

Handling Vinegar Variables to Shorten Rainbow Key Pairs

Gustavo Zambonin Matheus S. P. Bittencourt
Ricardo Custódio



Universidade Federal de Santa Catarina
gustavo.zambonin@posgrad.ufsc.br

July 11

AFRICACRYPT 2019

Outline

- ▶ Context
 - ▶ Multivariate cryptography
- ▶ Rainbow signature scheme
 - ▶ Description
- ▶ Related works
- ▶ Our contributions
 - ▶ Approach
 - ▶ Results
- ▶ Open problems

Context

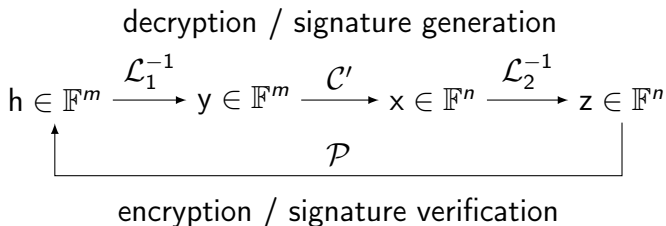
Introduction

- ▶ Security of digital signature schemes is based on problems from number theory
 - ▶ Solved efficiently by Shor's algorithm on quantum computers
- ▶ Post-quantum cryptography aims to create cryptosystems based on problems immune to quantum speed-ups
 - ▶ Several active branches, standardisation calls
- ▶ We focus on the Rainbow digital signature scheme
 - ▶ Based on systems of multivariate equations over finite fields

Context

Multivariate cryptography

- ▶ Based on the difficulty of polynomial system solving and extended isomorphism of polynomials problems
- ▶ Bipolar construction, with central trapdoor



- ▶ When $m \leq n$, resulting signature schemes have comparatively small signatures and large keys

Rainbow signature scheme

Overview

- ▶ Formalised in [DS05], currently on Round 2 of the NIST standardisation process
- ▶ Easy description, good balance between signature and key sizes
 - ▶ Generalized version of Unbalanced Oil and Vinegar [KPG99]
- ▶ Systems of equations compose keys, which are orders of magnitude greater than conventional ones
 - ▶ RSA at 3072 bits, elliptic curves at 256 bits, Rainbow at ≈ 1 Mb

Rainbow signature scheme

Preliminaries

- ▶ Parameters are the order q of a finite field, $u, n \in \mathbb{N}$ and $0 < v_1 < \dots < v_u < v_{u+1} = n$
- ▶ For $1 \leq \ell \leq u$, set vinegar variables $V_\ell = \{1, \dots, v_\ell\}$ and oil variables $O_\ell = \{v_\ell + 1, \dots, v_{\ell+1}\}$, with $o_\ell = |O_\ell|$
- ▶ Define vector spaces spanned by quadratic Oil-Vinegar polynomials

$$P_\ell = \sum_{i,j \in V_\ell} \alpha_{ij} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i x_i + \delta,$$
$$\alpha_{ij}, \beta_{ij}, \gamma_i, \delta \in \mathbb{F}_q$$

Rainbow signature scheme

Key generation

- ▶ Let $m = n - v_1$ be the number of equations in the keys
- ▶ Randomly pick two invertible affine transformations $\mathcal{L}_1 : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m$ and $\mathcal{L}_2 : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$
- ▶ Central map is a function $\mathcal{C} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$
 - ▶ Exactly o_ℓ polynomials and their respective coefficients are randomly chosen from each P_ℓ
- ▶ Private key is the 3-uple $(\mathcal{L}_1, \mathcal{C}, \mathcal{L}_2)$, public key is the composition $\mathcal{P} = \mathcal{L}_1 \circ \mathcal{C} \circ \mathcal{L}_2$

Rainbow signature scheme

Preimage of the central map

- ▶ Vinegar variables of a layer are exactly the oil and vinegar variables from the previous layer
- ▶ This enables the inversion of each Oil-Vinegar layer recursively
- ▶ With $u = 2$, the initial configuration of $\mathcal{C}$ is

	$V_1 \times V_1$	$V_1 \times O_1$	$O_1 \times O_1$	$V_1 \times O_2$	$O_1 \times O_2$	$O_2 \times O_2$	V_1	O_1	O_2	δ
$\ell = 1$			0	0	0	0			0	★
$\ell = 2$						0				★

