Our current research in multivariate cryptography

Gustavo Zambonin

zambonin.org

Laboratório de Segurança em Computação
Universidade Federal de Santa Catarina

January 29th, 2020

- Quantum-safe cryptography (mainly signatures) through multivariate quadratic equations over finite fields
- Several families with different constructions or polynomial spaces (HFE, **Oil–Vinegar**, MQDSS etc.)
- Signature operations are very efficient but key sizes are large systems of equations (up to 100KB)
- We focus on the Rainbow signature scheme in our research, a generalization of UOV submitted to NIST
- How can we **securely reduce** the key sizes of Rainbow instances without limiting parameter sets?

- We have observed that the literature contains strategies that are mostly incompatible between themselves

- Furthermore, several private key reductions are based on the insecure introduction of structures into the key

- We aim to provide a method that reduces public and private keys **at the same time**

- To create a signature, random values are substituted into the private keys, yielding solvable* systems of equations

- What if such values are pre-substituted into the private key? It may then be stored in a smaller fashion

- We provide ways to obtain the original private key and show that this rarely happens
- The general structure of the scheme is not changed, thus making it a generic framework, which we call Rainbow-η
- This method is not conflicting with strategies that reduce public keys, achieving our original goal
- 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*, pages 391–408, July 2019

NIST Cat.	n	m	$\lvert\mathcal{K}_{Pr}\rvert$	$\lvert\mathcal{K}^{\eta}_{Pr}\rvert$	Difference
I-c	88	48	143384	33024	-76.97%
III-c	140	72	537780	99656	-81.47%
V-c	188	96	1274316	218984	-82.82%

Security	Variant	$\lvert\mathcal{K}_{Pr}\rvert$	$\lvert\mathcal{K}^{\eta}_{Pr}\rvert$	$\lvert\mathcal{K}_{Pu}\rvert$	Difference
128	Classic	105006	24924	139320	-32.78%
	Cyclic			48411	-69.98%
	LRS2			45547	-71.16%

- Key sizes are in number of $\mathbb{F}_{256}$ elements, or bytes

- More precise security considerations, e.g. cryptanalysis and side-channel attacks, are currently being worked on