Multivariate Cryptography
Part 2: UOV and Rainbow

Albrecht Petzoldt

PQCrypto Summer School 2017
Eindhoven, Netherlands
Tuesday, 20.06.2017

Oil-Vinegar Polynomials [Pa97]

Let $\mathbb{F}$ be a (finite) field. For $o, v \in \mathbb{N}$ set $n = o + v$ and define

$$p(x_1, \ldots, x_n) = \underbrace{\sum_{i=1}^{v}\sum_{j=i}^{v} \alpha_{ij} \cdot x_i \cdot x_j}_{v \times v \text{ terms}} + \underbrace{\sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ij} \cdot x_i \cdot x_j}_{v \times o \text{ terms}} + \underbrace{\sum_{i=1}^{n} \gamma_i \cdot x_i}_{\text{linear terms}} + \delta$$

- $x_1, \ldots, x_v$: Vinegar variables
- $x_{v+1}, \ldots, x_n$: Oil variables
- not fully mixed: no $o \times o$ terms

$v \times v$ terms	$v \times o$ terms	$o \times o$ terms	v terms	o terms	
quadratic	quadratic	0	linear in v	linear in o	δ

Oil-Vinegar Polynomials (2)

Let $\tilde{p}(x_1, \ldots, x_n)$ be the homogeneous quadratic part of $p(x_1, \ldots, x_n)$

$\tilde{p}$ can be written as quadratic form

$$\tilde{p}(x_1, \ldots, x_n) = (x_1, \ldots, x_n) \cdot M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ with}$$

$$M = \left(\begin{array}{ccc|ccc} \star & \ldots & \star & \star & \ldots & \star \\ \vdots & & \vdots & \vdots & & \vdots \\ \star & \ldots & \star & \star & \ldots & \star \\ \hline \star & \ldots & \star & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \star & \ldots & \star & 0 & \ldots & 0 \end{array}\right) \begin{matrix} \\ \\ \\ v \\ \\ \\ \end{matrix}$$

$$\begin{matrix} & & & v & & \end{matrix}$$

The Oil and Vinegar Signature Scheme - Key Generation

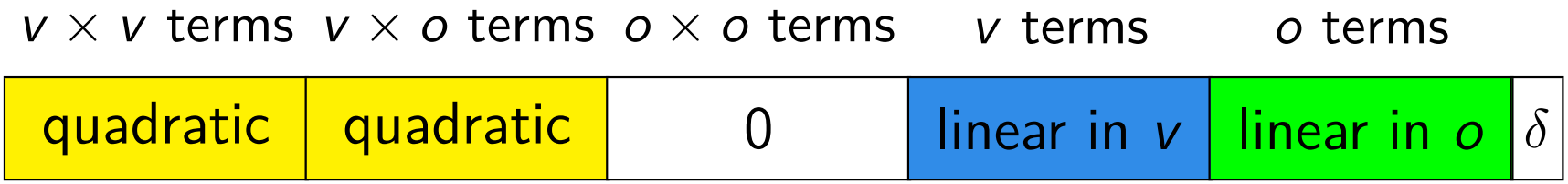
- Parameters: finite field $\mathbb{F}$, integers o, v, set $n = o + v$
- central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ consists of o Oil-Vinegar polynomials $f^{(1)}, \ldots, f^{(o)}$, i.e.

$$f^{(k)} = \sum_{i=1}^{v}\sum_{j=1}^{v} \alpha_{ij}^{(k)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} \gamma_i^{(k)} x_i + \delta^{(k)}$$

  with $\alpha_{ij}^{(k)}, \beta_{ij}^{(k)}, \gamma_i^{(k)}$ and $\delta^{(k)} \in_R \mathbb{F}$ $(1 \leq k \leq o)$.
- Compose $\mathbb{F}$ with a randomly chosen invertible affine map $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^o$
- *private key*: $\mathcal{F}, \mathcal{T}$

Inversion of the central map

Each central polynomial has the form



Inversion of the central map

Each central polynomial has the form

$v \times v$ terms	$v \times o$ terms	$o \times o$ terms	v terms	o terms	
quadratic	quadratic	0	linear in v	linear in o	δ

Choose random values for the Vinegar variables $x_1, \ldots, x_v$

$v \times v$ terms	$v \times o$ terms	$o \times o$ terms	v terms	o terms	
constant	linear in o	0	constant	linear in o	δ

$\Rightarrow$ Linear equation in the o Oil variables

Inversion of the central map (2)

Altogether we get o linear equations in the o variables $x_{v+1}, \ldots, x_n$

$\Rightarrow x_{v+1}, \ldots, x_n$ can be recovered by Gaussian elimination

If the system has no solution, choose other values for the Vinegar variables $x_1, \ldots, x_v$ and try again.

