Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes

TECHNISCHE UNIVERSITÄT DARMSTADT

Albrecht Petzoldt, Stanislav Bulygin and Johannes Buchmann
TU Darmstadt, Germany

PQCrypto 2013
Limoges, France
05. June 2013

Outline

TECHNISCHE UNIVERSITÄT DARMSTADT

1. Motivation: Multivariate Cryptography
2. The UOV Signature Scheme
3. UOV Schemes with partially circulant Public Key
4. The Verification Process
5. Extension to Rainbow
6. Hybrid approach and Application to QUAD (→ eprint)
7. Experiments and Results
8. Conclusion

Multivariate Cryptography

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i \cdot x_j \quad &+ \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} = 0 \\
\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i \cdot x_j \quad &+ \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} = 0 \\
&\vdots \\
\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i \cdot x_j \quad &+ \quad \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)} = 0
\end{aligned}$$

Problem MQ: Finding a vector $\mathbf{x} = (x_1, \ldots, x_n)$ such that

$p^{(1)}(\mathbf{x}) = \ldots = p^{(m)}(\mathbf{x}) = 0$ is a hard task.

Multivariate Cryptography (2)

TECHNISCHE UNIVERSITÄT DARMSTADT

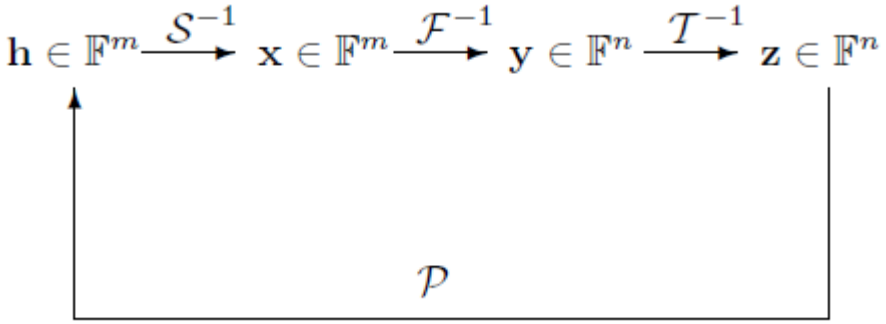
Construction

- Start with an easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \rightarrow \mathbb{F}^m$ (central map)
- Combine it with two invertible affine maps $\mathcal{S} : \mathbb{F}^m \rightarrow \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^n$
- The public key $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ is supposed to look like a random system

Multivariate Cryptography (3)

TECHNISCHE UNIVERSITÄT DARMSTADT

Signature Schemes



Signature generation: For a hashvalue $\mathbf{h} \in \mathbb{F}^m$ compute recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h})$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x})$ $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$ $\mathbf{z} \in \mathbb{F}^n$ and . The signature of the document is .

$\mathbf{z} \in \mathbb{F}^n$

Signature $\mathbf{h}' = \mathcal{P}(\mathbf{z})$n: T$\mathbf{h}' = \mathbf{h}$ the authenticity of a signature , one computes . If holds, the signature is accepted, otherwise rejected.

Multivariate Cryptography (4)

TECHNISCHE UNIVERSITÄT DARMSTADT

Advantages:

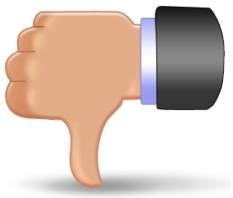
- Secure against attacks with quantum computers
- Great diversity of schemes and variations
- Enables fast en- and decryption as well as signature generation and verification
- Requires modest computational resources

  ➔ Can be implemented on low cost smart cards

Multivariate Cryptography (5)

TECHNISCHE UNIVERSITÄT DARMSTADT

Major Drawbacks



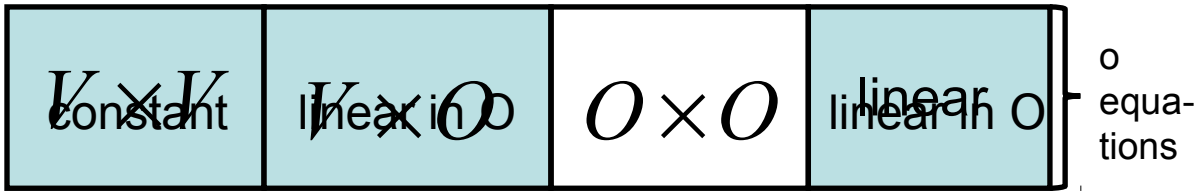
- Relatively young field of Research
  → Security is not so well understood
- No explicit parameter choices to meet given security levels known
- Large size of the public and private keys

➔ Multivariate Cryptography is not yet widely spread

The UOV Signature Scheme

TECHNISCHE UNIVERSITÄT DARMSTADT

- Two types of variables: Vinegar $V = \{x_1, \ldots, x_v\}$ and Oil $O = \{x_{v+1}, \ldots, x_{v+o}\}$
- Central map $\mathcal{F}$



- Inversion of $\mathcal{F}$

1. Choose the Vinegar variables at random
2. Solve the resulting linear system for the Oil variables

- Public Key: $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$ with an affine map $\mathcal{T} = (M_T, c_T)$.
- Private Key: $\mathcal{F}, \mathcal{T}$.

