On the randomness of Rainbow signatures

Gustavo Zambonin

Universidade Federal de Santa Catarina
Graduate Program in Computer Science

gustavo.zambonin@posgrad.ufsc.br

Outline

- Context
  - Multivariate cryptography
- Rainbow signature scheme
  - Description
- Our contributions
  - Rainbow-η
  - Cryptanalysis
- Conclusion
  - Open problems

Context

Introduction

- Security of digital signature schemes is mostly based on problems from number theory
  - Solved efficiently by Shor's quantum algorithm
- Post-quantum cryptography aims to create cryptosystems based on problems immune to quantum speed-ups
  - Several active branches, standardization 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 frequently also on isomorphism of polynomials problems

- Bipolar construction, with central trapdoor

decryption / signature generation

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

encryption / signature verification

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

Rainbow signature scheme

Overview

- Created by Ding and Schmidt (2005), currently a finalist of the NIST standardization process
- Easy description, good balance between signature and key sizes
  - Generalized version of Unbalanced Oil and Vinegar due to Kipnis et al. (1999)
- Keys are systems of equations, orders of magnitude larger than conventional ones
  - RSA at 3072 bits, elliptic curves at 256 bits, Rainbow at roughly 1 Mb

Rainbow signature scheme

Preliminaries

- Parameters are the order q of a finite field, $u, n \in \mathbb{N}$ 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 $O_\ell = \{v_\ell + 1, \ldots, v_{\ell+1}\}$, with $o_\ell = |O_\ell|$
- Consider 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

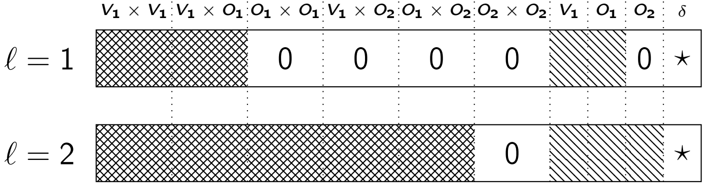
Key generation

- Let $m = n - v_1$ be the number of equations in the keys
- Randomly pick two invertible affine transformations $\mathcal{L}_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{L}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- Central map is a function $\mathcal{C} : \mathbb{F}_q^n \to \mathbb{F}_q^m$
  - Exactly o_ℓ polynomials and their respective coefficients are randomly chosen from each P_ℓ
- Private key is the triple $(\mathcal{L}_1, \mathcal{C}, \mathcal{L}_2)$, public key is the composition $\mathcal{P} = \mathcal{L}_1 \circ \mathcal{C} \circ \mathcal{L}_2$
  - Wolf (2005) shows that $\mathcal{L}_1$ is unneeded if $u = 1$

Rainbow signature scheme

Preimage of the central map

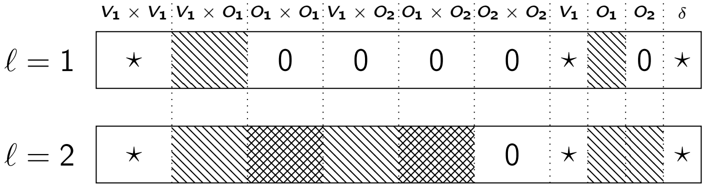
- Vinegar variables of a layer are exactly the oil and vinegar variables from the previous layer
- This enables the inversion of each Oil-Vinegar layer recursively
- With $u = 2$, the initial configuration of $\mathcal{C}$ is



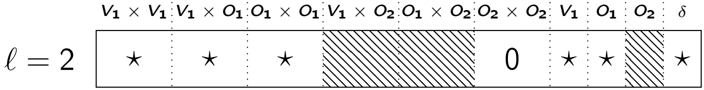
Rainbow signature scheme

Preimage of the central map

- Randomly choose variables in V_1 and substitute them



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



Rainbow signature scheme

Signature generation

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

Rainbow signature scheme

Signature verification

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

Evolution of our research

- Reduction of key sizes in Rainbow-like schemes
  - Current methods to reduce keys are not usually compatible between themselves
  - To the best of our knowledge, adding structure to the key space is a delicate matter
- Analysis of choice of vinegar variables in the signature generation of Rainbow
  - Early substitution of vinegars in the private key to allow its reduction
  - Consequences of manipulating the randomness of signatures

Initial proposal

Approach

- 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, denoted Rainbow-η
-

Initial proposal

Ensuring a preimage 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 due to Petzoldt et al. (2010)
- EU-CMA variant submitted to NIST by Ding et al. (2019) makes use of a salt that can be modified instead of V_1

Initial proposal

Effect of the construction

- Preimages with fixed elements are shuffled by $\mathcal{L}_2$, preserving the randomness of signatures
  - Statistical argument through differences of means, std. deviations, comparison of CDF and Q-Q plots
- Structure of the scheme is unchanged, conventional parameters are used
  - To the best of our knowledge, current algebraic cryptanalysis is ineffective
  - Side-channel attacks are not investigated, but we acknowledge that regenerating $\mathcal{C}$ is highly detectable

Initial proposal

Key pair reductions for newest NIST parameters due to Ding et al. (2020)