Toy Example

- $\mathbb{F} = \mathrm{GF}(7)$ and $o = v = 2$
- $\mathcal{F} = (f^{(1)}, f^{(2)})$ with

$$f^{(1)}(\mathbf{x}) = 2x_1^2 + 3x_1x_2 + 6x_1x_3 + x_1x_4 + 4x_2^2 + 5x_2x_4 + 3x_1 + 2x_2 + 5x_3 + x_4 + 6,$$
$$f^{(2)}(\mathbf{x}) = 3x_1^2 + 6x_1x_2 + 5x_1x_4 + 3x_2^2 + 5x_2x_3 + x_2x_4 + 2x_1 + 5x_2 + 4x_3 + 2x_4 + 1.$$

- Goal: Find a pre image $\mathbf{x} = (x_1, x_2, x_3, x_4)$ of $\mathbf{w} = (3, 4)$ under the central map $\mathcal{F}$.
- Choose random values for x_1 and x_2, e.g. $(x_1, x_2) = (1, 4)$, and substitute them into $f^{(1)}$ and $f^{(2)}$
  $\Rightarrow \tilde{f}^{(1)}(x_3, x_4) = 4x_3 + x_4 + 4,\ \tilde{f}^{(2)}(x_3, x_4) = 3x_3 + 4x_4$
- Solve linear system $\tilde{f}^{(1)} = w_1 = 3,\ \tilde{f}^{(2)} = w_2 = 4$
  $\Rightarrow (x_3, x_4) = (1, 2)$

The pre image of $\mathbf{w}$ is $\mathbf{x} = (1, 4, 1, 2)$.

Signature Generation

Given: message d

1. Use a hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}^o$ to compute $\mathbf{w} = \mathcal{H}(d)$
2. Compute a pre-image $\mathbf{x} \in \mathbb{F}^n$ of $\mathbf{w}$ under the central map $\mathcal{F}$
   - Choose random values for the Vinegar variables $x_1, \ldots, x_v$ and substitute them into the central map polynomials $f^{(1)}, \ldots, f^{(o)}$
   - Solve the resulting linear system for the Oil variables $x_{v+1}, \ldots, x_n$
   - If the system has no solution, choose other values for the Vinegar variables and try again.
3. Compute the signature $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{x})$.

Signature Verification

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

1. Compute $\mathbf{w} = \mathcal{H}(d)$.
2. Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z})$.

Accept the signature $\Leftrightarrow \mathbf{w} = \mathbf{w}$

The attack of Kipnis and Shamir on balanced OV [KS98]

Define

$$\begin{aligned} \mathcal{O} &:= \{\mathbf{x} \in \mathbb{F}^n : x_1 = \ldots = x_v = 0\} \quad \text{“Oilspace”} \\ \mathcal{V} &:= \{\mathbf{x} \in \mathbb{F}^n : x_{v+1} = \ldots = x_n = 0\} \quad \text{“Vinegarspace”} \end{aligned}$$

Let E be an “OV-matrix”, i.e. $E = \begin{pmatrix} \star & \star \\ \star & 0 \end{pmatrix}$ and $o \in \mathcal{O}$. Then we have $E \cdot o \in \mathcal{V}$ or $E \cdot \mathcal{O} \subset \mathcal{V}$. Analogously, we get $E^{-1} \cdot \mathcal{V} \subset \mathcal{O}$. For two OV matrices E and F we therefore get

$$(F^{-1} \cdot E) \cdot \mathcal{O} \subset \mathcal{O},$$

i.e. $\mathcal{O}$ is an invariant subspace of the matrix $F^{-1} \cdot E$.

OV Attack (2)

Let G_i be the matrix representing the homogeneous quadratic part of the i-th public polynomial. Then we have

$$G_i = T^T \cdot E_i \cdot T,$$

with E being an OV-matrix and T being the matrix representing $\mathcal{T}$. Let $o \in \mathcal{O}$ and $v = T^{-1}(o)$. We therefore get

$$\begin{aligned}(G_j^{-1} G_i) \cdot v &= (T^{-1} \cdot E_j^{-1} \cdot (T^T)^{-1} \cdot T^T \cdot E_i \cdot T) \cdot T^{-1}(o) \\ &= T^{-1} \cdot E_j^{-1} \cdot E_i \cdot o \in T^{-1}(\mathcal{O}),\end{aligned}$$

i.e. $T^{-1}(\mathcal{O})$ is an invariant subspace of the matrix $(G_j^{-1} \cdot G_i)$.