Partially Circulant UOV Schemes

TECHNISCHE UNIVERSITÄT DARMSTADT

- $D := \frac{v \cdot (v+1)}{2}$
- $\mathbf{b} = (b_1, \ldots, b_D) \in_R \mathbb{F}^D$
- $B[i] = \mathcal{R}^{i-1}(\mathbf{b}) \ (i = 1, \ldots, o)$

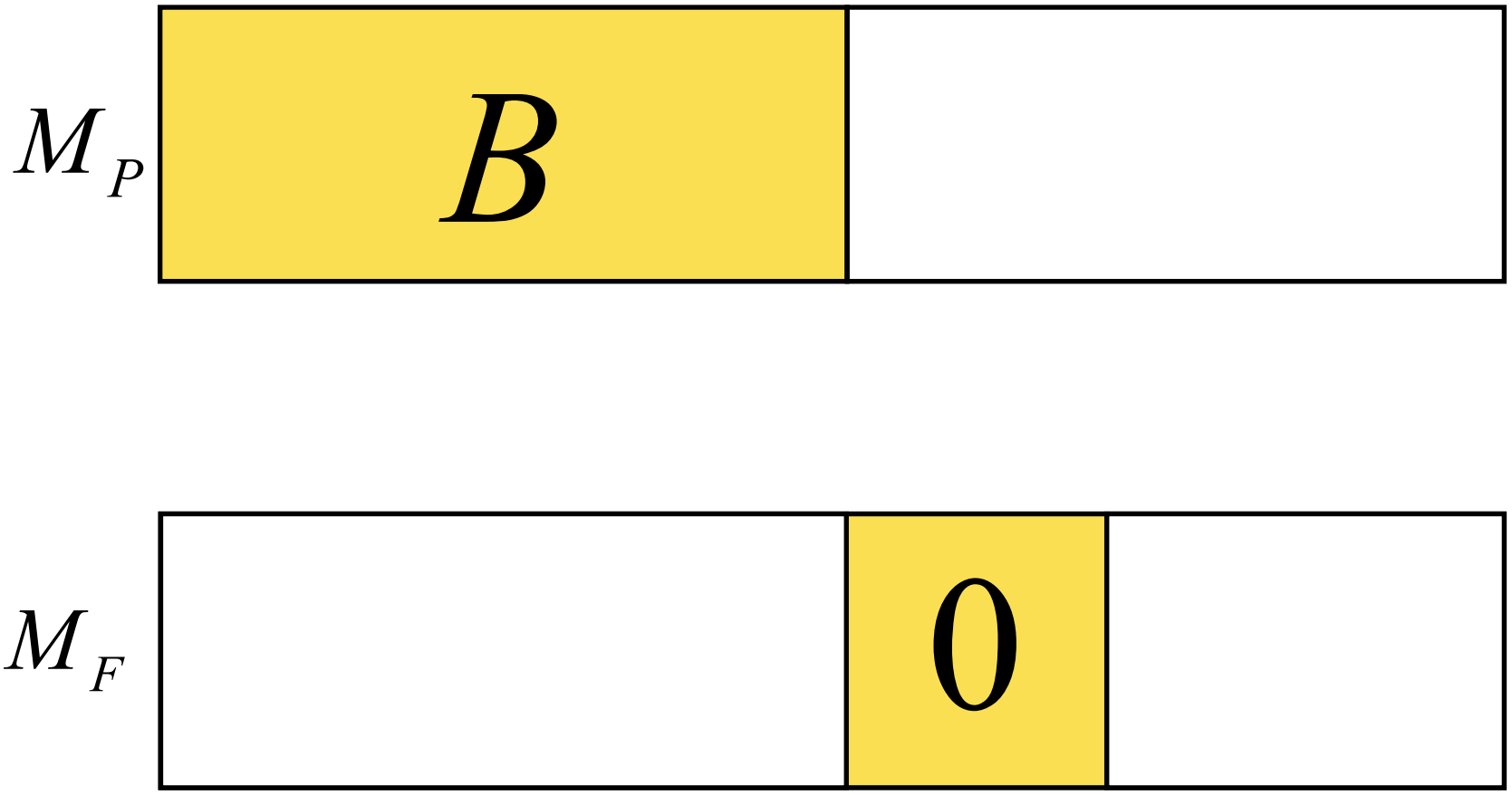
$$B = \begin{pmatrix} b_1 & b_2 & b_3 & \ldots & b_{D-1} & b_D \\ b_D & b_1 & b_2 & & b_{D-2} & b_{D-1} \\ \vdots & & & & & \vdots \\ b_{D-o+2} & b_{D-o+3} & b_{D-o+4} & \ldots & b_{D-o} & b_{D-o+1} \end{pmatrix}$$

