Reduction of Key Sizes on Rainbow-like Multivariate Signature Schemes

Gustavo Zambonin

Qualification Exam
Graduate Program in Computer Science

gustavo.zambonin@posgrad.ufsc.br

Outline

- Context
  - Motivation
  - Multivariate cryptography
- Research object
  - Related works
  - Hypothesis
  - Rainbow signature scheme
- Our proposal
  - Open problems
  - Preliminary results
- Chronology

Context

- Guarantee authenticity of messages sent digitally
- Security of digital signature schemes is based on problems from number theory
  - Integer factorization, discrete logarithm
- There exist quantum algorithms [Sho97] that solve such problems efficiently
- Post-quantum cryptography aims to create cryptosystems based on problems immune to quantum speed-ups

Motivation

- Foreshadowing of quantum computers
- Several active branches of post-quantum cryptography based on distinct mathematical structures
- Standardization calls by institutions such as NIST, IRTF and ETSI
- We focus on cryptosystems that are built upon the difficulty of solving systems of equations

Multivariate cryptography

- Cryptography based on systems of multivariate equations over finite fields
- Bipolar construction:

decryption / signature generation

$$\begin{tikzcd}[column sep=large] \mathbf{h} \in \mathbb{F}^m \arrow[r, "\mathcal{L}_1^{-1}"] & \mathbf{x} \in \mathbb{F}^m \arrow[r, "\mathcal{C}^{-1}"] & \mathbf{y} \in \mathbb{F}^n \arrow[r, "\mathcal{L}_2^{-1}"] & \mathbf{z} \in \mathbb{F}^n \arrow[lll, bend left, "\mathcal{P}"] \end{tikzcd}$$

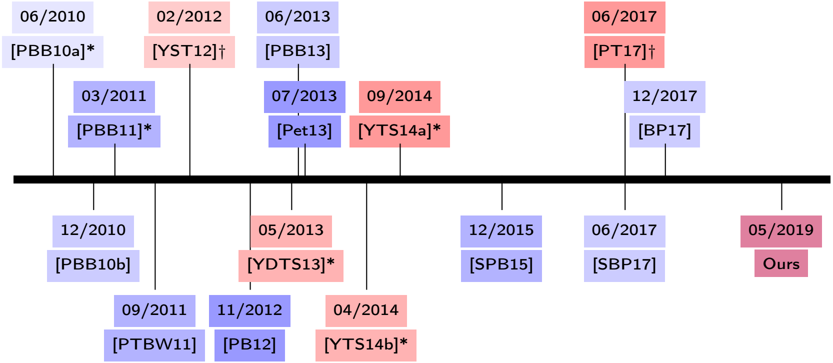
encryption / signature verification

- Focus on signatures ($m \leq n$): fast operations, small signatures and large keys, compared to current schemes

Research object

- Focus on the Rainbow signature scheme [DS05], currently on Round 2 of the NIST standardization process
- Easy description, good balance between signature and key sizes
- Keys are one to two orders of magnitude greater than conventional ones
- Generalized version of Unbalanced Oil and Vinegar [KPG99]

Related works



Works in blue optimise public keys, while red ones reduce private keys. Asterisks denote reparametrized works and crosses denote broken schemes.

Hypothesis

- To the best of our knowledge, works have reduced either private or public keys, but not both
- Introduction of structures in the keys may lower security
- **Can both reductions be achieved simultaneously**?

Rainbow signature scheme

Preliminaries

- Parameters are a finite field $\mathbb{F}_q$, integers u, n such that $u \leq n$ and $0 < v_1 < \cdots < v_u < v_{u+1} = n$
- For $1 \leq \ell \leq u$, set vinegar variables $V_\ell = \{1, \ldots, v_\ell\}$ and oil variables $O_\ell = \{v_\ell + 1, \ldots, v_{\ell+1}\}$
- 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

