Qing Chen
ECE 646
Final Project Specifications

List of team member:
Qing Chen

Project title:
Parameters Optimization of Post-Quantum Cryptography Schemes

Introduction and motivation:
The field of quantum computing has been proposed for over 30 years. Since "Shor's algorithm"– the quantum-computer discrete-logarithm that was published in 1994, quantum computer becomes a huge threat to all the current widely used cryptographic systems, such as RSA and ECDSA. Although the development of an actual quantum computer is slow, it is still worthwhile to prevent the danger in advance. Moreover, quantum computational operations have been executed by experiments on a very small number of quantum bits. In this context, post-quantum cryptography has been drawing more and more attention. Post-quantum cryptography refers to the cryptography schemes that can resist the attack from a quantum computer. There are four major families of post-quantum cryptography schemes: Hash-based, Code-based, Lattice-based and Multivariate cryptography schemes. Each of these families has some underlying mathematical problems that are difficult to solve. However, some algorithms have been proposed to solve these problems. Therefore, it is necessary to analyze the efficiency of these best known algorithms, and find out the optimal parameter sets of each respective post-quantum algorithm for selected security levels in order to resist those attacks.

My first motivation on this project is that the concepts of quantum are always attractive to me, and I am interested in the number theory and analysis of fascinating algorithms. My second motivation is that the project is likely to make some small partial contributions to GMU's Post-Quantum Cryptography Research Group, as they have been conducting a big research project in this area. To involve this research project, I can learn the state of the art in cryptography fields, which is exciting. This project specification is based on some subtasks listed in the proposal published by Dr. Gaj and Dr. Kaps.

Tentative list of alternative solutions to explore:
- Code-base cryptography
    - Computational syndrome decoding
    - Codeword finding
    - Complete decoding
    - Goppa bounded decoding
    - Information set decoding
- Lattice-base cryptography
    - LLL (Lenstra, Lenstra, Lovasz) algorithm
    - Schnorr's algorithm
- Multivariate cryptography
    - Linearization equations
    - Lazard-Faugère System Solvers (including Gröbner Bases, XL, 4, F5)

Tentative list of evaluation criteria:

- Given a selected security level, a usable parameters set (if exists) should resist attacks from the best known algorithms implemented on both classical computers and specialized machines in the average case.
- Given a selected security level, an optimal parameters set (if exists) should resist attacks from the best known algorithms implemented on both classical computers and specialized machines in the worst case.
- For the given selected level, if there is no parameters set existing to operate successfully in the worst case, one optimal parameter sets might be the one that fulfills the first criterion most effectively.

Tentative problems to investigate:

- Code-base cryptography
    - Hardness of decoding in a random linear code
    - Exponential indistinguishability of Goppa codes
    - Code equivalence problem
- Lattice-base cryptography
    - Shortest vector problem
    - Closest vector problem
    - Shortest independent vectors problem
- Multivariate cryptography
    - Solving a set of quadratic equations over a finite field

Hypothesis

A reliable solution to the optimal parameters for a selected security level will be the one that resists attacks effectively from the best known algorithm implemented on both general-purpose computers and specialized hardware. The complexity of both traditional and quantum cryptanalytical algorithms should be evaluated to guarantee that any future standard is resistant to both. Since a quantum computer is theoretically faster than a classical computer in terms of solving some selected cryptography problems, such as factoring and discrete logarithm problems, it is useful to find all the solutions that can work on a classical computer environment first given a selected security level. Then, among those choices of parameters sets that are successfully operating on the classical computer, the parameters sets that can protect attacks against a quantum computer at a given security level are potentially to be the optimal parameters set. To ulteriorly determine the best parameters set, we should also evaluate the complexity of implementation of its cryptography scheme.

