Ph.D. in Information Technology
Thesis Defense

May 15th, 2024
at 15:00
Room BIO1 – building 21

Simone PERRIELLO– XXXV Cycle

QUANTUM CIRCUITS FOR INFORMATION SET DECODING: QUANTUM CRYPTANALYSIS OF CODE-BASED CRYPTOSYSTEMS

Supervisor: Prof. Gerardo Pelosi

Abstract:

The emergence of quantum computing represents a profound challenge to the security of widely-adopted public-key cryptographic systems, which rely on the computational complexity of tasks such as factoring large integers or solving discrete logarithms. To confront this challenge, esteemed organizations like the U.S. National Institute of Standards and Technology (NIST), the Chinese Association for Cryptologic Research (CACR), and the European Telecommunications Standards Institute (ETSI) are actively engaged in the formulation of cryptographic primitives capable of withstanding both classical and quantum attacks. These novel cryptographic systems, collectively termed post-quantum cryptosystems, are at the forefront of standardization efforts. Among the leading contenders in this standardization endeavor, linear code-based cryptosystems, deriving their strength from the computational complexity of the Syndrome Decoding Problem (SDP), have gained significant recognition. The SDP is defined as the task of retrieving an error vector when provided with the parity check matrix of a randomly generated linear block error correction code and the syndrome of the error, as computed through the same matrix. Classically, the most effective technique for solving the SDP is the Information Set Decoding (ISD) method, which, notably, exhibits exponential complexity with respect to the parameters of the cryptosystems. Current quantum approaches to the SDP, on the other hand, do not surpass the quadratic speedup offered by adapting Grover’s algorithm to the ISD technique, and provide only asymptotic estimates of their computational cost, potentially hiding non-trivial constant and polynomial factors. The central focus of this study revolves around the precise computational complexity evaluation of quantum solvers for the SDP, tailored to cryptography-grade code parameters. Our approach introduces quantum circuits designed for universal quantum gate-based computing models, that are build upon the foundations laid by classic ISD techniques. Our scrutiny extends to both complete quantum solutions to the SDP and hybrid methodologies that effectively partition the computational load between classical and quantum computing resources. In our investigation, the approach stemming from Prange’s approach to the ISD technique stands out, as it displays a substantial enhancement in computational efficiency. Notably, it leads to a reduction in both the depth of quantum circuits and the depth-times-width metric by factors ranging from 2^{12} to 2^{24} applicable to concrete cryptography-grade parameters. Surprisingly, our

findings reveal that the gains achieved through the approach inspired by Lee and Brickell's ideas, which materialize as a hybrid classical-quantum algorithm, are somewhat modest. These enhancements range from 2^{10} to 2^{20} for the same cryptographic parameters, a result contrary to expectations based on classical counterparts, where Lee and Brickell's approach prevails over Prange's one. However, the hybrid approach substantially reduces the size and depth of quantum circuits, rendering the estimates more realistic and facilitating parallel execution on separate quantum computing platforms. Our quantitative analysis of computational costs brings forth a significant conclusion: all code-based cryptoschemes under the scrutiny of esteemed organizations such as NIST, particularly BIKE, HQC, and McEliece, unequivocally surpass the predefined threshold for computational hardness. Put simply, they prove to be computationally more demanding than the task of breaking a corresponding symmetric cipher with appropriately-sized key lengths. Furthermore, a critical vulnerability in the Classic McEliece cryptoscheme is unveiled. Parallelizing this algorithm across multiple quantum processing units erodes its security, plunging it below the targeted security threshold by a factor of 16. An ancillary contribution of this research is the development of a set of quantum circuits capable of solving common algebraic and algorithmic problems, including Gauss-Jordan Elimination over finite fields, bit string sorting, and Hamming weight computation, which may be of independent interest in the field of quantum computing.

Daniele CATTANEO – XXXV Cycle

TECHNOLOGY AND APPLICATIONS OF COMPILER-BASED PRECISION TUNING

Supervisor: Prof. Giovanni Agosta

The complexity and resource requirements of computer software appear to increase every day, and much of this software performs many high-precision calculations. In order to save computational resources and power, it is possible to reduce the precision of these calculations, but special care must be taken in order to ensure the results are sufficiently correct for each given use-case. Reducing precision in computer software is a task mostly performed manually, but being a hard and tedious task for the programmer, often this is not done. However, by performing this transformation in an automatic way through a specifically-designed compiler, it is possible to reduce programmer effort and therefore increase the adoption of this kind of technique. While this is a promising approach, current precision tuning solutions are not ready for widespread adoption in the industry, due to several limitations that only make them effective in a narrow range of situations. In this work we attempt to improve the current state-of-the-art in precision tuning by introducing novel approaches to tackle several of the problems that are the most impactful with respect to the adoption of this technique at large. We describe an improved data type allocation algorithm that allows for faster compilation times with respect to other state-of-the-art approaches, while properly taking into account user requirements with respect to the speedup and output precision. Then, we propose a methodology to handle low-precision mathematical routines while avoiding combinatorial explosion in library code size. We also discuss how to extend precision tuning tools to support multiprocessor architectures and GPGPU-type accelerators. Finally, we show the potential impact of precision tuning on real-world applications such as fall detection devices and motor controllers.One more application where precision tuning

is of surprising interest is the world of real-time computing. We show that by applying precision tuning one can automatically optimize software in order to ensure an execution time constraint is satisfied. All of these contributions are implemented within the TAFFO precision tuning framework, and are validated through an extensive set of experiments performed on embedded systems and HPC-like systems alike.

PhD Committee

Prof. William Fornaciari, Politecnico di Milano

Prof. Biagio Cosenza, Università degli Studi di Salerno

Prof. Bartolomeo Montrucchio, Politecnico di Torino