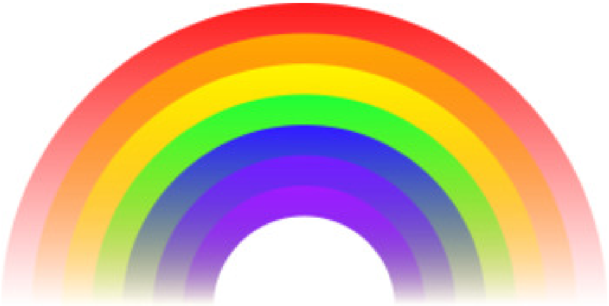
Rainbow

proposed by:
Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt and Bo-Yin Yang

First NIST PostQuantum Standardization Workshop

Fort Lauderdale, Florida
04/12/2018

Rainbow



Type: Signature Scheme

Family: Multivariate Cryptography

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

The Oil and Vinegar Signature Scheme - Key Generation

- Parameters: finite field $\mathbb{F}$, integers o, v, set $n = o + v$
- central map $\mathcal{F} : \mathbb{F}^n \rightarrow \mathbb{F}^o$ consists of o Oil-Vinegar polynomials $f^{(1)}, \ldots, f^{(o)}$.
- Compose $\mathbb{F}$ with a randomly chosen invertible affine map $\mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^o$
- *private key*: $\mathcal{F}, \mathcal{T}$

Signature Generation

- $\mathcal{P}^{-1} = \mathcal{T}^{-1} \circ \mathcal{F}^{-1}$.
- Inversion of $\mathcal{F}$
  - random assign vinegar values

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

  - solve the resulting linear system with o equations and o variables to derive the oil values
  - If the system does not have a solution, repeat.

(U)OV

- balanced case ($o = v$) broken by Kipnis, Shamir
- Unbalanced Oil and Vinegar (UOV) with $v \gg o$ [KP99]
- Signature is more than twice the hash
  $\Rightarrow$ Rainbow

The Rainbow Signature Scheme (2005) - 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*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

Variable Structure

$$\underbrace{x_1, \ldots, x_{v_1}}_{\text{vinegar variables}}, \underbrace{x_{v_1+1}, \ldots, x_{v_1+o_1}}_{\text{oil variables}}$$

$$\underbrace{x_1, \ldots, x_{v_1}, x_{v_1+1}, \ldots, x_{v_1+o_1}}_{\text{vinegar variables}}, \underbrace{x_{v_1+o_1+1}, \ldots, x_{v_1+o_1+o_2}}_{\text{oil variables}}$$

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 $\mathcal{F}$
   - Choose random values for the vinegar variables $y_1, \ldots, y_v$ and substitute into the polynomials $f^{(v+1)}, \ldots, f^{(n)}$
   - For $i = 1$ to u
     - Solve the linear system $f^{(i)} = x_i$ $(i = v_i + 1, \ldots, v_{i+1})$ by Gaussian Elimination
     - Substitute the values of $y_{v_i+1}, \ldots, y_{v_{i+1}}$ into the polynomials $f^{(v_{i+1}+1)}, \ldots, f^{(n)}$.
4. Compute the signature $\sigma \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

Signature Generation

- assign random values to the vinegar variables of the first layer

$$\underbrace{x_1, \ldots, x_{v_1}}_{\text{vinegar variables}}, \underbrace{x_{v_1+1}, \ldots, x_{v_1+o_1}}_{\text{oil variables}}$$

- solve the resulting linear system for the oil variables of the first layer
- $x_1, \ldots, x_{v_1+o_1}$ are known and substitute them into the second layer

$$\underbrace{x_1, \ldots, x_{v_1}, x_{v_1+1}, \ldots, x_{v_1+o_1}}_{\text{vinegar variables}}, \underbrace{x_{v_1+o_1+1}, \ldots, x_{v_1+o_1+o_2}}_{\text{oil variables}}$$

- Solve the resulting linear system for $x_{v_1+o_1+1}, \ldots, x_{v_1+o_1+o_2}$.
- If one of the linear systems has no solution, choose other values for the vinegar variables of the first layer.

