Rainbow

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

The 2nd NIST Standardization Conference for Post-Quantum Cryptosystems

Santa Barbara, USA
22.09.2019

Multivariate Cryptography

MPKC: Multivariate Public Key Cryptosystem
Public Key: System of nonlinear multivariate polynomials

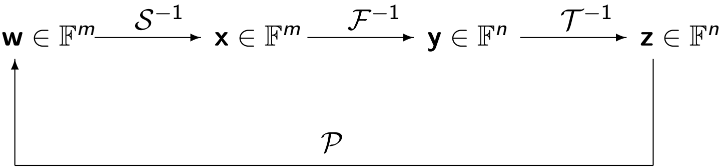
$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}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

Construction

- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible affine (or 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 and $\mathcal{S}, \mathcal{T}$ are used to protect $\mathcal{F}$
- **Private key**: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$ allows to invert the public key

Signature Schemes ($m \leq n$)

Signature Generation



Signature Verification

Signature Generation: Given a document $d \in \{0,1\}^\star$, use a hash function $\mathcal{H}$ to compute $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$, compute recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x}) \in \mathbb{F}^n$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. The signature of the message d is $\mathbf{z} \in \mathbb{F}^n$.

Signature Verification: Given signature $\mathbf{z} \in \mathbb{F}^n$, hash value $\mathbf{w} \in \mathbb{F}^m$, compute $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$. If $\mathbf{w}' = \mathbf{w}$ holds, the signature is accepted, otherwise rejected.

Unbalanced Oil-vinegar (UOV) schemes

The design of Rainbow is based on the UOV by Patarin etc invented in 1999.

- $F = (f_1(x_1, .., x_o, x'_1, ..., x'_v), \cdots, f_o(x_1, .., x_o, x'_1, ..., x'_v))$.

Unbalanced Oil-vinegar (UOV) schemes

The design of Rainbow is based on the UOV by Patarin etc invented in 1999.

- $F = (f_1(x_1, .., x_o, x'_1, ..., x'_v), \cdots, f_o(x_1, .., x_o, x'_1, ..., x'_v))$.
- $$f_l(x_1, ., x_o, x'_1, ., x'_v) = \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l.$$

  Oil variables: $x_1, ..., x_o$.

  Vinegar variables: $x'_1, ..., x'_v$.

How to invert OV map?

$$f_l(x_1, .., x_o, \underbrace{x'_1, .., x'_v}_{\textbf{fix the values}}) =$$

$$\sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l.$$

How to invert OV map?

$$f_l(x_1, ., x_o, x'_1, ., x'_v) = \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l.$$

This implies high efficiency in signing since the main cost is to solve a small linear system.

How to invert OV map?

$$f_l(x_1, .., x_o, x'_1, .., x'_v) =$$
$$\sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l.$$

- F: linear in Oil variables: $x_1, .., x_o$.

$\Longrightarrow$ OV map: easy to invert.

This implies high efficiency in signing since the main cost is to solve a small linear system.

The Rainbow Signature Scheme

- finite field $\mathbb{F}$ with q elements, integers $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$
- set $V_i = \{1, \ldots, v_i\}$ and $O_i = \{v_i + 1, \ldots, v_{i+1}\}$ $(i = 1, \ldots, u)$ $\Rightarrow |V_i| = v_i$, $|O_i| = v_{i+1} - v_i := o_i$
- central map $\mathcal{F}$ consists of $m := n - v_1$ polynomials $f^{(v_1+1)}, \ldots, f^{(n)}$ of the form

$$f^{(k)}(x_1, \ldots, x_n) = \sum_{i,j \in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \delta^{(k)},$$

  where ℓ is the only integer such that $k \in O_\ell$.
- two invertible affine maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- **Public Key**: $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$
- **Private Key**: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

Signature Generation

Given a document $d \in \{0,1\}^\star$ to be signed, perform the following steps

1. Use a hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}^m$ to compute $\mathbf{w} = \mathcal{H}(d)$.
2. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m$.
3. The Vinegar variables are substituted by random values into the polynomials $f^{(v_1+1)}, \ldots, f^{(n)}$.
4. for l:=1 to u do Solve the linear system provided by $f^{(v_i+1)}, \ldots f^{(v_{i+1})}$ to get the values of $y_{v_i+1}, \ldots, y_{v_{i+1}}$ and substitute them into the polynomials $f^{(v_{i+1}+1)}, \ldots, f^{(n)}$.
5. Set $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}^n$.
6. Compute the signature $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

Signature Verification

Given a document $d \in \{0,1\}^\star$ and a signature $\mathbf{z} \in \mathbb{F}^n$, compute

- $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$ and
- $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$.

If $\mathbf{w}' = \mathbf{w}$ holds, the signature is accepted; otherwise it is rejected.