OV Attack (3)

1. Choose an index $j \in \{1, \ldots, o\}$ such that G_j is invertible and compute $G_j^{-1} \cdot G_i$
2. Compute the inverant subspaces of $G_j^{-1} \cdot G_i$
   $\Rightarrow$ Separation of Oil and Vinegar Variables
   $\Rightarrow$ Find equivalent affine transformation $\mathcal{T}$
   $\Rightarrow$ Find equivalent central map $\mathcal{F}$ by $\mathcal{F} = \mathcal{P} \circ \mathcal{T}^{-1}$

OV Attack - Summary

- The attack breaks the balanced OV scheme in polynomial time.
- The attack works also for $v < o$
- For $v > o$ the complexity of the attack is about $q^{v-o} \cdot o^4$.

$\Rightarrow$ Choose $v \approx 2 \cdot o$ (unbalanced Oil and Vinegar (UOV)) [KP99]

Other Attacks

- **Collision Attack**: To prevent collision attacks against the hash function, one needs $o \geq \frac{\text{seclev}}{\text{Log}_2(q)}$.
- **Direct Attack**: Try to solve the public equation $\mathcal{P}(\mathbf{z}) = \mathbf{w}$ as an instance of the MQ-Problem
  $\Rightarrow$ public systems of UOV behave much like random systems
  However: The public systems of UOV are highly underdetermined ($n = 3 \cdot m$)

  Result [Thomae]: A multivariate system of m equations in $n = \omega \cdot m$ variables can be solved in the same time as a determined system of $m - \lfloor \omega \rfloor + 1$ equations.

  $\Rightarrow$ m has to be increased by 2.

Other Attacks (2)

- **UOV-Reconciliation attack**: Try to find a linear transformation $\mathcal{T}$ which transforms the public matrices G_i into the form of UOV matrices

$$(T^T)^{-1} \cdot G_i \cdot T^{-1} = \begin{pmatrix} \star & \star \\ \star & 0 \end{pmatrix}$$

$\Rightarrow$ Each Zero-term yields a quadratic equation in the elements of T.
$\Rightarrow$ T can be recovered by solving several systems of multivariate quadratic equations

Parameters

security level (bit)	scheme	public key size (kB)	private key size (kB)	hash size (bit)	signature (bit)
80	UOV(GF(16),40,80)	144.2	135.2	160	480
	UOV(GF(256),27,54)	89.8	86.2	216	648
100	UOV(GF(16),50,100)	280.2	260.1	200	600
	UOV(GF(256), 34,68)	177.8	168.3	272	816
128	UOV(GF(16),64,128)	585.1	538.1	256	768
	UOV(GF(256),45,90)	409.4	381.8	360	1,080
192	UOV(GF(16),96,192)	1,964.3	1,786.7	384	1,152
	UOV(GF(256),69,138)	1,464.6	1,344.0	552	1,656
256	UOV(GF(16),128,256)	4,644.1	4,200.3	512	1,536
	UOV(GF(256),93,186)	3,572.9	3,252.2	744	2,232

UOV - Summary

- unbroken since 1999 $\Rightarrow$ high confidence in security
- not the fastest multivariate scheme
- very large key sizes
- (comparably) large signatures

$\Rightarrow$ Can we do better?

The Rainbow Signature Scheme

- proposed in 2005 by J. Ding and D. Schmidt [DS05]
- multi layer version of UOV
- reduces number of variables in the public key
  $\Rightarrow$ better performance
  $\Rightarrow$ smaller key sizes
  $\Rightarrow$ smaller signatures

Key Generation

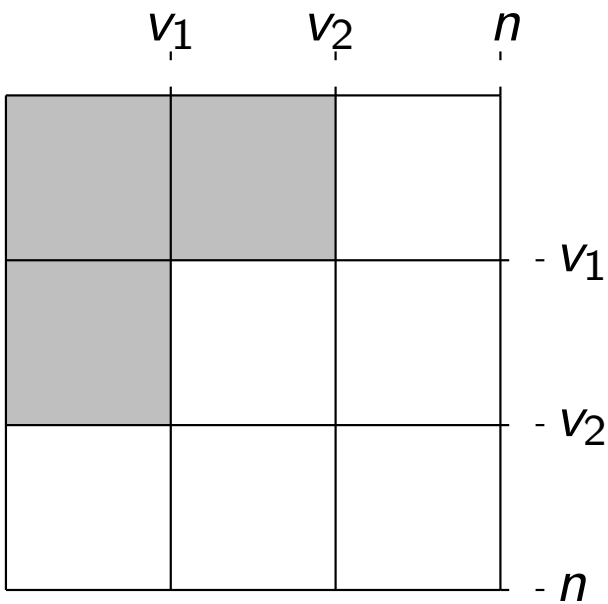
- Finite field $\mathbb{F}$, integers $0 < v_1 < \cdots < v_u < v_{u+1} = n$.
- Set $V_i = \{1, \ldots, v_i\}$, $O_i = \{v_i + 1, \ldots, v_{i+1}\}$, $o_i = v_{i+1} - v_i$.
- Central map $\mathcal{F}$ consists of $m = n - v_1$ polynomials $f^{v_1+1}, \ldots, f^{(n)}$ of the form