- $M_T = (t_{ij})_{i,j=1}^{n}$
- $\alpha_{ij}^{rs} = \begin{cases} t_{ir} \cdot t_{js} & (i = j) \\ t_{ir} \cdot t_{is} + t_{is} \cdot t_{jr} & \text{otherwise} \end{cases}$

$$A = \begin{pmatrix} \alpha_{11}^{11} & \alpha_{12}^{11} & \ldots & \alpha_{vn}^{11} \\ \alpha_{11}^{12} & \alpha_{12}^{12} & & \alpha_{vn}^{12} \\ \vdots & & & \vdots \\ \alpha_{11}^{vn} & \alpha_{12}^{vn} & \ldots & \alpha_{vn}^{vn} \end{pmatrix}$$

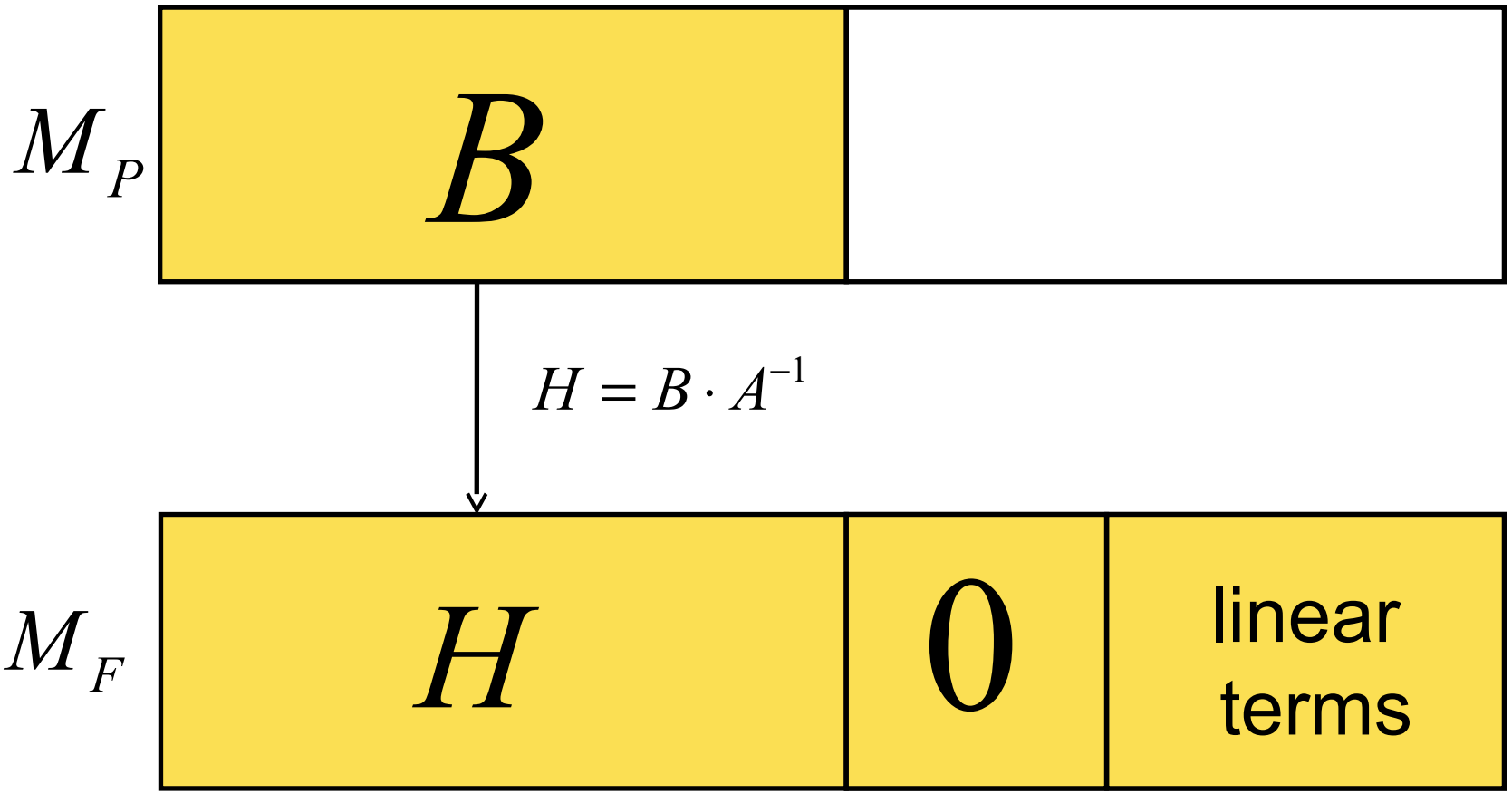
Partially Circulant UOV Schemes (2)