Parameters	Variant	$\#\mathbf{sk}$	$\#\mathbf{sk}^{\eta}$	$\#\mathbf{pk}$	Difference
$(\mathbb{F}_{16}, 36, 32, 32)$	Classic	103 616	27 026	161 600	−28.88%
	nCyclic			60 160	−67.13%
$(\mathbb{F}_{256}, 68, 32, 48)$	Classic	626 016	107 652	882 080	−34.37%
	nCyclic			264 576	−75.32%
$(\mathbb{F}_{256}, 96, 36, 64)$	Classic	1 408 704	204 384	1 930 600	−36.07%
	nCyclic			536 104	−77.83%

Cryptanalysis of vinegar variables

Introduction

- Found in works related only to side-channel attacks
  - Introduction of faults leading to zero out or reuse of vinegar variables
- Practical fault attacks are not easily performed, as argued by Mus et al. (2020)
  - If a user fixes V_1 through Rainbow-η, then faults are not needed
- We propose an attack that leads to an equivalent private key from signatures with the same V_1
  - Closely related to the UOV attack due to Kipnis et al. (1999) that broke balanced OV

Cryptanalysis of vinegar variables

Equivalent keys

- Due to the bipolar construction, there exist equivalent private keys that compose to the same public key
  - Extended isomorphism of polynomials problem in the case of Rainbow
- It is shown by Wolf (2005) that there are several redundant private keys in the key space of Rainbow
  - Security is not reduced if simpler $\mathcal{L}_1$ and $\mathcal{L}_2$ are chosen
- Several algebraic attacks are based on finding equivalent keys from some structure introduced to the scheme

Cryptanalysis of vinegar variables

UOV attack ($u = 1$)

- The set $\{(0, \ldots, 0, x_{v+1}, \ldots, x_n) \in \mathbb{F}^n\}$ with usual binary operations is the oil subspace $\mathcal{O}$, and $\widetilde{\mathcal{O}} = \mathcal{L}_2^{-1}(\mathcal{O})$
- For $f^{(i)}, f^{(j)} \in \mathcal{C}$, $f^{(i)} \circ (f^{(j)})^{-1}$ preserves a part of $\mathcal{O}$

  (composition of maps from unique symmetric matrices out of homogeneous quadratic $f^{(i)}, f^{(j)}$)
  - Similarly, $\widetilde{\mathcal{O}}$ is invariant under combinations of public polynomials
- Finding the common invariant subspace $\widetilde{\mathcal{O}}$ leads to an equivalent map $\widetilde{\mathcal{L}}_2$, and **sk'** $= (\mathcal{P} \circ \widetilde{\mathcal{L}}_2, \widetilde{\mathcal{L}}_2^{-1})$
  - Complexity is $q^{n-1-2\cdot o_u} \cdot o_u^4$ field multiplications

Cryptanalysis of vinegar variables

Breaking Rainbow-η

- UOV attack is also applicable to Rainbow, since it can be interpreted as a large, single UOV scheme
- If $u = 1$, for any two $\mathbf{z}^{(i)}, \mathbf{z}^{(j)}$ produced with Rainbow-η, then $\mathcal{L}_2(\mathbf{z}^{(i)} - \mathbf{z}^{(j)}) = (0, \ldots, 0, *, \ldots, *) \in \mathcal{O}$
- From at least $m + 1$ signatures, obtain m linearly independent vectors of $\widetilde{\mathcal{O}}$
  - Obtain a basis of the subspace and thus $\widetilde{\mathcal{L}}_2$
- If $u > 1$, we need to solve for the remaining $x_{v_1+1}, \ldots, x_{v_u}$
  - Polynomial system with m quadratic equations and $m - o_u$ variables

Conclusion

- Elimination of randomness from Rainbow signatures is not recommended
  - Signatures look statistically random but still leak information
  - Private key size is greatly reduced at the expense of security
- Attack in polynomial time if $u = 1$ and all vinegar variables fixed
  - If $u > 1$, performing the attack is easier than all other known cryptanalytic methods by a large margin
  - If V_1 is only partially fixed, Shim and Koo (2020) argue that the resulting scheme is still insecure

Conclusion

Open problems

- Storage of previously used vinegar variables to prevent reuse
  - Private key becomes stateful and larger
- Poor random number generation on signature generation may be exploited
- Countermeasures against tampering of intermediate signing steps
  - Checksum alongside signature
  - Obtain vinegar variables deterministically from private key and message

References I

Ding, J., Chen, M.-S., Patarin, J., Petzoldt, A., Schmidt, D., and Yang, B.-Y. (2020). Modified Parameters of Rainbow in Response to a Refined Analysis of the Rainbow Band Separation Attack by the NIST Team and the Recent New MinRank attacks.

Ding, J., Chen, M.-S., Petzoldt, A., Schmidt, D., and Yang, B.-Y. (2019). Rainbow - Algorithm Specification and Documentation. Round 2 Submission, NIST Post-Quantum Cryptography Standardization Process.

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

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

Mus, K., Islam, S., and Sunar, B. (2020). QuantumHammer: A Practical Hybrid Attack on the LUOV Signature Scheme.

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

Shim, K.-A. and Koo, N. (2020). Algebraic Fault Analysis of UOV and Rainbow With the Leakage of Random Vinegar Values. *IEEE Transactions on Information Forensics and Security*, 15:2429–2439.

References II

Wolf, C. (2005). *$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Polynomials in Public Key Cryptography*. PhD thesis, Katholieke Universiteit Leuven.