$$f^{(k)} = \sum_{i,j \in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \delta^{(k)},$$

  with coefficients $\alpha_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\gamma_i^{(k)}$ and $\delta^{(k)}$ randomly chosen from $\mathbb{F}$ and ℓ being the only integer such that $k \in O_\ell$.
- Choose randomly two affine (or linear) transformations $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$.
- *public key*: $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$
- *private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

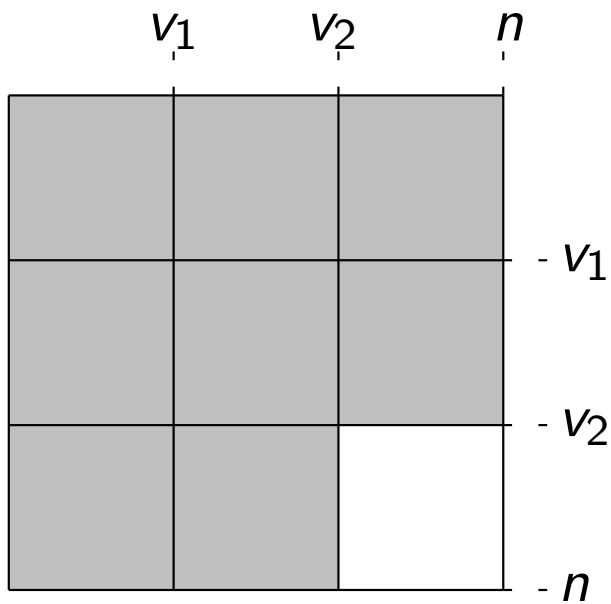
Rainbow schemes with two layers

$F^{(k)} =$



$v_1 + 1 \leq k \leq v_2$

$F^{(k)} =$



$v_2 + 1 \leq k \leq n$

Inversion of the central map

Idea:

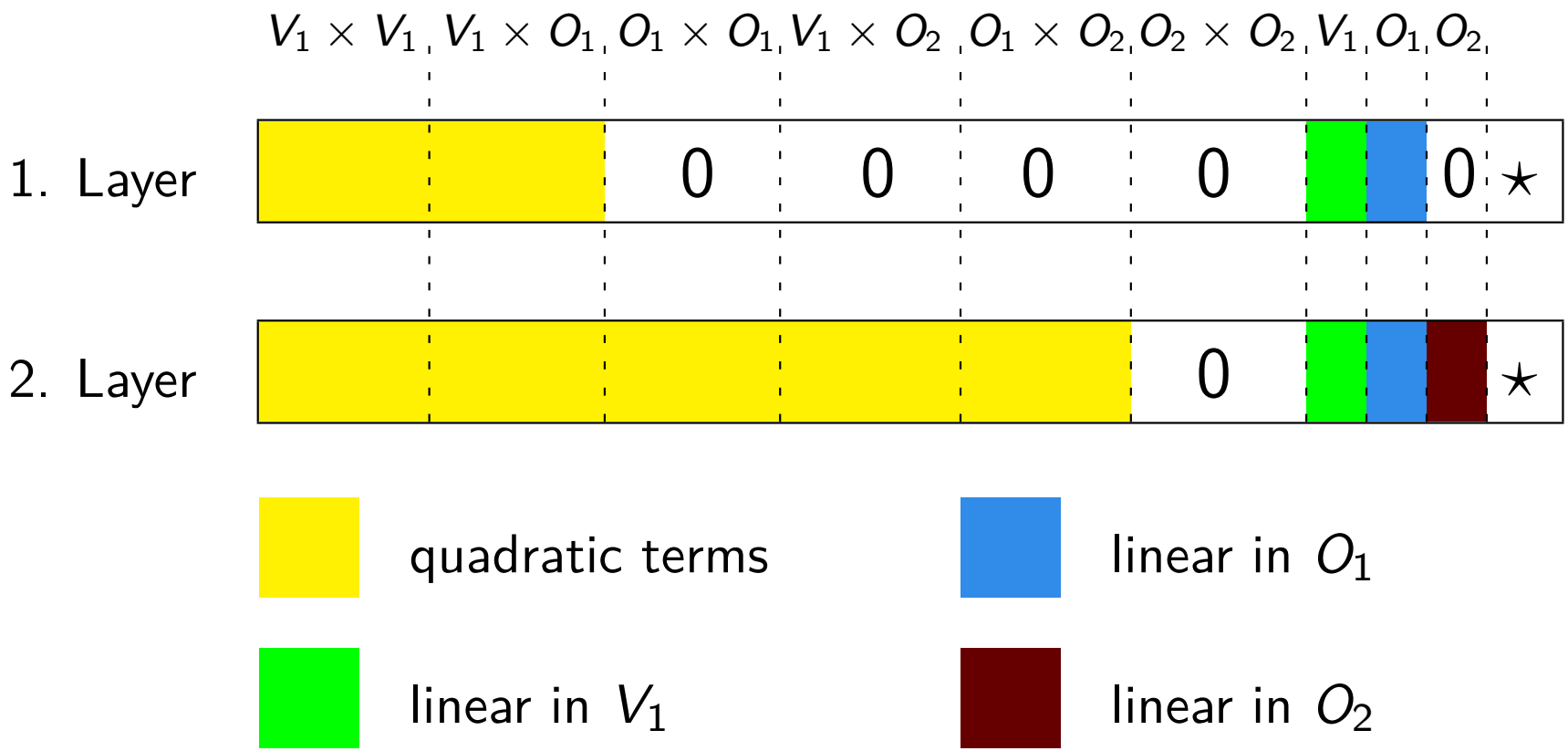
- Invert the single UOV layers recursively.
- Use the variables of the i-th layer as the Vinegar variables of the $i+1$-th layer.

Input: Rainbow central map $\mathcal{F} = (f^{(v_1+1)}, \ldots, f^{(n)})$, vector $\mathbf{y} \in \mathbb{F}^m$.
Output: vector $\mathbf{x} \in \mathbb{F}^n$ with $\mathcal{F}(\mathbf{x}) = \mathbf{y}$.

1: Choose random values for the variables $x_1, \ldots, x_{v_1}$ and substitute these values into the polynomials $f^{(i)}$ $(i = v_1 + 1, \ldots n)$.
2: **for** $\ell = 1$ to u **do**
3: Perform Gaussian Elimination on the polynomials $f^{(i)}$ $(i \in O_\ell)$ to get the values of the variables x_i $(i \in O_\ell)$.
4: Substitute the values of x_i $(i \in O_\ell)$ into the polynomials $f^{(i)}$ $(i = v_{\ell+1} + 1, \ldots, n)$.
5: **end for**