TECHNISCHE UNIVERSITÄT DARMSTADT



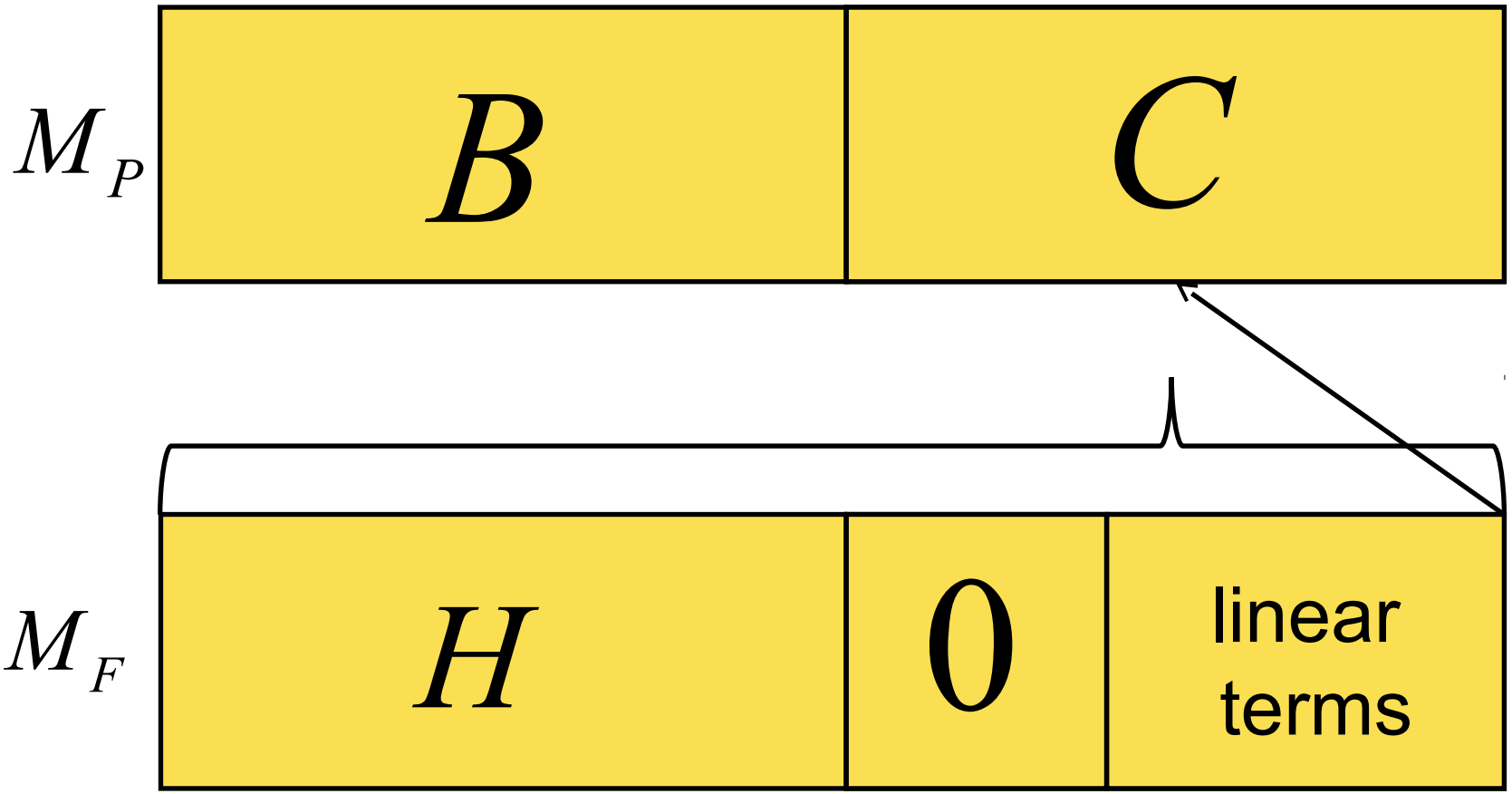
Partially Circulant UOV Schemes (2)