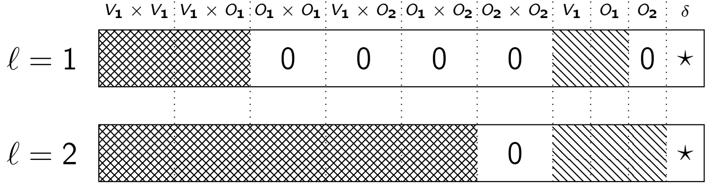
Key generation

- Let $m = n - v_1$ and $o_\ell = v_{\ell+1} - v_\ell$
- Randomly pick two affine transformations $\mathcal{L}_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{L}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- Central map is a function $\mathcal{C} : \mathbb{F}_q^n \to \mathbb{F}_q^m$
  - A total of o_ℓ polynomials and 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

Inversion of the central map

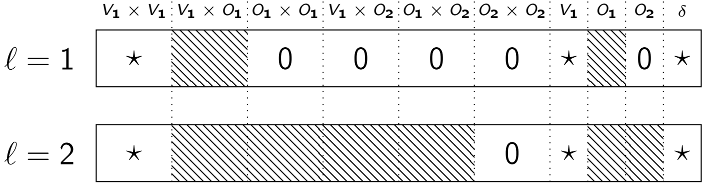
- Vinegar variables of a layer are exactly the oil and vinegar variables from the previous layer
- This enables the inversion of each Oil-Vinegar layer recursively
- With $u = 2$, the initial configuration of $\mathcal{C}$ is



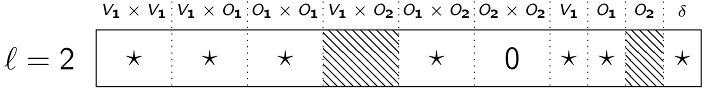
Rainbow signature scheme

Inversion of the central map

- Randomly choose variables in V_1 and substitute them



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



Rainbow signature scheme

Signature generation

- Consider a cryptographic hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{F}_q^m$ and a message M, and compute the digest $\mathbf{h} = \mathcal{H}(M)$
- Obtain the value $\mathbf{x} = \mathcal{L}_1^{-1}(\mathbf{h})$
- Generate the pre-image of $\mathbf{x}$ under the central map, $\mathbf{y} = \mathcal{C}^{-1}(\mathbf{x})$, as per the operations above
- Compute the final signature $\mathbf{z} = \mathcal{L}_2^{-1}(\mathbf{y})$

Rainbow signature scheme

Signature verification

- Obtain $\mathbf{h}$ from the message M
- Compute $\mathbf{h}' = \mathcal{P}(\mathbf{z})$
- The signature is valid if $\mathbf{h} = \mathbf{h}'$, and invalid otherwise

Our proposal

- Introduction of structures in the private key is dangerous and may lead to security holes
- Observe that, to invert the central map, vinegar variables are chosen randomly every time a preimage is computed
- If these variables are changed less often, or fixed, they simplify the central map matrix representation
- Indeed, the central map may be stored in a linearized fashion, and regenerated only occasionally

Our proposal

- We propose to fix the V_1 variables throughout the central map
- A possible implementation of this method is to use a PRNG to regenerate $\mathcal{C}$ every time it is needed
- The linear relations described in CyclicRainbow [PBB10b] are another way to obtain the original central map
- The EUF-CMA variant described in [DCP$^+$17] provides a salt that can be modified instead of vinegar variables

Our proposal

- Only variables in V_1 are fixed, since V_2 and beyond need the digest to be calculated
- Strategy is not hindered by current cryptanalytic methods, since the choice of parameters does not change
- General framework for every Rainbow-like scheme
- Can be applied on top of variants that reduce the public key, confirming our hypothesis