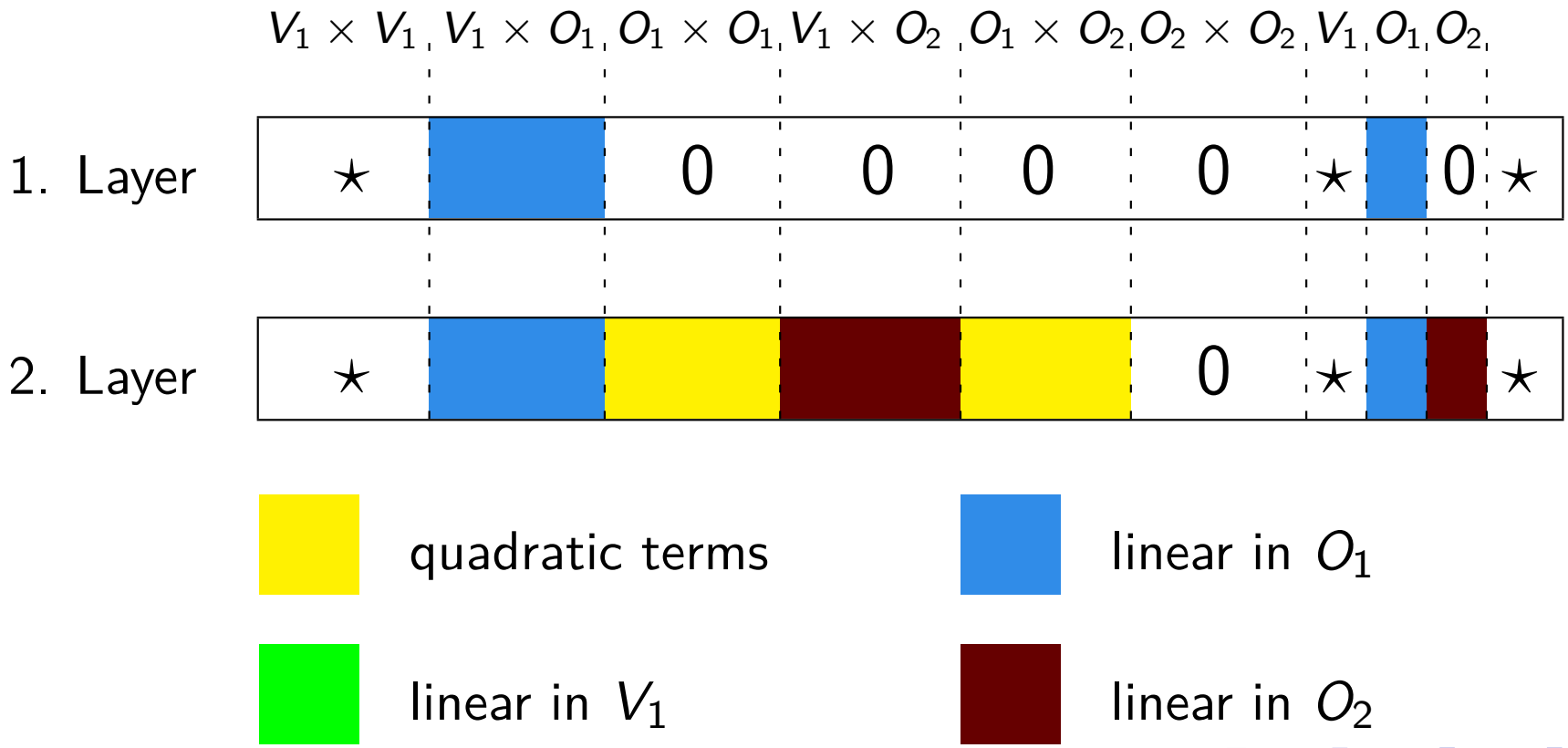
Rainbow Schemes with two layers

The central map $\mathcal{F}$ consists of quadratic polynomials of two types



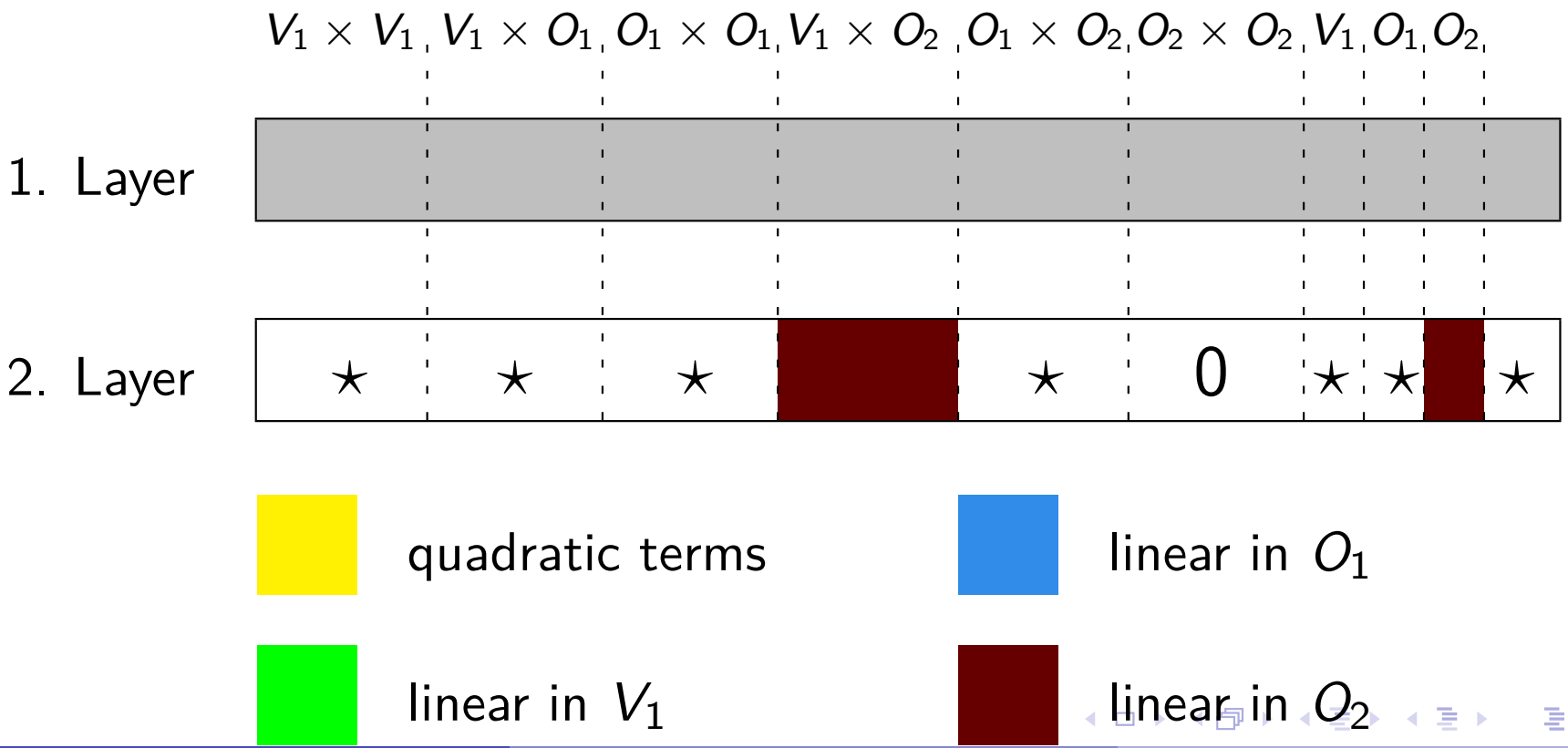
Rainbow Schemes with two layers

Step 1: Choose random values for the Vinegar variables $x_1, \ldots, x_{v_1}$ and substitute them into the central polynomials



Rainbow Schemes with two layers

Step 2: Solve the o_1 linear equations given by the polynomials of the first layer for $x_{v_1+1}, \ldots, x_{v_2}$ and substitute into the polynomials of the second layer



Rainbow Schemes with two layers

Step 3: Solve the o_2 linear equations given by the o_2 polynomials of the second layer for $x_{v_2+1}, \ldots, v_n$.

Toy Example

- $\mathbb{F} = \mathrm{GF}(7)$, $(v_1, o_1, o_2) = (2, 2, 2)$
- central map $\mathcal{F} = (f^{(3)}, \ldots, f^{(6)})$ with

$$
\begin{aligned}