TECHNISCHE UNIVERSITÄT DARMSTADT



Partially Circulant UOV Schemes (2)

TECHNISCHE UNIVERSITÄT DARMSTADT



The verification process (1)

TECHNISCHE UNIVERSITÄT DARMSTADT

Standard approach

- Signature $\mathbf{z} = (z_1, \ldots, z_n)$
- Vector $\mathrm{mon} = (z_1^2, z_1 z_2, \ldots, z_n^2, z_1, \ldots, z_n, 1)$
- Macauley matrix

$$M_P = \begin{pmatrix} p_{11}^{(1)} & p_{12}^{(1)} & \cdots & p_{nn}^{(1)} & p_1^{(1)} & \cdots & p_n^{(1)} & p_0^{(1)} \\ p_{11}^{(2)} & p_{12}^{(2)} & \cdots & p_{nn}^{(2)} & p_1^{(2)} & \cdots & p_n^{(2)} & p_0^{(2)} \\ \vdots & & & & & & & \vdots \\ p_{11}^{(o)} & p_{12}^{(o)} & \cdots & p_{nn}^{(o)} & p_1^{(o)} & \cdots & p_n^{(o)} & p_0^{(o)} \end{pmatrix}$$

$$\mathcal{P}(\mathbf{z}) = \begin{pmatrix} M_P[1] \cdot \mathrm{mon}^T \\ \vdots \\ M_P[m] \cdot \mathrm{mon}^T \end{pmatrix}$$

The verification process (2)

TECHNISCHE UNIVERSITÄT DARMSTADT

Alternative approach

- extended signature vector $\text{sign} = (z_1, \ldots, z_n, 1)$
- Matrix $MP^{(k)}$

$$MP^{(k)} = \begin{pmatrix} p_{11}^{(k)} & p_{12}^{(k)} & p_{13}^{(k)} & \cdots & p_{1n}^{(k)} & p_1^{(k)} \\ 0 & p_{22}^{(k)} & p_{23}^{(k)} & \cdots & p_{2n}^{(k)} & p_2^{(k)} \\ 0 & 0 & p_{33}^{(k)} & & p_{3n}^{(k)} & p_3^{(k)} \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & p_{nn}^{(k)} & p_n^{(k)} \\ 0 & 0 & \ldots & 0 & 0 & p_0^{(k)} \end{pmatrix}$$

$$\mathcal{P}(\mathbf{z}) = \begin{pmatrix} \text{sign} \cdot MP^{(1)} \cdot \text{sign}^T \\ \text{sign} \cdot MP^{(2)} \cdot \text{sign}^T \\ \vdots \\ \text{sign} \cdot MP^{(o)} \cdot \text{sign}^T \end{pmatrix}$$

Example (o,v)=(2,4)

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\text{sign} \cdot MP^{(1)} \cdot \text{sign}^T = (s_1, \ldots, s_6, 1) \cdot \begin{pmatrix} a & b & c & d & e & f & \star \\ 0 & g & h & i & j & k & \star \\ 0 & 0 & l & m & n & o & \star \\ 0 & 0 & 0 & p & q & r & \star \\ 0 & 0 & 0 & 0 & \star & \star & \star \\ 0 & 0 & 0 & 0 & 0 & \star & \star \\ 0 & 0 & 0 & 0 & 0 & 0 & \star \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ 1 \end{pmatrix}$$

=(as_1, bs_1+gs_2, $cs_1+hs_2+ls_3$, $ds_1+is_2+ms_3+ps_4$, $es_1+js_2+ns_3+qs_4+\star$,
$fs_1+ks_2+os_3+rs_4+\star$, $\star$) $\cdot (s_1, \ldots, s_6, 1)^T$

$$\text{sign} \cdot MP^{(2)} \cdot \text{sign}^T = (s_1, \ldots, s_6, 1) \cdot \begin{pmatrix} r & a & b & c & d & e & \star \\ 0 & f & g & h & i & j & \star \\ 0 & 0 & k & l & m & n & \star \\ 0 & 0 & 0 & o & p & q & \star \\ 0 & 0 & 0 & 0 & \star & \star & \star \\ 0 & 0 & 0 & 0 & 0 & \star & \star \\ 0 & 0 & 0 & 0 & 0 & 0 & \star \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ 1 \end{pmatrix}$$

