TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

A Multivariate Signature Scheme with a Partially Cyclic Public Key

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

SCC 2010, Royal Holloway, University of London
25. June 2010

Contents

1. Motivation
2. The Oil and Vinegar Signature Scheme
3. Construction
4. Description of the scheme
5. Security
6. Parameters
7. Future Work

Motivation (1)

Multivariate Public Key Cryptography

- Secure against attacks with quantum computers
- Suitable for the use on low cost devices
- Fast and efficient
- But: large keys

Motivation (2)

Key size reduction

Reduction of the private key

Use sparse central polynomials (e.g. TTS)

Reduction of the public key

The Oil and Vinegar Signature Scheme

- Choose two integers o and v, set $n = o + v$.
- Set $V = \{1, \ldots, v\}$ and $O = \{v+1, \ldots, n\}$.
- Choose randomly o quadratic polynomials $q^{(1)}, \ldots, q^{(o)}$ of the form

$$q^{(k)}(x_1, \ldots, x_n) = \sum_{i,j \in V, i \le j} q_{ij}^{(k)} x_i x_j + \sum_{i \in V, j \in O} q_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} q_i^{(k)} x_i + q_0^{(k)}, \quad (k = 1, \ldots, o)$$

- Define the central map Q as $Q = (q^{(1)}, \ldots, q^{(o)})$
- Choose randomly an affine invertible map $T = (M_T, c_T)$.
- **public key**: $P = Q \circ T$
- **Private key**: Q, T

For security reasons it is necessary to choose $v \ge 2o$.

Oil and Vinegar (2)

Signature generation

- Compute $h = H(m) \in K^o$
- Compute one preimage y of h under Q
  - Choose the vinegar variables $x_1, \ldots, x_v$ at random
  - Solve the resulting linear system for the oil variables
- Compute $z = T^{-1}(y) \in K^n$

Signature verification

- Compute $h = H(m)$ and $w = P(z)$

If $w = h$ holds, the signature is accepted, otherwise rejected.

Construction (1)

$$P = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} x_i x_j + \sum_{i=1}^{n} p_i^{(1)} x_i + p_0^{(1)},$$

$$\ldots,$$

$$\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(o)} x_i x_j + \sum_{i=1}^{n} p_i^{(o)} x_i + p_0^{(o)}$$

↓ graded lexicographical ordering

$$M_P = \begin{pmatrix} p_{11}^{(1)} & p_{12}^{(1)} & \ldots & p_{nn}^{(1)} & p_1^{(1)} & \ldots & p_n^{(1)} & p_0^{(1)} \\ \vdots & & & & & & & \vdots \\ p_{11}^{(o)} & p_{12}^{(o)} & \ldots & p_{nn}^{(o)} & p_1^{(o)} & \ldots & p_n^{(o)} & p_0^{(o)} \end{pmatrix} = \begin{pmatrix} \pi_{11} & \ldots & \pi_{1d} \\ \vdots & & \vdots \\ \pi_{o1} & \ldots & \pi_{od} \end{pmatrix}$$

where $d = \frac{(n+1)\cdot(n+2)}{2}$.

We want $M_P = (B \mid C),$

where B is a partially circulant matrix.

Construction (2)

Due to the relation $P = Q \circ T$ we get the following equations between the quadratic coefficients of P and Q :

$$p_{ij}^{(k)} = \sum_{r=1}^{n} \sum_{s=r}^{n} \alpha_{ij}^{rs} \cdot q_{rs}^{(k)} = \sum_{r=1}^{v} \sum_{s=r}^{n} \alpha_{ij}^{rs} \cdot q_{rs}^{(k)} \qquad (1)$$

with

$$\alpha_{ij}^{rs} = \begin{cases} t_{ri} \cdot t_{si} & (i = j) \\ t_{ri} \cdot t_{sj} + t_{rj} \cdot t_{si} & \text{otherwise} \end{cases}$$

Assign the coefficients of T some elements of K.

→ We get linear relations between the $p_{ij}^{(k)}$ and the $q_{rs}^{(k)}$.

Construction (3)

For $i = 1, \ldots, o$ we define two $D = \frac{v \cdot (v+1)}{2} + o \cdot v$-vectors

$$v_P^{(i)} = (p_{kl}^{(i)} \mid 1 \le k \le v, k \le l \le n)$$

and

$$v_Q^{(i)} = (q_{kl}^{(i)} \mid 1 \le k \le v, k \le l \le n)$$

containing the first D coefficients of the i-th public and central polynomials.