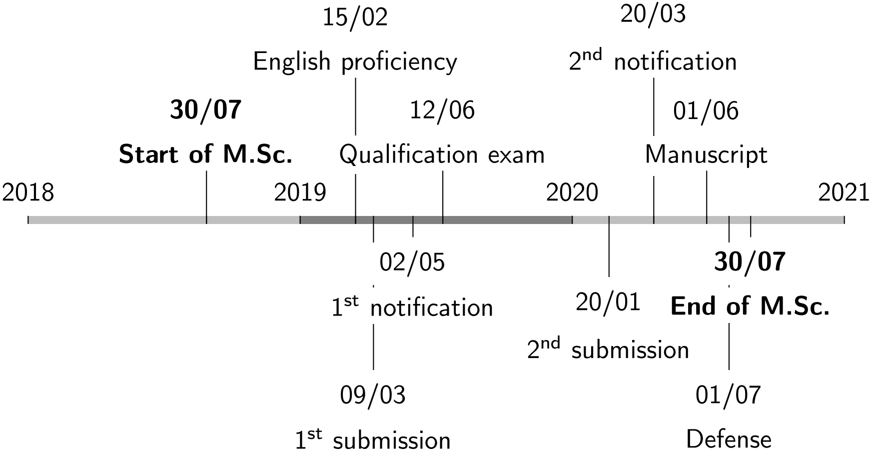
Open problems

- Given multiple signatures created with the same set of vinegar variables, is it possible to unveil information about the private key?
- Does every signature needs its own set of vinegar variables or is the cost of regenerating the central map amortized?
- Is it possible to create a constant-time implementation with this strategy?
- Do there exist parameter sets which optimize the private key size?

Preliminary results [ZBC19]

Parameters	Variant	$\lvert\mathcal{K}_{Pr}\rvert$	$\lvert\mathcal{K}_{Pr}^{\eta}\rvert$	$\lvert\mathcal{K}_{Pu}\rvert$	Difference
	Classic			25740	-28.76%
$(\mathbb{F}_{256}, 17, 13, 13)$	Cyclic	19546	6524	10618	-62.15%
	LRS2			9789	-63.98%
	Classic			60390	-31.60%
$(\mathbb{F}_{256}, 26, 16, 17)$	Cyclic	46131	12474	22246	-67.41%
	LRS2			20662	-68.89%
	Classic			139320	-32.78%
$(\mathbb{F}_{256}, 36, 21, 22)$	Cyclic	105006	24924	48411	-69.98%
	LRS2			45547	-71.16%

Chronology


15/02
English proficiency
20/03
2nd notification
30/07
Start of M.Sc.
12/06
Qualification exam
01/06
Manuscript
2018
2019
2020
2021
02/05
1st notification
20/01
2nd submission
30/07
End of M.Sc.
09/03
1st submission
01/07
Defense

References I

W. Beullens and B. Preneel.
Field Lifting for Smaller UOV Public Keys.
In A. Patra and N. Smart, editors, *Progress in Cryptology – INDOCRYPT 2017*, volume 10698 of *Lecture Notes in Computer Science*, December 2017.

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.

References II

A. Petzoldt and S. Bulygin.
Linear Recurring Sequences for the UOV Key Generation Revisited.
In T. Kwon, M.-K. Lee, and D. Kwon, editors, *Information Security and Cryptology – ICISC 2012*, volume 7839 of *Lecture Notes in Computer Science*, pages 441–455, November 2012.

A. Petzoldt, S. Bulygin, and J. Buchmann.
A Multivariate Signature Scheme with a Partially Cyclic Public Key.
In J.-C. Faugère and C. Cid, editors, *International Conference on Symbolic Computation and Cryptography*, pages 229–235, June 2010.

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.

A. Petzoldt, S. Bulygin, and J. Buchmann.
Linear Recurring Sequences for the UOV Key Generation.
In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography – PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 335–350, March 2011.

References III

A. Petzoldt, S. Bulygin, and J. Buchmann.
Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes.
In P. Gaborit, editor, *Post-Quantum Cryptography*, volume 7932 of *Lecture Notes in Computer Science*, pages 188–202, June 2013.

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.

A. Petzoldt, E. Thomae, S. Bulygin, and C. Wolf.
Small Public Keys and Fast Verification for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Public Key Systems.
In B. Preneel and T. Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 475–490, September 2011.

References IV

A. Szepieniec, W. Beullens, and B. Preneel.
MQ Signatures for PKI.
In T. Lange and T. Takagi, editors, *Post Quantum Cryptography*, volume 10346 of *Lecture Notes in Computer Science*, pages 224–240, June 2017.

P. W. Shor.
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.
SIAM Journal on Computing, 26(5):1484–1509, October 1997.

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 V

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.

G. Zambonin, M. S. P. Bittencourt, and R. Custódio.
Handling Vinegar Variables to Shorten Rainbow Private Keys.
In J. Buchmann, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2019*, volume 11627 of *Lecture Notes in Computer Science*, July 2019.