f^{(3)} &= x_1^2 + 3x_1x_2 + 5x_1x_3 + 6x_1x_4 + 2x_2^2 + 6x_2x_3 + 4x_2x_4 + 2x_2 + 6x_3 + 2x_4 + 5,\\
f^{(4)} &= 2x_1^2 + x_1x_2 + x_1x_3 + 3x_1x_4 + 4x_1 + x_2^2 + x_2x_3 + 4x_2x_4 + 6x_2 + x_4,\\
f^{(5)} &= 2x_1^2 + 3x_1x_2 + 3x_1x_3 + 3x_1x_4 + x_1x_5 + 3x_1x_6 + 6x_1 + 4x_2^2 + x_2x_3 + 4x_2x_4\\
&+ x_2x_5 + 3x_2x_6 + 3x_2 + 3x_3x_4 + x_3x_5 + 2x_3x_6 + 2x_3 + 3x_4x_5 + x_5 + 6x_6,\\
f^{(6)} &= 2x_1^2 + 5x_1x_2 + x_1x_3 + 5x_1x_4 + 5x_1x_6 + 6x_1 + 5x_2^2 + 3x_2x_3 + 5x_2x_5 + 4x_2x_6\\
&+ x_2 + 3x_3^2 + 5x_3x_4 + 4x_3x_5 + 2x_3x_6 + 4x_3 + x_4^2 + 6x_4x_5 + 3x_4x_6\\
&+ 4x_4 + 4x_5 + x_6 + 2.
\end{aligned}
$$

- Goal: Find pre image $\mathbf{x} \in \mathbb{F}^6$ of $\mathbf{y} = (6, 2, 0, 5)$ under the map $\mathcal{F}$

Toy Example (2)

- Choose random values for the Vinegar variables x_1 and x_2, e.g. $(x_1, x_2) = (0, 1)$ and substitute them into the polynomials $f^{(3)}, \ldots, f^{(6)}$.

