Quantum algorithms for solving systems of polynomial equations

We are seeking an excellent candidate for a 5 to 6-month research internship at the interface of computational mathematics, algebraic and real algebraic geometry, with the goal of solving challenging problems which arise in optical system design. This internship is proposed to students willing to pursue a Ph.D. after obtaining their Master degree.

The internship will be hosted by PolSys team (Polynomial Systems) of Sorbonne Université and CNRS.

Key words: Computer algebra, quantum algorithms, quantum cryptanalysis

The context of multivariate cryptography

Solving polynomial systems has numerous applications in many scientific areas, including cryptography. Indeed, the so-called multivariate cryptosystems relying on the hardness of solving polynomial systems of quadratic equations are currently under scrutiny by the American National Institute for Standards and Technology (NIST) and may become the future cryptographic standards. The reason is that solving systems of polynomial equations is notoriously difficult and it is expected to be so even for quantum computers, meaning that multivariate cryptosystems offer post-quantum security.

Multivariate cryptography is an active topic leading to many cryptographic schemes [1, 3, 6, 14, 18] and requiring a significant effort in terms of cryptanalysis. Over the years, this showed that some of these schemes were actually insecure [2, 15], while giving a fair confidence in schemes such as UOV [14] which have withstood more than 25 years of cryptanalysis.

However, most of the attacks against multivariate schemes were classical attacks, i.e. attacks that can be implemented and run on a classical computer. Given that multivariate schemes are supposed to be resistant against quantum computers, it is surprising to see that very little effort has been made to leverage the power of quantum algorithms in a cryptanalytic context.

The purpose of this internship is to study this matter by answering the following question: can the current algorithms for solving systems of polynomial equations benefit from a significant speed-up by using quantum subroutines?

Quantum algorithms for polynomial systems

In the classical setting, the most widely used approaches are based on three techniques: the computation of Gröbner bases [8, 9, 10] or the XL heuristic [5], the geometric resolution algorithm [12] and the symbolic or hybrid symbolic/numeric homotopy techniques [17]. Over finite fields and especially in a cryptographic setting, it is often beneficial to combine such algorithms with an enumerative approach when the base field is small enough.

Quite naturally, the current quantum algorithms for solving polynomial systems are quantum adaptations of these approaches [4, 11, 20], replacing several key subroutines with quantum algorithms such as quantum linear algebra [13, 19] or using Grover's algorithm [16] for a faster enumeration. This approach has been already investigated in the context of the so-called linear-algebra based algorithms for computing Grbner bases or the XL heuristic. Indeed, such algorithms reduce the problem of solving systems of polynomial equations to Gaussian elimination problems in matrices.

This first approach already yields a speed-up, brought by quantum linear algebra algorithms which are then used on the Macaulay matrices generated by Grbner bases algorithms (such matrices are named after the mathematician Francis Sowerby Macaulay).

The fact that Macaulay matrices are notoriously ill-conditioned makes it all the more relevant to study approaches relying on a different paradigm, namely the use of Hensel lifting to iteratively build approximate solutions until the precision is large enough to guarantee that the returned solutions are exact solutions. We expect that this approach can make it easier to identify and leverage the peculiarities of the systems such as sparsity, multihomogeneity, etc. in order to derive sharper complexity bounds.

Organization and expected outcome of the internship

As sketched above, the internship will focus on algorithmic paradigms that differ from the ones classically used to compute Grbner bases, namely the geometric resolution algorithms (see e.g. [12]) and symbolic homotopy techniques (see e.g. [7]).

Both algorithms rely on Hensel liftings which can be seen as a symbolic variation of Newton iteration. While Newton iteration iteratively (and numerically) approaches solutions to a given problem, making smaller and smaller the distance of the approximant to the solution, Hensel lifting approaches symbolically algebraic objects (such as a rational parametrization of a curve) modulo powers of a given indeterminate. A key similarity, with Newton iteration, is that, Hensel lifting, as it is used in the geometric resolution algorithm and symbolic homotopy techniques, relies on the inversion of Jacobian matrices at the current approximant.

Hence, Hensel lifting is used to compute a "lazy" rational paramatrization of a curve $\mathscr{C}$, starting from a parametrization of the set of points obtained by intersecting $\mathscr{C}$ with a generic hyperplane. In a sense, boils down to perform Newton iteration with entries which are zero-dimensional parametrizations with coefficients which are truncated power series.

Hence, our goal is to investigate how to adapt the quantum Newton iteration designed in [20] to this setting, establish the corresponding complexity results and compare with the state of the art quantum algorithms.

