Reduction of Key Sizes on Rainbow-like Multivariate Signature Schemes

Gustavo Zambonin

INE410111 — Research Methodology in Computer Science

gustavo.zambonin@posgrad.ufsc.br

Context

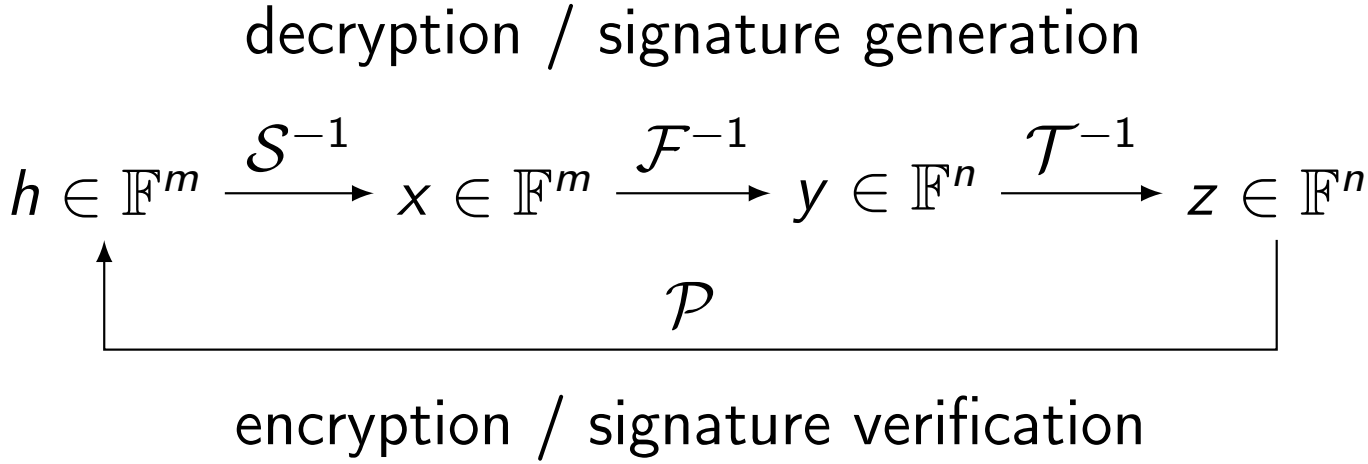
- Guarantee protection and privacy of messages sent digitally
- Security of digital signature schemes is based on problems from number theory
- There exist quantum algorithms [Sho97] that solve these problems efficiently
- Post-quantum cryptography aims to create cryptosystems based on problems immune to quantum speedups

Motivation

- Imminent threat from quantum computers
- Several active branches of post-quantum cryptography
  - Focus on cryptosystems that are based on the difficulty of solving systems of equations
- Standardization calls by institutions such as NIST and IRTF
- Development of quantum computers by corporations, such as Google and Intel

Multivariate cryptography

- Cryptography based on systems of multivariate quadratic equations over finite fields

