) = X_i$ $(i = 1, \ldots, k)$ by XL or a Gröbner basis algorithm
4. Compute $\mathbf{y} = (\phi^{-1}(Y_1), \ldots, \phi^{-1}(Y_k), v_1, \ldots, v_v) \in \mathbb{F}^n$
5. Compute the signature $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}^n$, message d

- Compute $\mathbf{w} = \mathcal{P}(d) \in \mathbb{F}^m$
- Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$
- Accept the signature $\mathbf{z} \Leftrightarrow \mathbf{w}' = \mathbf{w}$.

Security

Min Rank attack

Theorem

If $v \leq \ell$ holds, the rank of the quadratic form associated to $\mathcal{F}^{(i)}$ is less or equal to $k + v$

Vinegar maps are chosen completely random $\Rightarrow$ upper bound is tight

$$\text{Complexity}_{\text{MinRank}} = \ell^{(k+v+1)\cdot\omega}$$

with $2 < \omega \leq 3$.

Direct attack

Theorem

The degree of regularity of a direct attack against an HMFEv system is, under the assumption of $v \leq \ell$ bounded by

$$d_{\text{reg}} \leq \begin{cases} \frac{(q-1)\cdot(k+v-1)}{2} & \text{for } q \text{ even and } k+v \text{ odd} \\ \frac{(q-1)\cdot(k+v)}{2} & \text{otherwise.} \end{cases}$$

Experiments over small fields
$\Rightarrow$ bound is relativelty tight
$\Rightarrow$ concrete choice of k and v is not important, as long as $k+v$ is fixed and $k, v \geq 2$

Direct attacks (2)

Experiments over large fields

GF(31)	parameters (k, ℓ, v)	(2,6,4)	(2,7,4)	(2,8,4)	random
	m,n	12,12	14,14	16,16	16,16
	d_{reg}	14	16	18	18
	time (s)	1,911	164,089	-	-
	memory (MB)	953	17,273	ooM	ooM
GF(256)	parameters (k, ℓ, v)	(3,3,6)	(3,4,6)	(3,5,6)	random
	m,n	9,9	12,12	15,15	15,15
	d_{reg}	11	14	17	17
	time (s)	3.9	1,853	-	-
	memory (MB)	23.7	952	ooM	ooM

$\Rightarrow$ we can reach high values of d_{reg}

$\Rightarrow$ HMFEv systems behave very similar to random systems

$$\text{Complexity}_{\text{Direct}} = 3 \cdot \binom{n + d_{\text{reg}}}{d_{\text{reg}}}^2 \cdot \binom{n}{2}.$$

Quantum Attacks

With the help of Grover's algorithm, a binary multivariate system with n variables can be solved using

$$2^{(n/2)} \cdot 2 \cdot n^3 \text{ operations}$$

$\Rightarrow$ large impact on multivariate schemes over small fields (e.g. HFEv-)
$\Rightarrow$ no significant impact on multivariate schemes over large fields (e.g. HMFE)

Parameter Choice

How to choose the parameter k?

- Efficiency: Choose k as small as possible
- Security: too small k might make the scheme insecure

$\Rightarrow$ odd q: choose $k = 2$, choose the coefficients of $f^{(1)}$ and $f^{(2)}$ such that $p(X) = \det(F_1 + X \cdot F_2)$ is irreducible
$\Rightarrow$ even q: choose $k = 3$

Key Sizes and Comparison

quantum security level (bit)		public key size (kB)	private key size (kB)	signature size (bit)
80	Rainbow (GF(256),17,13,13)	25.1	19.9	344
	Gui (GF(2),120,9,3,3,2)	110.7	3.8	129
	HMFEv (GF(31),2,18,8)	**22.5**	**3.5**	**218**
	HMFEv (GF(256),3,9,12)	**21.6**	**6.0**	**312**
128	Rainbow (GF(256),36,21,22)	136.0	102.5	632
	Gui (GF(2),212,9,3,4,2)	592.8	11.6	222
	HMFEv (GF(31),2,28,12)	**81.8**	**8.9**	**337**
	HMFEv (GF(256),3,15,16)	**85.8**	**15.2**	**488**
256	Rainbow (GF(256),86,45,46)	1,415.7	1,046.3	1,416
	Gui (GF(2),464,9,7,8,2)	6,253.7	56.4	488
	HMFEv (GF(31),2,55,21)	**583.9**	**38.0**	**649**
	HMFEv (GF(256),3,31,26)	**659.4**	**65.3**	**952**

Comparison with HFEv-/Gui

Major advantages:

- fewer equations and variables in the public key
  $\Rightarrow$ smaller key sizes
- larger internal state
  $\Rightarrow$ no "double-signing" needed
  $\Rightarrow$ Easier to implement, greater efficiency
- larger field size
  $\Rightarrow$ easier to scale to higher levels of security

Implementation and Efficiency

Central step in signature generation: Inversion of $\mathcal{F}_V$
Two steps:

1. Gröbner Basis Step: Find a univariate polynomial $p : \mathbb{E} \to \mathbb{E}$ in the ideal $\langle f_V^{(1)}, \ldots, f_V^{(k)} \rangle$.
   k small $\Rightarrow$ can be performed efficiently by a specially designed algorithm
2. Solving Step: Solve the univariate polynomial p by Berlekamps algorithm

Efficiency

quantum security level (bit)		sign. gen. time (ms)	verification time (ms)
62	Gui (GF(2),96,5,6,6)	0.07	0.02
	Gui(GF(2),95,9,5,5)	0.18	0.02
	Gui(GF(2),94,17,4,4)	0.73	0.02
80	**HMFEv (GF(31),2,18,8)**	**0.131**	**0.0085**
	HMFEv (GF(256),3,9,12)	**0.261**	**0.0236**
83	Gui(127,9,4,6,2)	0.28	0.015
128	**HMFEv (GF(31),2,28,12)**	**0.26**	**0.0259**
	HMFEv (GF(256),3,15,16)	**0.443**	**0.063**

Conclusion

Proposal of a new efficient multivariate signature scheme of the HFEv-type which

- can be defined over large fields
  $\Rightarrow$ reduces the number of equations and variables $\Rightarrow$ smaller key sizes
  $\Rightarrow$ improves scalability to higher levels of security
- resists all known attacks against MPKCs
- is very efficient

$\Rightarrow$ HMFEv is a promising candidate for the upcoming standardization process of post-quantum signature schemes

The End

Thank you for your attention

Questions?