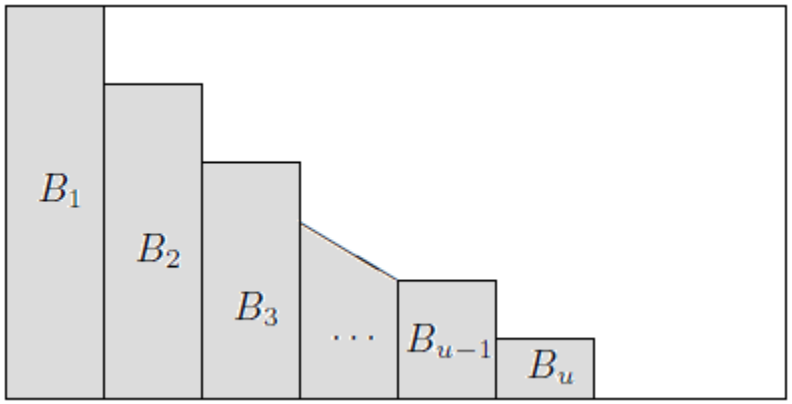
= (rs_1, as_1+fs_2, $bs_1+gs_2+ks_3$, $cs_1+hs_2+ls_3+os_4$, $ds_1+is_2+ms_3+ps_4+\star$,
$es_1+js_2+ns_3+qs_4+\star$, $\star$) $\cdot (s_1, \ldots, s_6, 1)^T$

Extension to Rainbow

TECHNISCHE UNIVERSITÄT DARMSTADT

- Several layers of Oil and Vinegar

M_P



Use the same idea as for UOV for each Rainbow layer separately

Hybrid approach (→ eprint)

TECHNISCHE UNIVERSITÄT DARMSTADT

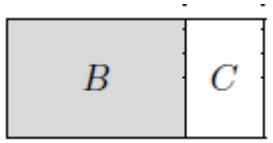
- Evaluate the structured part with the alternative approach and the random looking part with the standard approach

UOV

$$MP^{(k)} = \begin{pmatrix} p_{11}^{(k)} & p_{12}^{(k)} & \cdots & p_{1v}^{(k)} & p_{1,v+1} & \cdots & p_{1,n-1}^{(k)} & p_{1,n}^{(k)} \\ 0 & p_{22}^{(k)} & \cdots & p_{2v}^{(k)} & p_{2,v+1}^{(k)} & \cdots & p_{2,n-1}^{(k)} & p_{2,n}^{(k)} \\ 0 & 0 & \ddots & & & & & \vdots \\ 0 & \cdots & 0 & p_{v,v}^{(k)} & p_{v,v+1}^{(k)} & \cdots & p_{v,n-1}^{(k)} & p_{v,n}^{(k)} \end{pmatrix} \in \mathbb{F}^{v \times n}$$

$$\text{mon} = (z_{v+1}^2, z_{v+1} \cdot z_{v+2}, z_{v+1} \cdot z_{v+3}, \ldots, z_n^2, z_1, z_2, \ldots, z_n, 1)$$

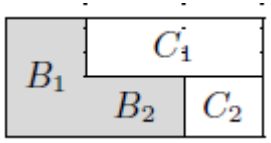
$$p^{(k)}(x_1, \ldots, x_n) = \underbrace{(x_1, \ldots, x_v) \cdot MP^{(k)} \cdot (x_1, \ldots, x_n)^T}_{\text{structured part}} + \underbrace{C[k] \cdot \text{mon}^T}_{\text{random part}}$$



Hybrid approach (2)

TECHNISCHE UNIVERSITÄT DARMSTADT

Rainbow



First layer

$k = v_1+1, \ldots, v_2$

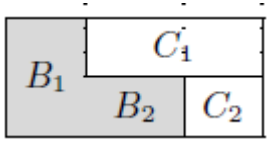
$$MP^{(k)} = \begin{pmatrix} p_{11}^{(k)} & p_{12}^{(k)} & \cdots & p_{1,v_1}^{(k)} & p_{1,v_1+1} & \cdots & p_{1,v_2-1}^{(k)} & p_{1,v_2}^{(k)} \\ 0 & p_{22}^{(k)} & \cdots & p_{2,v_1}^{(k)} & p_{2,v_1+1}^{(k)} & \cdots & p_{2,v_2-1}^{(k)} & p_{2,v_2}^{(k)} \\ 0 & 0 & \ddots & & & & & \vdots \\ 0 & 0 & 0 & p_{v_1,v_1}^{(k)} & p_{v_1,v_1+1}^{(k)} & \cdots & p_{v_1,v_2-1}^{(k)} & p_{v_1,v_2}^{(k)} \end{pmatrix} \in \mathbb{F}^{v_1 \times v_2}$$