$$\begin{aligned}
\tilde{f}^{(3)} &= 5x_3 + 6x_4 + 2, \tilde{f}^{(4)} = x_3 + 5x_4, \\
\tilde{f}^{(5)} &= 3x_3x_4 + x_3x_5 + 2x_3x_6 + 3x_3 + 3x_4x_5 + 4x_4 + 2x_5 + 2x_6, \\
\tilde{f}^{(6)} &= 3x_3^2 + 5x_3x_4 + 4x_3x_5 + 2x_3x_6 + x_4^2 + 6x_4x_5 + 3x_4x_6 + 4x_4 + 2x_5 + 5x_6 + 1.
\end{aligned}$$

- Set $\tilde{f}^{(3)} = y_1 = 6$ and $\tilde{f}^{(4)} = y_2 = 2$ and solve for x_3, x_4
  $\Rightarrow (x_3, x_4) = (3, 4)$
- Substitute into $\tilde{f}^{(5)}$ and $\tilde{f}^{(6)}$
  $\Rightarrow \tilde{\tilde{f}}^{(5)} = 3x_5 + x_6 + 5, \tilde{\tilde{f}}^{(6)} = 3x_5 + 2x_6 + 1$
- Set $\tilde{\tilde{f}}^{(5)} = y_3 = 0$ and $\tilde{\tilde{f}}^{(6)} = y_4 = 5$, solve for x_5 and x_6
  $\Rightarrow (x_5, x_6) = (0, 2)$

A pre image of $\mathbf{y} = (6, 2, 0, 5)$ is given by $\mathbf{x} = (0, 1, 3, 4, 0, 2)$.

Signature Generation

Given: message d

1. Use a hash function $\mathcal{H} : \{0,1\} \to \mathbb{F}^m$ to compute $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$
2. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m$.
3. Compute a pre-image $\mathbf{y} \in \mathbb{F}^n$ of $\mathbf{x}$ under the central map $\mathcal{F}$
4. Compute the signature $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

Signature Verification

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

1. Compute $\mathbf{w} = \mathcal{H}(d)$.
2. Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z})$.

Accept the signature $\mathbf{z} \Leftrightarrow \mathbf{w}' = \mathbf{w}$.

Security

Rainbow is an extension of UOV
$\Rightarrow$ All attacks against UOV can be used against Rainbow, too.

Additional structure of the central map allows several new attacks

- **MinRank Attack**: Look for linear combinations of the matrices G_i of low rank
- **HighRank Attack**: Look for the linear representation of the variables appearing the lowest number of times in the central polynomials.
- **Rainbow-Band-Separation Attack**: Variant of the UOV-Reconciliation Attack using the additional Rainbow structure [DY08]

$\Rightarrow$ Parameter Selection for Rainbow is a challenging task

Parameters

security level (bit)	parameters $\mathbb{F}, v_1, o_1, o_2$	public key size (kB)	private key size (kB)	hash size (bit)	signature (bit)
80	GF(16),17,20,20	33.4	22.3	160	228
	GF(256),19,12,13	25.3	19.3	200	352
100	GF(16),22,25,25	65.9	43.2	200	288
	GF(256), 27,16,16	57.2	44.3	256	472
128	GF(16),28,32,32	136.6	87.6	256	368
	GF(256),36,21,22	136.0	102.5	344	632
192	GF(16),45,48,48	475.9	301.8	384	564
	GF(256),58,33,34	523.5	385.5	536	1,000
256	GF(16),66,64,64	1,194.4	763.9	512	776
	GF(256),86,45,46	1,415.7	1,046.3	728	1,416

Rainbow - Summary

- no weaknesses found since 2005
- very efficient, much faster than RSA
- suitable for low cost devices
- shorter signatures and smaller key sizes than UOV

$\Rightarrow$ Good candidate for the upcoming standardization process of post-quantum signature schemes

References

Pa97 J. Patarin: The oil and vinegar signature scheme, presented at the Dagstuhl Workshop on Cryptography (September 97)

KS98 A. Kipnis, A. Shamir: Cryptanalysis of the Oil and Vinegar Signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257–266. Springer, 1988.

KP99 A. Kipnis, J. Patarin, L. Goubin: Unbalanced Oil and Vinegar Schemes. EUROCRYPT 1999. LNCS vol. 1592, pp. 206–222 Springer, 1999.

DS05 J. Ding, S. Schmidt: Rainbow, a new multivariate polynomial signature scheme. ACNS 2005. LNCS vol. 3531, pp. 164–175 Springer, 2005.

DY08 J. Ding, B.Y. Yang, C.H.O. Chen, M.S. Chen, C.M. Cheng: New Differential-Algebraic Attacks and Reparametrization of Rainbow. ACNS 2008, LNCS 5037, pp.242–257, Springer 2008.