Hybrid Number Field Sieve (NFS): Classical and Quantum approaches.

Reference	CYBERINSTITUTE-INT-20008
Description	The Number Field Sieve (NFS)[1] is currently the best integer factoring algorithm for general RSA moduli on classical computers. While we know that Shor's quantum algorithm[2] solves the problem in quantum polynomial-time, the size of the fault-tolerant quantum computer needed for its concrete application seems currently beyond reach for the next decades. On the other hand, there are several bottlenecks in the NFS algorithm which are almost "combinatorial in nature" (e.g., the core of the sieving part). Several approaches have been proposed in order to mix quantum computing and classical computing for NFS. Among them, the work of Bernstein, Biasse and Mosca[3] and more recently the work of Mosca et al[4, 7], using speedup with a quantum SAT solver (and not requiring a fault-tolerant quantum computer) or works of Gidney and Ekera[9] using "noisy qubits". In complement, there has been several attempts to develop alternative to NSF based on quantum SAT solving (even using quantum annealing as in the DWAVE calculator - https://www.dwavesys.com/) such as [5, 6]. The goal of this internship is to compare at the low-level, combining both number theory, algorithmic improvements and quantum computing, the above results and develop our own experiments in order to refine the thresholds proposed by the different authors with the specific goal to reduce the number of qubits required to apply the quantum part of such "Hybrid NFS version" and contribute to some benchmarking for a classical-quantum cryptanalysis of RSA, complementary to the results of [8]. <u>References</u> [1] Joe P. Buhler, Hendrik W. Lenstra, Jr., and Carl Pomerance. *Factoring integers with the number field sieve*. In Arjen K. Lenstra and Hendrik W. Lenstra, Jr., editors, The development of the number field sieve, volume 1554 of Lecture Notes in Mathematics, pages 50?94. Springer Berlin Heidelberg, 1993. [2] Peter Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM Journal on Computing, 26(5) :1484-1509,1997. [3] Daniel J. Bernstein and Jean-François Biasse and Michele Mosca. *A low-resource quantum factoring algorithm*, Cryptology ePrint Archive, Report 2017/352,2017. [4] Michele Mosca and João Marcos Vensi Basso and Sebastian R. Verschoor. *On speeding up factoring with quantum SAT solvers*, 2019. Arxiv :1910.09592. [5] Michele Mosca and Sebastian R. Verschoor. *Factoring semi-primes with (quantum) SAT-solvers*. 2019. arXiv :1910.09592. [6] Shuxian Jiang, Keith A. Britt, Alexander J. McCaskey, Travis S. Humble, Sabre Kais. *Quantum Annealing for Prime Factorization*. 2018. arXiv :1804.02733 [7] João Marcos Vensi Basso and Sebastian R. Verschoor. *NFS-SAT* (GitHub repository). Oct. 2019. https://github.com/sebastianv89/NFS-SAT. [8] Vlad Gheorghiu and Michele Mosca. *Benchmarking the quantum cryptanalysis of symmetric, public-key and hash based cryptographic schemes*, 2019. arXiv :1902.02332. [9] Craig Gidney, Martin Ekerå. *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. 2019. arXiv :1905.09749 <u>Context:</u> The Grenoble Alpes Cybersecurity Institute – in short, Cyber@Alps – is a project selected in 2017 by the Cross-Disciplinary Program (CDP) of the IDEX Univ. Grenoble Alpes and aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy protection challenges. Our main technical focus are on cost effective secure elements, security of critical infrastructures all along their life cycle, vulnerability analysis and global challenges in terms of risk analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad (https://cybersecurity.univ-grenoble-alpes.fr)
Prerequisites	The candidate should have a strong cursus in mathematics (including number theory and computer algebra), and should have

financed by IDEX Université Grenoble Alpes

	attended successfully advanced courses in physics (including quantum physics) and quantum computing. The candidate should also have basic knowledge in complexity theory. Knowledge in advanced learning models would be much appreciated. The candidate should be fluent in english.

Tutors	Philippe Elbaz-Vincent, Mehdi Mhalla
Applications	Please send your resume, application letter with two recommendations (including education director), first year master's degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr For more information on the internship, please contact philippe.elbaz-vincent@univ-grenoble-alpes.fr
Location	Institut Fourier, 100 rue des Mathématiques, 38610 Gières
Starting date	February-March 2020
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.

financed by
IDEX Université Grenoble Alpes