Additionally, we define a $D \times D$ matrix A containing the coefficients of the equations (1).

$$A = \left(\alpha_{ij}^{rs} \middle| \begin{array}{l} 1 \le i \le v, i \le j \le n \text{ for the columns} \\ 1 \le r \le v, r \le s \le n \text{ for the rows} \end{array} \right) = \begin{pmatrix} \alpha_{11}^{11} & \alpha_{12}^{11} & \ldots & \alpha_{vn}^{11} \\ \alpha_{11}^{12} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \alpha_{11}^{vn} & \ldots & \ldots & \alpha_{vn}^{vn} \end{pmatrix}$$

Construction (4)

We obtain for $i = 1, \ldots, o$

$$v_P^{(i)} = v_Q^{(i)} \cdot A \quad (2)$$

We can use these relations to reduce the public key size of UOV by a large factor.

Of 1000 matrices A over GF(256) were invertible

(o,v)	(2,4)	(5,10)	(10,20)	(15,30)	(20,40)
# invertible	993	996	997	995	994

Assuming that A is invertible, we can prove the following theorem:

Construction (5)

Theorem: For every $s \leq \frac{v \cdot (v+1)}{2} + ov$, $\vec{b} = (b_1, \ldots, b_s) \in_R K^s$ and invertible affine map $T = (M_T, c_T) : K^n \to K^n$ there exist two quadratic maps $P, Q : K^n \to K^o$ such that

1. Q is a UOV map
2. We have $P = Q \circ T$ as a composition of mappings
3. The entries of the matrix M_P fulfill

$$\pi_{ij} = b_{(j-i \bmod s)+1} \quad (1 \leq i \leq o, 1 \leq j \leq s)$$

The Scheme (1)

- Key Generation

1. For $s \leq D$ choose a vector $\vec{b} = (b_1, \ldots, b_s) \in_R K^s$.
2. Choose an affine map $T = (M_T, c_T) : K^n \to K^n$ at random. If M_T is not invertible, choose again.
3. Compute for T the corresponding matrix A. If A is not invertible, go back to step 2.
4. For $i = 1, \ldots, o$ set

$$v_P^{(i)} = S^{i-1}(\vec{b}),$$

where $S(\vec{b})$ is the cyclic right shift of the vector $\vec{b}$.

The Scheme (2)

5. Solve for $i = 1, \ldots, o$ the linear systems given by equation (2) to get the vectors $v_Q^{(i)}$ and therewith the quadratic coefficients of the central polynomials.
6. Choose the coefficients of the linear terms of the central polynomials at random.
7. Compute the public key as $P = Q \circ T$.

The Scheme (3)

- The public key consists of the vector $\vec{b}$ and the last $\frac{(n+1)\cdot(n+2)}{2} - s$ columns of M_P .
- The private key consists of the maps Q and T .
- **public key size:**

$$s + o \cdot \left(\frac{(n+1)\cdot(n+2)}{2} - s \right) = o \cdot \frac{(n+1)\cdot(n+2)}{2} - s \cdot (o-1)$$ field elements

- **private key size:**

$$o \cdot \left(\frac{v\cdot(v+1)}{2} + o \cdot v + n + 1 \right) + n \cdot (n+1)$$ field elements

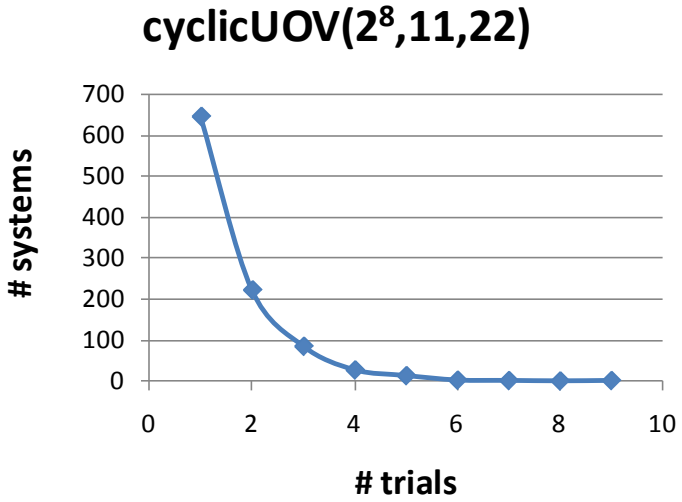
- The signature generation and verification works as in the standard UOV scheme.