Rainbow signature scheme

Preimage of the central map

- Randomly choose variables in V_1 and substitute them

	$V_1 \times V_1$	$V_1 \times O_1$	$O_1 \times O_1$	$V_1 \times O_2$	$O_1 \times O_2$	$O_2 \times O_2$	V_1	O_1	O_2	δ
$\ell = 1$	*		0	0	0	0	*		0	*
$\ell = 2$	*					0	*		*	*

- Solve o_1 linear equations in the first layer to obtain V_2 (if possible), and then solve the remaining o_2 equations

	$V_1 \times V_1$	$V_1 \times O_1$	$O_1 \times O_1$	$V_1 \times O_2$	$O_1 \times O_2$	$O_2 \times O_2$	V_1	O_1	O_2	δ
$\ell = 2$	*	*	*			0	*	*		*

Rainbow signature scheme

Signature generation

- ▶ Consider a cryptographic hash function $\mathcal{H}$ and a message M , and compute the digest $h = \mathcal{H}(M)$
- ▶ With possession of the private key, obtain the value $y = \mathcal{L}_1^{-1}(h)$
- ▶ Generate the preimage of y under the central map, $x = \mathcal{C}'(y)$, as per the previous operations
- ▶ Compute the final signature $z = \mathcal{L}_2^{-1}(x)$

Rainbow signature scheme

Signature verification

- ▶ Obtain h from the message M
- ▶ With possession of the public key, compute $h' = \mathcal{P}(z)$
- ▶ The signature is valid if $h = h'$, and invalid otherwise

Related works

Reduction of key sizes in Rainbow-like schemes

Work	Parameters	$\Delta \mathcal{K}_{Pr} $	$\Delta \mathcal{K}_{Pu} $
CyclicRainbow [PBB10]	$(\mathbb{F}_{256}, 19, 14, 14)$	—	−59.78%
NC-Rainbow [YST12]	$(\mathbb{F}_{256}, 36, 24, 24)$	−79.63%	—
MB-Rainbow [YDTS13]	$(\mathbb{F}_{256}, 31, 19, 24)$	−37.19%	—
RainbowLRS2 [Pet13]	$(\mathbb{F}_{256}, 36, 21, 22)$	—	−67.31%
NT-Rainbow [YTS14b]	$(\mathbb{F}_{256}, 31, 21, 22)$	−41.29%	—
MNT-Rainbow [YTS14a]	$(\mathbb{F}_{256}, 31, 19, 24)$	−76.38%	—
Lite-Rainbow-0 [SPB15]	$(\mathbb{F}_{256}, 36, 12, 31)$	−99.99%	—
Lite-Rainbow-1 [SPB15]	$(\mathbb{F}_{256}, 36, 12, 31)$	—	−70.92%
Circulant Rainbow [PT17]	$(\mathbb{F}_{256}, 26, 23, 23)$	−45.22%	—

Our proposal

Approach

- ▶ To the best of our knowledge, works have reduced either private or public keys, but not both
 - ▶ Current methods to reduce keys are not usually compatible between themselves
- ▶ Recall that vinegar variables are chosen randomly every time a preimage of $\mathcal{C}$ is computed
- ▶ We propose to store $\mathcal{C}$ such that variables in V_1 are already chosen and substituted
 - ▶ General framework for Rainbow-like schemes

Our proposal

Solvability of $\mathcal{C}$

- ▶ It may occur that the initial choice of V_1 leads to unsolvable systems of equations in the preimage step
 - ▶ Low probability for common values of q
- ▶ Maintain the ability for the scheme to correctly sign any message
- ▶ To obtain the original $\mathcal{C}$, we use a seed or the linear relations from [PBB10]
- ▶ The EUF-CMA variant described in [DCP⁺17] makes use of a salt that can be modified instead of V_1

Our proposal

Effect of the construction

- ▶ Preimages with fixed elements are shuffled by $\mathcal{L}_2$, preserving the dissimilarity of signatures
 - ▶ Statistical argument through means, standard deviations, CDF and Q-Q plot
- ▶ Structure of the scheme is unchanged, classical parameters are reused
 - ▶ To the best of our knowledge, current algebraic cryptanalysis is ineffective

