Security Analysis of the Rainbow-η Signature Scheme

Gustavo Zambonin

School of Electrical Engineering and Computer Science
University of Ottawa

March 4th, 2021

International Research Mobility Symposium @ Carleton University

Context

- Digital signatures are widely used to provide authenticity, integrity and non-repudiation to communications
- Their security is usually based on problems from number theory, solved efficiently by Shor's quantum algorithm
- **Quantum-safe cryptography** aims to create public-key cryptosystems secure against quantum computers
- We focus on the Rainbow signature scheme, based on systems of multivariate equations over finite fields
- Signature generation and verification are efficient but key sizes are large systems of equations (up to 100KB)

Strategy

- Large keys are a problem for embedded devices and efficient secure communications over a network (HTTPS)
- How can we **securely reduce** the key sizes of Rainbow without limiting parameter configuration?
- To generate a signature, random values are substituted into the private key, creating solvable systems of equations
- What if such values are pre-substituted into the private key? It may then be stored in a smaller fashion
- The result is Rainbow-η, which reduces the key pair by up to 71%, but lacks precise security analysis

Analysis

- Due to the pre-substitution of values in the private key of Rainbow-η, the randomness of signatures is not preserved
- A small number of signatures can be collected by an attacker and used to create an **equivalent private key**
- Complexity of the attack for usual parameters is non-trivial, but still much smaller than desired
- Proof-of-concept implementations of the attack in SageMath and Magma for small parameters
- Rainbow-η is not recommended as a secure signature scheme (cf. `https://github.com/zambonin/msc`)