$$\text{mon}^{(1)} = (z_1 z_{v_2+1}, z_1 z_{v_2+2}, \ldots, z_1 z_n, z_2 z_{v_2+1}, \ldots z_{v_1} z_n, z_{v_1+1}^2, z_{v_1+1} z_{v_1+2}, \ldots, z_{v_1+1} z_n, z_{v_1+2}^2, \ldots, z_n^2, z_1, \ldots, z_n, 1)$$

$$p^{(k)}(x_1, \ldots, x_n) = \underbrace{(x_1, \ldots, x_{v_1}) \cdot MP^{(k)} \cdot (x_1, \ldots, x_{v_2})^T}_{\text{structured part}} + \underbrace{C_1[k - v_1] \cdot (\text{mon}^{(1)})^T}_{\text{random part}}$$

Hybrid approach (3)

Rainbow



Second layer

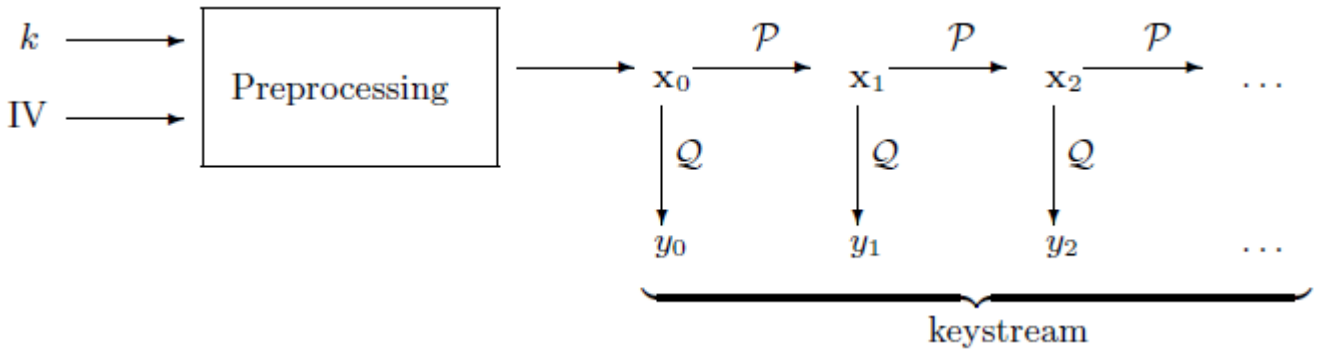
$k = v_2{+}1, \ldots, n$

$$MP^{(k)} = \begin{pmatrix} p_{11}^{(k)} & p_{12}^{(k)} & \cdots & p_{1,v_2}^{(k)} & p_{1,v_2+1} & \cdots & p_{1,n-1}^{(k)} & p_{1,n}^{(k)} \\ 0 & p_{22}^{(k)} & \cdots & p_{2,v_2}^{(k)} & p_{2,v_2}^{(k)} & \cdots & p_{2,n-1}^{(k)} & p_{2,n}^{(k)} \\ 0 & 0 & \ddots & & & & & \vdots \\ 0 & 0 & 0 & p_{v_2,v_2}^{(k)} & p_{v_2,v_2+1}^{(k)} & \cdots & p_{v_2,n-1}^{(k)} & p_{v_2,n}^{(k)} \end{pmatrix} \in \mathbb{F}^{v_2 \times n}$$

$$\mathrm{mon}^{(2)} = (z_{v_2+1}^2, z_{v_2+1}z_{v_2+2}, \ldots, z_{v_2+1}z_n, z_{v_2+2}^2, \ldots, z_n^2, z_1, \ldots, z_n, 1)$$

$$\Rightarrow \quad p^{(k)}(x_1, \ldots, x_n) = \underbrace{(x_1, \ldots, x_{v_2}) \cdot MP^{(k)} \cdot (x_1, \ldots, x_n)^T}_{\text{structured part}} + \underbrace{C_2[k - v_2] \cdot (\mathrm{mon}^{(2)})^T}_{\text{random part}}$$

Application to QUAD (→ eprint)



- The systems $\mathcal{P}$ and $\mathcal{Q}$ can be chosen partially circulant
- Experiments indicate that this does not weaken the security of the scheme

→ Key stream generation can be sped up significantly

Experiments and Results (1)