Security Analysis of Rainbow

- Generic MQ problem – NP-hard
- Direct attacks do not work (as hard as generic problem)
- Simple structure – simple, easy to implement and well understood attacks
  Main attacks: Algebraic attack, OV attack, Rank attacks and RainbowBand Separation attacks
- Practical attacks match closely to theoretical estimates.
- No substantial but incremental update of Rainbow cryptanalysis since 2008

Rainbow - Highlights

- Solid history: UOV 1999 and Rainbow 2004
- existentially unforgeable under chosen message attacks
- very efficient signature generation and verification (signature generation at least 20 times faster than that of all competitors)
- easy to implement and naturally resist passive side channel attacks
- very short signatures (48 bytes for Level I, II) but relatively large PK size
- accepted as a 2nd round candidate for the NIST standardization process of post-quantum cryptosystems

Changes to the first round submission

- Reduction of the number of parameter sets
  We now have three parameter sets
  - (GF(16),32,32,32) for NIST security category I and II,
  - (GF(256),68,36,36) for NIST security category III and IV and
  - (GF(256),92,48,48) for the NIST security category V and VI.
- Inclusion of two other modes
  - cyclic Rainbow
    $\Rightarrow$ Reduction of the public key size by up to 70 %
  - compressed Rainbow
    $\Rightarrow$ Reduction of the public key size by up to 70 %
    $\Rightarrow$ Private key is stored as a 64B seed
    $\Rightarrow$ Slower signature generation and verification process

Changes to the first round submission (2)

- Speed up of the Key Generation algorithm
  - use of homogeneous keys
  - use of specially designed maps $\mathcal{S}$ and $\mathcal{T}$ (equivalent keys)

$$S = \begin{pmatrix} 1_{o_1 \times o_1} & S'_{o_1 \times o_2} \\ 0_{o_2 \times o_1} & 1_{o_2 \times o_2} \end{pmatrix}, \quad T = \begin{pmatrix} 1_{v_1 \times v_1} & T^{(1)}_{v_1 \times o_1} & T^{(2)}_{v_1 \times o_2} \\ 0_{o_1 \times v_1} & 1_{o_1 \times o_1} & T^{(3)}_{o_1 \times o_2} \\ 0_{o_2 \times v_1} & 0_{o_2 \times o_1} & 1_{o_2 \times o_2} \end{pmatrix}$$

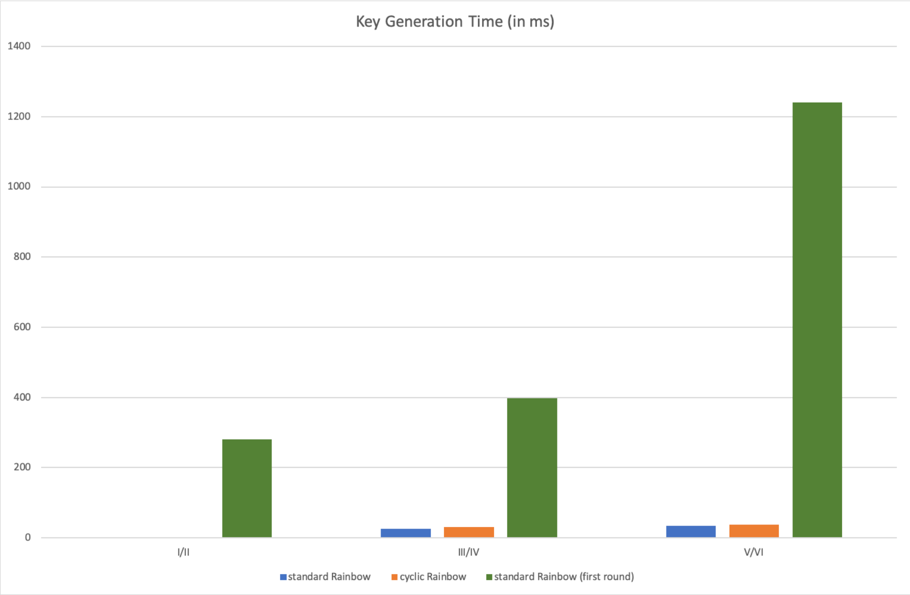
$\Rightarrow$ Key Generation can be performed using matrix vector products

$\Rightarrow$ Significant speed up of the key generation process

Key Sizes

NIST security category	standard Rainbow		cyclic Rainbow		compressed Rainbow	
	$\|pk\|KB$	$\|sk\|KB$	$\|pk\|KB$	$\|sk\|KB$	$\|pk\|KB$	$\|sk\|$
I/II	149.0	93.0	58.1	93.0	58.1	64B
III/IV	710.6	511.4	206.7	511.4	206.7	64B
V/VI	1,705.5	1,227.1	491.9	1,227.1	491.9	64B

Signature sizes: 48B, 140B, 184B


Key Generation Time (in ms)
1400
1200
1000
800
600
400
200
0
I/II
III/IV
V/VI
standard Rainbow
cyclic Rainbow
standard Rainbow (first round)

The End

Thank you for your attention

Questions?