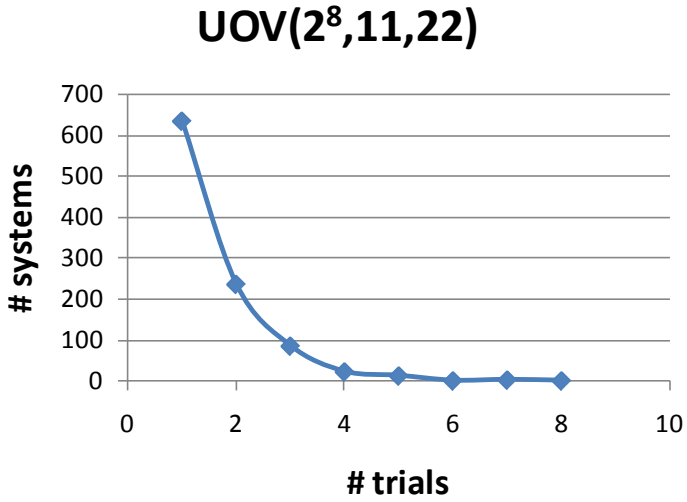
Security (1)

Direct attacks

When attacking the scheme directly, one has to solve a system of o quadratic equations in o+v variables. Therefore, before applying an algorithm like XL or F4, one has to guess at at least v variables to create a determined system.

Does the determined system always have a solution?





Security (2)

Direct attacks (2)

During this guessing process, a major part of the cyclic structure of the original public key gets lost.

We solved determined systems with MAGMA‘s F4 algorithm.

Scheme(2^8,o,v)	10,20	11,22	12,24	13,26	14,28
UOV	54 s	388 s	3141 s	24265 s	173425 s
cyclicUOV	53 s	387 s	3142 s	24258 s	173417 s

Security (3)

UOV Reconciliation

The goal of this attack is to find a basis change of variables which transforms the public key into UOV form

In the first step of the attack one has to solve a system of o quadratic equations in v variables. Again, we have to guess at some of the variables. By doing so, we get a system which looks very similar to the system we got in the direct attack.

Scheme(2^8,o,v)	10,20	11,22	12,24	13,26	14,28
UOV	55 s	386 s	3137 s	24258 s	173419 s
cyclicUOV	54 s	384 s	3136 s	24261 s	173415 s

Security (4)

Rank attacks

Let H_i be the symmetric matrix representing the homogenous quadratic part of the i-th public polynomial.

In the MinRank attack one tries to find a linear combination $H = \sum_{i=1}^{o} \alpha_i H_i$ with $\mathrm{rank}(H) = r < n$.

cyclicUOV	(2^8,o,v,n)	(8,16,24)	(10,20,30)	(12,24,36)	(16,32,48)	(20,40,60)
Rank(H)	n	9964	9957	9959	9964	9958
	n-1	0	0	0	0	0
	n-2	36	43	41	36	42
UOV						
Rank(H)	n	9965	9963	9962	9966	9965
	n-1	35	37	38	34	35
	n-2	0	0	0	0	0

Parameters

Considering our security analysis, we propose the following parameters for our scheme: $q = 256,\ o = 25,\ v = 50$

	Public key size (kB)	Private key size (kB)	Hashsize (bit)	Signature size (bit)
UOV(2^8,24,48)	63.3	61.1	192	576
Rainbow(2^8,17,13,13)	25.7	19.1	208	344
cyclicUOV (2^8,25,50)	12.3	69.1	200	600

→ Reduction of the public key size by **83%**

→ Reduction of the number of multiplications needed for signature verification by **42%**

Future Work (1)

- Extend the security analysis
- Polynomial decomposition
- …

Future Work (2)

We had $P = (B \mid C)$ with a partially circulant matrix B

Try to create UOV-schemes with other forms of the matrix B, for example

- LFSR with a small seed
- PRNG (e.g. AES) with small seed
- Fully random matrix

Future Work (3)

- Extension of the idea to the Rainbow and the enSTS Signature Schemes
- more complex, since $P = S \circ Q \circ T$ is a concatenation of 3 maps
- smaller private key
- smaller signature size
- higher efficiency

Thank you for your attention

Questions ?