Concretely, the work of the internship will be articulated around the following tasks.

- study and become familiar with the geometric resolution algorithms and symbolic homotopy techniques, as described in the setting of classical computing.

  This task requires to deeply understand these algorithms, from a theoretical point of view but also a practical one (maybe a prototype implementation could be useful) and master the complexity results related to these algorithms.

- become familiar with the main quantum algorithms for algebra (linear algebra, Newton's method),

  This task requires to master the main differences between those quantum algorithms and the classical ones, as well as the rationale behind the differences of the complexity statements in the quantum model and the classical one.

- put together the necessary tools to propose a quantum version the geometric resolution and homotopy techniques, and perform an analysis of its complexity in terms of qubits and number of gates/operations,

  Here, we expect compelxity results depending of course on some conditioning measure which should be as explicit as possible

- if time allows, improve the subroutines from existing literature to achieve better performance.

Scientific environment. This internship will be co-supervised by Simon Abelard (EPITA) Mohab Safey El Din (Sorbonne Université & CNRS). It will take place at Sorbonne Université, in the computer science lab LIP6, which is located on the Pierre-et-Marie-Curie campus, at the heart of Paris. The intern will be welcome in the PolSys team, which develops and implements fast computer algebra algorithms, for polynomial system solving and their applications, such as coding theory, combinatorics, cryptography, and robotics. The intern will work in a kind and international environment gathering PhD students and Post-Docs representing several nationalities, and animated with several working groups and a monthly seminar. All computing facilities will be provided.

Weekly meetings with the supervision team will be organized.

Prerequisites. We are looking for exceptional candidates who are excited about computer algebra, quantum algorithms and cryptography, in a broad sense.

We expect curiosity and openness, experience with mathematical software, strong interpersonal and communicative skills, and willingness to dive into new topics, including the implementation of powerful mathematical algorithms.

How to apply. Applicants should send a full CV, a letter of motivation and the grades obtained during the last two years to

simon.abelard@protonmail.com, mohab.safey@lip6.fr

References

[1] Ward Beullens. Mayo: practical post-quantum signatures from oil-and-vinegar maps. In *International Conference on Selected Areas in Cryptography*, pages 355–376. Springer, 2021.

[2] Ward Beullens. Breaking rainbow takes a weekend on a laptop. In *Annual International Cryptology Conference*, pages 464–479. Springer, 2022.

[3] Antoine Casanova, Jean-Charles Faugere, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. *GeMSS: a great multivariate short signature*. PhD thesis, UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team ..., 2017.

[4] Yu-Ao Chen and Xiao-Shan Gao. Quantum algorithm for boolean equation solving and quantum algebraic attack on cryptosystems. *Journal of Systems Science and Complexity*, 35(1):373–412, 2022.

[5] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.

[6] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security*, pages 164–175. Springer, 2005.

[7] Mohab Safey El Din and Éric Schost. Bit complexity for multi-homogeneous polynomial system solving—application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, 2018.

[8] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[9] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). *Proceedings of ISSAC 2002*, 2002.

[10] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[11] Jean-Charles Faugere, Kelsey Horan, Delaram Kahrobaei, Marc Kaplan, Elham Kashefi, and Ludovic Perret. Fast quantum algorithm for solving multivariate quadratic equations. *arXiv preprint arXiv:1712.07211*, 2017.

[12] Marc Giusti, Grégoire Lecerf, and Bruno Salvy. A Gröbner free alternative for polynomial system solving. *Journal of complexity*, 17(1):154–211, 2001.

[13] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[14] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.

[15] Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil and vinegar signature scheme. In *Annual international cryptology conference*, pages 257–266. Springer, 1998.

[16] Aamir Mandviwalla, Keita Ohshiro, and Bo Ji. Implementing grover's algorithm on the ibm quantum computers. In *2018 IEEE international conference on big data (big data)*, pages 2531–2537. IEEE, 2018.

[17] Alexander Morgan and Andrew Sommese. Computing all solutions to polynomial systems using homotopy continuation. *Applied Mathematics and Computation*, 24(2):115–138, 1987.

[18] Jacques Patarin, Benoît Cogliati, Jean-Charles Faugèare, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, and Brice Minaud. Vox. *Specification document of NIST PQC Standardization of Additional Digital Signature Scheme*, 2023.

[19] Anupam Prakash. *Quantum algorithms for linear algebra and machine learning.* University of California, Berkeley, 2014.

[20] Cheng Xue, Yuchun Wu, and Guoping Guo. Quantum newton's method for solving the system of nonlinear equations. In *Spin*, volume 11, page 2140004. World Scientific, 2021.