Our proposal

Private key reduction

NIST Cat.	n	m	$ \mathcal{K}_{Pr} $	$ \mathcal{K}_{Pr}^\eta $	Difference
I-a	96	64	100208	33152	-66.92%
I-b	92	56	114308	31676	-72.29%
I-c	88	48	143384	33024	-76.97%
III-b	144	80	409463	87628	-78.60%
III-c	140	72	537780	99656	-81.47%
IV-a	152	96	376140	103336	-72.53%
V-c	188	96	1274316	218984	-82.82%
VI-a	204	128	892078	233044	-73.88%
VI-b	196	112	1016868	217244	-78.64%

Our proposal

Whole key pair reduction for $q = 256$

Security	Variant	$ \mathcal{K}_{Pr} $	$ \mathcal{K}_{Pr}^\eta $	$ \mathcal{K}_{Pu} $	Difference
80	Classic			25740	-28.76%
	Cyclic	19546	6524	10618	-62.15%
	LRS2			9789	-63.98%
100	Classic			60390	-31.60%
	Cyclic	46131	12474	22246	-67.41%
	LRS2			20662	-68.89%
128	Classic			139320	-32.78%
	Cyclic	105006	24924	48411	-69.98%
	LRS2			45547	-71.16%

Open problems

- ▶ Measure key sizes on schemes which already optimise the private key
- ▶ Propose parameter sets to specifically reduce private keys, e.g. maximise v_1 according to known boundaries
- ▶ Measure new relative cost of key generation and signature generation steps
- ▶ Observe whether unsuccessful choices of V_1 leak private information, leading to side-channel attacks

References I



J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, and B.-Y. Yang.
Rainbow - Algorithm Specification and Documentation.
Round 1 Submission, NIST Post-Quantum Cryptography Standardisation
Process, December 2017.



J. Ding and D. Schmidt.
Rainbow, a New Multivariable Polynomial Signature Scheme.
In J. Ioannidis, A. Keromytis, and M. Yung, editors, *Applied Cryptography and
Network Security*, volume 3531 of *Lecture Notes in Computer Science*, pages
164–175, June 2005.



A. Kipnis, J. Patarin, and L. Goubin.
Unbalanced Oil and Vinegar Signature Schemes.
In J. Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of
Lecture Notes in Computer Science, pages 206–222, April 1999.



A. Petzoldt, S. Bulygin, and J. Buchmann.
CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public
Key.
In G. Gong and K. C. Gupta, editors, *Progress in Cryptology – INDOCRYPT
2010*, volume 6498 of *Lecture Notes in Computer Science*, pages 33–48,
December 2010.

References II



A. Petzoldt.

Selecting and Reducing Key Sizes for Multivariate Cryptography.

PhD thesis, Technische Universität Darmstadt, July 2013.



Z. Peng and S. Tang.

Circulant Rainbow: A New Rainbow Variant With Shorter Private Key and Faster Signature Generation.

IEEE Access, 5:11877–11886, June 2017.



K.-A. Shim, C.-M. Park, and Y.-J. Baek.

Lite-Rainbow: Lightweight Signature Schemes Based on Multivariate Quadratic Equations and Their Secure Implementations.

In A. Biryukov and V. Goyal, editors, *Progress in Cryptology – INDOCRYPT 2015*, volume 9462 of *Lecture Notes in Computer Science*, pages 45–63, December 2015.



T. Yasuda, J. Ding, T. Takagi, and K. Sakurai.

A Variant of Rainbow with Shorter Secret Key and Faster Signature Generation.

In K. Chen, Q. Xie, W. Qiu, S. Xu, and Y. Zhao, editors, *ACM Workshop on Asia Public-Key Cryptography*, pages 57–62, May 2013.

References III



T. Yasuda, K. Sakurai, and T Takagi.

Reducing the Key Size of Rainbow Using Non-commutative Rings.

In O. Dunkelman, editor, *Topics in Cryptology – CT-RSA 2012*, volume 7178 of *Lecture Notes in Computer Science*, pages 68–83, February 2012.



T. Yasuda, T. Takagi, and K. Sakurai.

Efficient variant of Rainbow using sparse secret keys.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 5(3):3–13, September 2014.



T. Yasuda, T. Takagi, and K. Sakurai.

Efficient Variant of Rainbow without Triangular Matrix Representation.

In M. S. Mahendra, E. J. Neuhold, M. A. Tjoa, and I. You, editors, *Information and Communication Technology*, volume 8407 of *Lecture Notes in Computer Science*, pages 532–541, April 2014.