Tentative questions to answer

- What would be the average and worst case for each post-quantum cryptography scheme?
- What is the optimized computational complexity for each post-quantum cryptography scheme?
- What is the optimized computational complexity for each algorithm provided as a solution?
- Given a particular security level, what are the approaches to find the optimal parameters?
- What are the existing software and hardware implementations of each post-quantum algorithm, and what kind of parameter choices and security claims do these implementations make?
- What are the parameter choices recommended by existing standards?

Time schedule

Date	Goal
October 15	• Complete the final project specification
October 25	• Find out any parameter choices for each respective post-quantum cyptography scheme recommended by existing standards • Complete the review of basic concepts of Code-based, Lattice based and Multivariate cryptography • Complete the draft for review section of the paper
PROGRESS REPORT COMPLETE	
Nov 1	• Collect information about all parameter sets that have been proposed in the literature for Lattice-based algorithm and their claimed security levels • Complete the research on underlying problems for Lattice-based cryptography
Nov 8	• Analyze the best known algorithms to solve the underlying problems for Lattice-based cryptography • Find out any existing software and hardware implementations related to Lattice-based algorithms and their corresponding parameter choices and security claims • Choose optimal parameters of Lattice-based cryptography for selected security levels
PROGRESS REPORT COMPLETE	
Nov 15	• Collect information about all parameter sets that have been proposed in the literature for Code-based algorithm and their claimed security levels • Complete the research on underlying problems for Code-based cryptography
Nov 22	• Analyze the best known algorithms to solve the underlying problems for Code-based cryptography • Find out any existing software and hardware implementations related to Code-based algorithms and their corresponding parameter choices and security claims • Choose optimal parameters of Code-based cryptography for selected security levels
PROGRESS REPORT COMPLETE	
Nov 29	• Collect information about all parameter sets that have been proposed in the literature for Multivariate algorithm and their claimed security levels • Complete the research on underlying problems for Multivariate cryptography
Dec 6	• Analyze the best known algorithms to solve the underlying problems for Multivariate cryptography • Find out any existing software and hardware implementations related to Multivariate algorithms and their corresponding parameter choices and security claims • Choose optimal parameters of Multivariate cryptography for selected security levels
PROGRESS REPORT COMPLETE	
Dec 10	• Compare all the cryptography schemes • Analyze all the results and complete the conclusions section of the paper • Integrate all the analysis and research results to the written report
Dec 12	• Complete the initial version of the report
Dec 16	• Complete the slides and practice for the presentation
Dec 19	• Complete the final report

Tentative table of contents of my final report

Tentative list of literature

[1] D. J. Bernstein, J. Buchmann and E. Dahmen, *Post-Quantum Cryptography*, Springer-Verlag Berlin Heidelberg, 2009.

[2] D. Micciancio and O. Regev, "Lattice-Based Cryptography," New York University Courant Institute of Mathematical Sciences, 2008.

[3] I. V. Maurich and T. Güneysu, "Lightweight Code-based Cryptography: QC-MDPC McEliece Encryption on Reconfigurable Devices," *Proc. DATE 2014.*, Dresden, Germany, 2014.

[4] S. Heyse, I. Maurich and T. Güneysu, "Smaller Keys for Code-based Cryptography: QCMDPC McEliece Implementations on Embedded Devices," *Proc. CHES 2013*., 2013.

[5] N. Patterson, "The algebraic decoding of Goppa codes," in *IEEE Transactions on Information Theory.*, 1975, vol.21, pp. 203–207.

[6] D. V. Sarwate, "On the complexity of decoding Goppa codes (Corresp.)," in *IEEE Transactions on Information Theory.*, 1977, vol.23, pp. 515–516.

[7] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proceedings of the twenty-ninth annual ACM symposium on the theory of computing*, 1997, pp. 284–293.

[8] R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Laboratory DSN, 1978.

[9] A. K. Lenstra, H. W. Lenstra and L. Lovász. "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[10] C. P. Schnorr. "A hierarchy of polynomial time lattice basis reduction Algorithms," *Theoretical Computer Science*, vol. 53, pp. 201–224, 1987.