TECHNISCHE UNIVERSITÄT DARMSTADT

- Implementation in C
- Lenovo ThinkPad, Intel Core 2Duo 2.53 GHz, 4 GB RAM

	Public key size (kB)	reduction factor	Verification time (ms)	Speed up factor
UOV(256,28,56)	99.9		0.98 (standard)	
cyclicUOV(256,28,56)	16.5	6.1	0.20 (alternative)	4.9
			0.18 (hybrid)	5.5
UOV(31,33,66)	108.5		1.75 (standard)	
cyclicUOV(31,33,66)	17.1	6.3	0.34 (alternative)	5.5
			0.32 (hybrid)	5.7

Experiments and Results (2)

TECHNISCHE UNIVERSITÄT DARMSTADT

	Public key size (kB)	reduction factor	Verification time (ms)	Speed up factor
Rainbow(256,17,13,13)	25.1		0.26 (standard)	
cyclicRainbow (256,17,13,13)	9.5	2.6	0.12 (alternative)	2.1
			0.12 (hybrid)	2.1
Rainbow(31,14,19,14)	25.3		0.45 (standard)	
cyclicRainbow (31,14,19,14)	9.5	2.6	0.22 (alternative)	2.0
			0.19 (hybrid)	2.3

Experiments and Results (3)

TECHNISCHE UNIVERSITÄT DARMSTADT

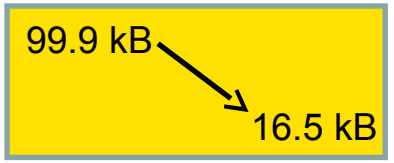
	Data throughput (kB/s)	CPUcycles/byte	Speed up factor
QUAD(16,30)	71.7	35,265	
cyclicQUAD(16,30)	458.3	5,513	6.4
QUAD(256,26)	157.3	15,777	
cyclicQUAD(256,26)	853.6	2,820	5.5

Conclusion

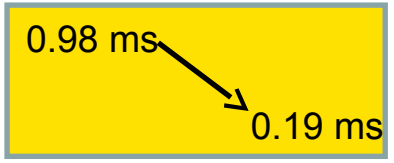
TECHNISCHE UNIVERSITÄT DARMSTADT

Structured versions of UOV

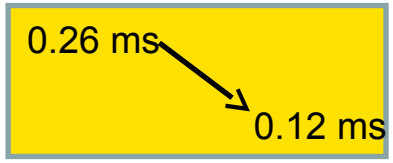
- Reduce public key size

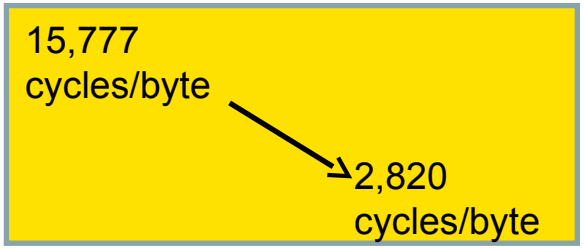


- Speed up the verification process



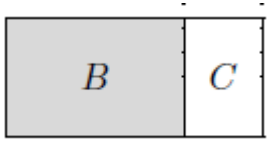
- Technique can be extended to Rainbow and QUAD





Thank you for your attention

TECHNISCHE UNIVERSITÄT DARMSTADT



$$\mathcal{P}(\mathbf{z}) = \begin{pmatrix} \text{sign} \cdot MP^{(1)} \cdot \text{sign}^T \\ \text{sign} \cdot MP^{(2)} \cdot \text{sign}^T \\ \vdots \\ \text{sign} \cdot MP^{(o)} \cdot \text{sign}^T \end{pmatrix}$$

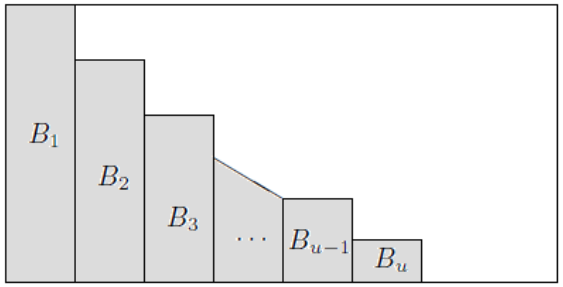
0.98 ms → 0.19 ms

Questions?

www.eprint.iacr.org/2013/263

www.eprint.iacr.org/2013/315

$$\mathcal{P}(\mathbf{z}) = \begin{pmatrix} M_P[1] \cdot \text{mon}^T \\ \vdots \\ M_P[m] \cdot \text{mon}^T \end{pmatrix}$$



0.26 ms → 0.12 ms

$$p^{(k)}(x_1, \ldots, x_n) = \underbrace{(x_1, \ldots, x_v) \cdot MP^{(k)} \cdot (x_1, \ldots, x_n)^T}_{\text{structured part}} + \underbrace{C[k] \cdot \text{mon}^T}_{\text{random part}}$$