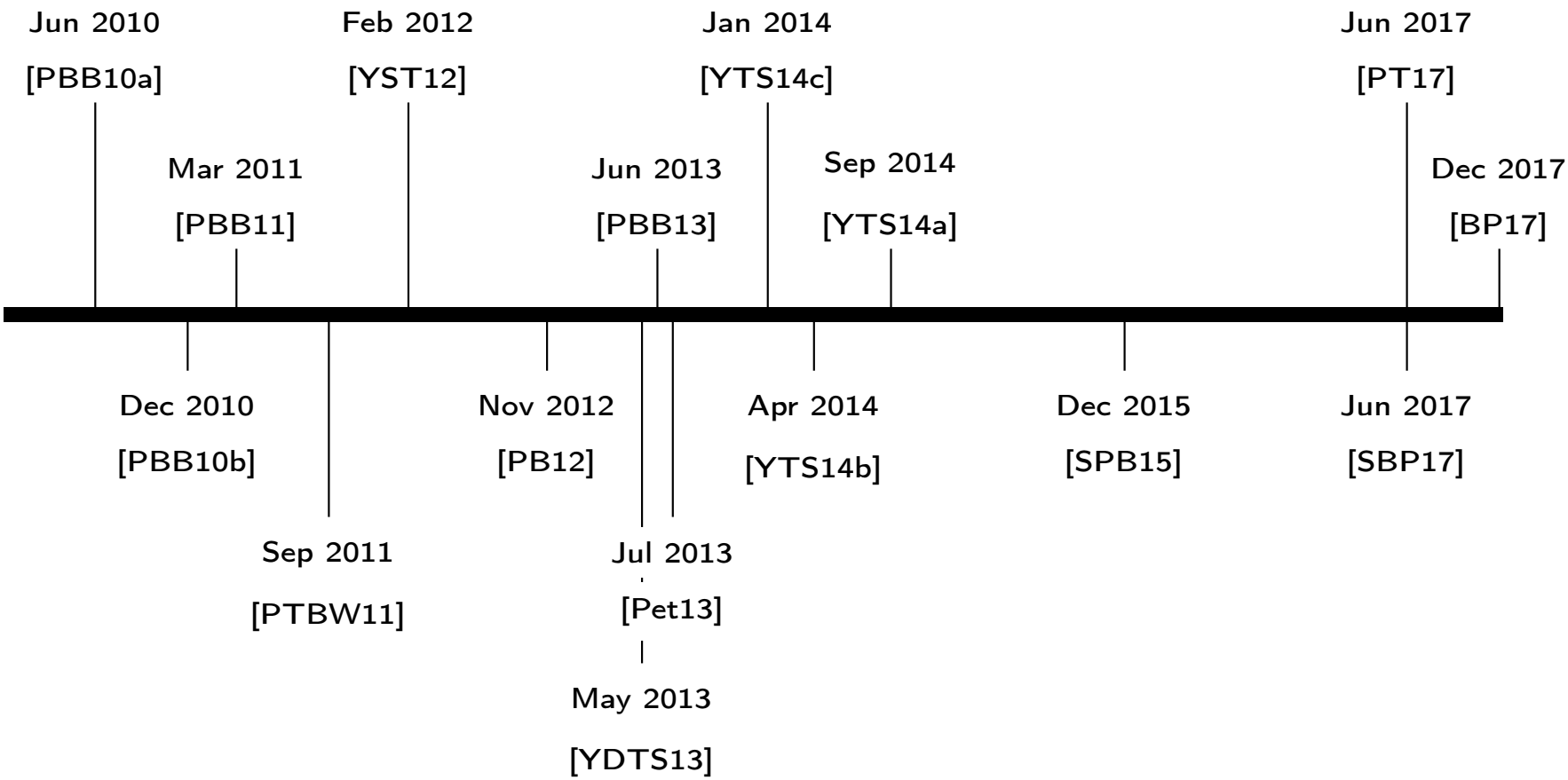


- Fast operations, small signature sizes, large keys

Underlying issue

- Focus on the Rainbow signature scheme, due to Ding and Schmidt [DS05], submitted to NIST for standardization
- Easy description, good balance between signature and key sizes
- Keys in the order of 10 KB, while classical schemes feature sub-1 KB
- Introduction of structures in the keys may lower security

Related works



Hypothesis

- Works have reduced either private or public keys, separately
- Do there exist any restrictions in doing both at the same time?
- Is it possible to generate a structured public key from a similarly composed private key?
- Introduction of matrix symmetries as possible arrangements may lower security

Objectives

- Establishment of fit matrix structures to be introduced
- Measurement of security achieved by keys created with those matrices
- Development of a method in which private and public keys are structurally related
- Description of a new signature scheme with carefully chosen parameters for devices with distinct requirements

Methodology

- Review schemes that reduce key sizes, cryptanalysis of these, and study matrix-like symmetric structures
- Create an algorithm to generate a compact private-public key pair
- Apply currently known cryptanalytic methods to test security of signatures created by these keys
- Compare performance and security with related works
- Publish and present results through papers, dissertation etc.

Expected results

- Identify the relationship between matrix types and their effect on security
- Deep analysis on how to maintain structure when generating a key pair
- Present a Rainbow-like signature scheme that features reduction of private and public key sizes
- International collaboration and scientific contributions

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 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. 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.

References II


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.


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.

References III


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.


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.

References IV

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.

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.

References V

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.

T. Yasuda, T. Takagi, and K. Sakurai.
Security of Multivariate Signature Scheme Using Non-commutative Rings.
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E97.A(1):242–252, January 2014.