Signature Verification

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

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

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

Design Decisions

- underlying field: GF(16), GF(31) and GF(256)
  $\Rightarrow$ tradeoff between key size, signature size, performance and security
- 2 Rainbow layers
  - better performance than 1 layer (UOV)
  - more than two layers do not provide significantly better performance, but make it more difficult to defend the scheme against attacks
- choose the size of the layers to be equal (with one exception)

EUF-CMA Security

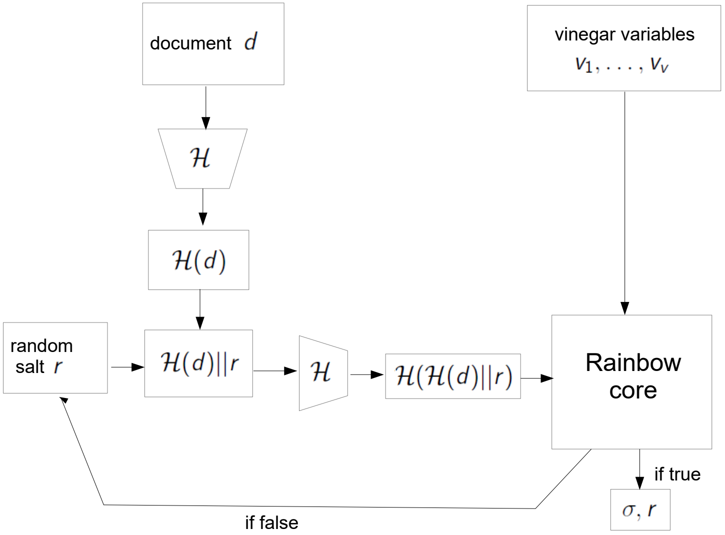
Idea: Use of a 128 bit nonce

Signature Generation:

- For a document d to be signed, compute $\mathcal{H}(d)$ first (leads to better performance).
- Choose random values for the vinegar variables $v_1, \ldots, v_v$.
- Choose a 128-bit random salt r; if Rainbow does not output a signature for $\mathcal{H}(\mathcal{H}(d)||r)$, choose another salt and try again.
- The final signature is (σ, r), where σ is the standard Rainbow signature.

Signature Verification: Check, if $\sigma \in \mathbb{F}^n$ is a valid signature for $\mathcal{H}(\mathcal{H}(d)||r)$.

EUF-CMA-Secure Signature Generation Process



Implementation

Representation of field elements

- Elements of GF(31): integers in $\{0, \ldots, 30\}$
- Elements of GF(16) and GF(31):
  - Elements of GF(2): bits
  - Elements of GF(4): linear polynomials over GF(2)
  - Elements of GF(16): linear polynomials over GF(4)
  - Elements of GF(256): linear polynomials over GF(16)

Implementation (2)

- multiplication of finite field elements
  - GF(31): common multiplication / reduction
  - GF(16) and GF(256)
    - reference implementation: logic bit operations / polynomial multiplication
    - optimized implementation: query log/exp-tables with AVX2 instructions (for time constancy)
- constant time Gaussian elimination to prevent timing attacks
- constant time MQ-evaluation to compute the $v \times v$ terms of the central map
- optimized implementation: AVX2 vector instructions

$\Rightarrow$ Much more details in the proposal

Security

- no security proof / reduction to a hard problem
- security is measured by the complexity of known attacks
  - colission attacks against the hash function
  - direct attacks
  - MinRank attack
  - HighRank attack
  - RBS attack
  - UOV attack

$\Rightarrow$ Detailed analysis of all attacks (including quantum improvements) in the proposal

Parameters over GF(16)

parameter set	parameters v_1, o_1, o_2	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit)	NIST security category
Ia	32,32,32	148.5	97.9	256	512	I
IVa	56,48,48	552.2	367.3	384	736	IV
VIa	76,64,64	1,319.7	871.2	512	944	VI

- Signature size includes 128 bit salt

Parameters over GF(16) - Performance

		key generation	signature generation	signature verification
Ia	cycles	1,302M/1,081M	601k/75.5k	350k/25.5k
	time (ms)	394/328	0.182/0.023	0.106/0.008
	memory	3.3MB/3.0MB	3.0MB/3.0MB	2.6MB/2.8MB
IVa	cycles	11,176M/8,673M	1,823k/899k	1,241k/181k
	time (ms)	3,387/2,628	0.552/0.272	0.376/0.055
	memory	4.3MB/4.1MB	3.0MB/3,3MB	2.8MB/3.2MB
VIa	cycles	45,064M / 6,689M	3,916k / 575k	2,897k/367k
	time (ms)	13,655/2,027	1.187/0.174	0.878/0.111
	memory	6.1MB/6.1MB	3.8MB/3.9MB	3.8MB/3.8MB

Performance on
NIST Reference Platform (Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, no special processor instructions) /

Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, AVX2 vector instructions

$\Rightarrow$ By using AVX2 instructions, we can speed up signature generation and verification by approximately 85 %. With regard to key generation, the speed up is only important for high levels of security.

