Quantum Cryptanalysis of Multivariate Cryptosystems

Research Internship Proposal

General Information.

Keywords: Cryptology - cryptanalysis - multivariate quadratic equations - quantum algorithms.
City and Country: Rennes, France.
Team: CAPSULE, in the IRISA lab, located in Université de Rennes 1
Advisor 1: Pierre-Alain Fouque, team leader (`pierre-alain.fouque /at/ univ-rennes1.fr`)
Advisor 2: André Schrottenloher (`andre.schrottenloher /at/ inria.fr`)

Context. Large-scale quantum computing devices have the potential to disrupt traditional cryptographic methods, due to their ability to break some problems such as *factoring* and *discrete logarithm* [Sho94] which are believed to be classically intractable. This has led to a massive effort of research and design of new *post-quantum* cryptographic schemes, based on different hardness assumptions, which are believed to hold against quantum computers. Currently this effort is embodied by the NIST post-quantum standardization process [NIS16], which started in 2016 and is still ongoing.

Multivariate cryptosystems form one of the families being actively studied. They are based on the hardness of solving multivariate polynomial equation systems. However, despite having been around for quite some time, none of the 2016 NIST candidates made it to standardization. Notably, the digital signature candidate Rainbow was broken very lately in the competition [Beu22]. At the same time, the *quantum* security of multivariate cryptosystems, i.e., attacks that may be applicable using a quantum computer, has not received much attention either.

Objective. The goal of this internship will be to advance the security analysis of post-quantum multivariate cryptosystems.

On the one hand, we will study generic algorithms for solving multivariate equation systems. At the moment, the best algorithm for multivariate quadratic equations (MQ_2) is given by [FHK+17]. We will try to improve on this algorithm, by taking inspiration from other classical algorithms for MQ_2 (see [BMSV22] for a short survey).

On the other hand, we will study the security of concrete designs. While the NIST candidates were broken or weakened during the competition, the original UOV scheme is still widely believed secure [KPG99] and the digital signature scheme MAYO [Beu21], which is a variant of UOV, was recently proposed by Beullens. Notably, MAYO differs from UOV by adding a new structure (the "whipping" structure), and it is not known yet if this structure can lead to better attacks than the known attacks on the standard UOV assumptions.

References.

Beu21. Ward Beullens. MAYO: practical post-quantum signatures from oil-and-vinegar maps. In *SAC*, volume 13203 of *Lecture Notes in Computer Science*, pages 355–376. Springer, 2021.

Beu22. Ward Beullens. Breaking rainbow takes a weekend on a laptop. In *CRYPTO (2)*, volume 13508 of *Lecture Notes in Computer Science*, pages 464–479. Springer, 2022.

BMSV22. Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. *IACR Cryptol. ePrint Arch.*, page 708, 2022.

FHK+17. Jean-Charles Faugère, Kelsey Horan, Delaram Kahrobaei, Marc Kaplan, Elham Kashefi, and Ludovic Perret. Fast quantum algorithm for solving multivariate quadratic equations. *CoRR*, abs/1712.07211, 2017.

KPG99. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.

NIS16. NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2016.

Sho94. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS*, pages 124–134. IEEE Computer Society, 1994.

Expected Ability of Candidates. Candidates should have some background in cryptography (not necessarily multivariate / asymmetric). Knowledge of basic quantum algorithms (Shor, Grover) will be helpful, but is not required. It is not required to speak french.