Parameters over GF(31)

parameters v_1, o_1, o_2	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit)	NIST security category
36,28,28	148.3	103.7	268	624	I,II
64,32,48	512.1	371.4	384	896	III, IV
84,56,56	1,321.0	922.4	536	1,176	IV

- Signatures include 128 bit salt
- For the second parameter set, the layers were chosen to be unbalanced in order to enhance the security of the scheme against quantum HighRank attacks

Parameters over GF(31) - Performance

		key generation	signature generation	signature verification
Ib	cycles	4,578M/141M	2,044/426k	1,944k/496k
	time (ms)	1,378/42.83	0.619/0.129	0.589/0.15
	memory	3.6MB/3.6MB	3.3MB/3.2MB	2.9MB/2.9MB
IIIb	cycles	26,172M/813M	5,471k/1,469k	4,908k/1,791k
	time (ms)	7,931/246	1.658/0.445	1.487/0.543
	memory	5.7MB/5.9MB	3.6MB/4.1MB	3.9MB/4.1MB
VIb	cycles	164,689M / 3,518M	16,755k /3,655k	11,224k/4,690k
	time (ms)	49,906/1,066	5.077/1.108	3.401/1.421
	memory	10.3MB/10.0MB	4.4MB/5.3MB	6.0MB/6.0MB

Performance on
NIST Reference Platform (Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, no special processor instructions) /

Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, AVX2 vector instructions

$\Rightarrow$ With regard to key generation, the speedup by AVX2 instructions is dramatic (97-98%). For signature generation and verification, we get a speed up of approximately 75 %.

Parameters over GF(256)

parameters v_1, o_1, o_2	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit)	NIST security category
40,24,24	187.7	140.0	384	832	I , II
68,36,36	703.9	525.2	576	1,248	III, IV
92,48,48	1,683.3	1,244.4	768	1,632	V, VI

- Signatures include 128 bit salt

Parameters over GF(256) - Performance

		key generation	signature generation	signature verification
Ic	cycles	4,089M/183M	1,521/111k	939k/57.5k
	time (ms)	1,239/55.4	0.461/0.034	0.0.285/0.017
	memory	3.3MB/3.3MB	3.0MB/3.0MB	2.8MB/2.8MB
IIIc	cycles	31,612M/1,430M	4,047k/326k	2,974k/275k
	time (ms)	9,579/433	1.226/0.099	0.901/0.083
	memory	4.6MB/4.6MB	2.9MB/3.5MB	3.1MB/3.3MB
Vc	cycles	116,046M / 4,633M	8,688k /616k	6,174k/472k
	time (ms)	35,165/1,404	2.633/0.187	1.871/0.143
	memory	7.0MB/7.0MB	3.7MB/4.2MB	3.9MB/4.5MB

Performance on
NIST Reference Platform (Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, no special processor instructions) /

Intel Xeon E3-1225 v5 (Skylake), 3.3 GHz, AVX2 vector instructions

$\Rightarrow$ Independently of parameter choice and kind of algorithm, we get, by the use of AVX2 instructions, a speed up of 90-95 %.

Parameters - Overview

security category	GF(16)	GF(31)	GF(256)
I	Ia	Ib	Ic
II	-	Ib	Ic
III	-	IIIb	IIIc
IV	IVa	IIIb	IIIc
V	-	-	Vc
VI	VIa	VIb	Vc

Optimal Parameters

security	size		running time	
category	key	signature	key generation	signature generation
I	Ia	Ia	Ib	Ia
II	Ib	Ib	Ib	Ic
III	IIIb	IIIb	IIIb	IIIc
IV	IIIb	IVa	IIIb	IIIc
V	Vc	Vc	Vc	Vc
VI	VIa	VIa	Vb	Vc

$\Rightarrow$ Each of our parameter sets is optimal with regard to at least one category

Advantages and Limitations

Advantages:

- Simple and easy to implement
- Practical security well understood
- very fast
- modest computational resources
- Implementation immune against timing attacks

Limitations:

- Large key sizes