

Towards a Quantum-Resistant Future: Experiences in Post-Quantum Cryptography Education

Thomas J. Borrelli
tjbcis@rit.edu

Department of Computer Science
Rochester Institute of Technology
Rochester, New York, USA

Monika Polak
mpolak@cs.rochester.edu

Department of Computer Science
University of Rochester
Rochester, New York, USA

Sumita Mishra
sumita.mishra@rit.edu

Department of Cybersecurity
Rochester Institute of Technology
Rochester, New York, USA

Stanisław Radziszowski
spr@cs.rit.edu

Department of Computer Science
Rochester Institute of Technology
Rochester, New York, USA

ABSTRACT

With recent progress in the development of cryptographically relevant Quantum Computing (QC), significant effort is being made in the cryptography community to create viable long-term solutions against the threat of QC breaking classical public-key security schemes. The current Post-Quantum Cryptography (PQC) standardization process led by the NIST has made some selections and is about to recommend new cryptographic protocols resistant to QC. This work reports our experiences teaching a first-in-kind module-based course in Quantum-Resistant Cryptography (QRC) at two universities.

ACM Reference Format:

Thomas J. Borrelli, Sumita Mishra, Monika Polak, and Stanisław Radziszowski. 2024. Towards a Quantum-Resistant Future: Experiences in Post-Quantum Cryptography Education. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2025)*, Feb 26–Mar 01, 2024, Pittsburgh, PA, USA. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3626252.3630823>

1 INTRODUCTION

The advent of quantum computing (QC) [7, 10] is expected to significantly impact several of the widely used cryptosystems. Our current digital infrastructure relies on public-key cryptosystems based on algorithms such as the Rivest, Shamir, and Adleman (RSA) algorithm, Digital Signature Algorithm (DSA), Elliptic-Curve DSA (ECDSA), and Diffie-Hellman Key Exchange (DHKE) algorithm [8, 9]. These cryptosystems are based on mathematical problems such as integer factorization (RSA) and discrete logarithms (DHKE, DSA and ECDSA) that are difficult to solve with classical computers. However, Shor’s algorithm [11] can be used with quantum computers to solve these mathematical problems in polynomial

time, thus making these widely used cryptosystems vulnerable and insecure. This impending threat necessitates the development of cryptosystems that can withstand QC [5].

Quantum-resistant cryptography (QRC) refers to algorithms and protocols that ensure security and privacy in the presence of quantum computers. Aided by the NIST standardization process [3], the development of QRC algorithms has recently gained momentum. Educators need to start preparing computing and engineering students for cryptography in the quantum era.

Our prior work [redacted] highlighted the curricular initiative of introducing QRC in the Computer Science curriculum. This work captures our experience in delivering a QRC course at two partnering institutions. Although the course was delivered as a semester-long elective at both institutions, we adopted a module-based design to provide flexibility for ease of integration of post-quantum topics in existing cryptography courses. The idea of a module-based curricular framework has been effectively investigated for computing education [2, 6, 12]. A course module is a self-contained unit of curriculum, enabling the instructor to either insert the module(s) in existing courses without requiring course approvals, or string the modules together to create a complete course. The existence of several key design principles in QRC enables the module-based design for this complex topic. The three main types of Quantum-Resistant Cryptosystems include lattice-based, hash-based and code-based schemes [9].

Our key contributions in this work include: the design of five modules for QRC instruction and a discussion of what worked well and what to improve, and the challenges, based on classroom experience and student feedback.

2 COURSE OVERVIEW

The course was offered four times: Spring 2022, Spring 2023 and Spring 2024 at Institution 1 and once (Spring 2024) at Institution 2. The current version of the syllabus is available at [redacted]. The course comprises several modules, each focusing on a different aspect of QRC. Initially, it was designed and taught by a team of three instructors. In 2024, one of the original instructors successfully transferred the course to Institution 2. Additionally, at Institution 2, a significant portion of the students enrolled were PhD candidates (40%), contributing to a rich academic environment.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted by ACM, provided that the copies are not made for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Unpublished working draft. Not for distribution.
SIGCSE 2025, Feb 26–Mar 1, 2025, Pittsburgh, PA, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0423-9/24/03...\$15.00
<https://doi.org/10.1145/3626252.3630823>

Table 1: Topic Schedule

Module	Week	Topics
Intro – I	1	Intro/Review
Intro – I	2	NIST competition NP Theory
Quantum – II	3	Intro to Quantum Computing
Quantum – II	4	Quantum algorithms
Lattice – III	5	Lattices, Shortest vector problem
Lattice – III	6	Lattice-based cryptography
Lattice – III	7	NTRU preliminaries
–	8	Midterm Exam and NTRU
Lattice – III	9	Learning With Errors (LWE)
Hash – IV	10	Hash-based signature schemes
Code – V	11	Error correcting codes
Code – V	12	Code-based cryptography
–	13–14	Student’s presentations

We delivered the course in a module-style that facilitates students focusing on a specific topic or concept. Topics are planned for a 14 weeks long semester (see Table 1) with two 75 minute classes per week.

Student feedback was very positive on the order and selection of course topics. The authors were also quite gratified that the new version of *Understanding Cryptography* [9] also had similar topics and coverage. Overall, the students were very satisfied with the course, based on the evaluations.

Based on previous student feedback and our own experiences, we changed the order of topics (Table 1) so that the following topics were more naturally built on the previous ones. We also introduced the SageMath tool early on, which many students started utilizing in their homeworks and presentations. In fact, some of the homework questions were created with tools such as SageMath in mind, and students were urged to utilize such tools for specific steps.

One of the crucial elements of our course is the student group presentations at the end of the term. In 2024, students teams worked in groups to discuss one of the four current finalists in the NIST selection process (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON). Each team had the entire class time and were able to present each cryptosystem at a detailed level. Another positive aspect of this approach is that the presentations seamlessly built upon the material covered in the course earlier in the semester (e.g., both CRYSTALS-Kyber and CRYSTALS-Dilithium are extensions of the LWE problem covered in Week 9 (Table 1)).

3 CHALLENGES

One item that came up in the student evaluation was that there were not many ready examples or assignments that are publicly available yet. This is somewhat to be expected as the nature of this class continues to evolve and at this point it does not appear that many other schools are teaching QRC. We are attempting to provide the scaffolding for students to take the next steps towards learning about more advanced cryptosystems.

In the near future, either QC will dramatically change the landscape of computing, or there will be no cryptographically relevant QC built. Expressed in terms of concept of quantum supremacy

[1], the on-going discussion of whether quantum supremacy was already achieved or soon will be, has the potential to continue for quite a while. If the answer is yes, then QRC should be in place already. On the other hand, if a large scale implementation of Shor’s Algorithm will not be feasible in any reasonable timeline, then the classical cryptography is fine.

The pressure by the governments and industry to develop QRC is already very significant, and it grows. We must have many computer scientists, cybersecurity specialists and computer engineers who understand QRC and its intricacies to deploy it on classical non-quantum computing systems.

4 CONCLUSIONS AND FUTURE WORK

Based on the experiences captured in this paper, we believe that the QRC course, which was tested at two institutions at both undergraduate and graduate levels, is an excellent addition to existing CS curricula, and is much needed.

It is also worth noting that during the last conference [4], NIST pointed out that cryptographically relevant quantum computers may be available in 2030 and that the U.S. Government’s transition to QR will happen in years 2023-2030. This prognosis shortens the time for migration to new standards by 10 years, compared to what was predicted just a year ago. These factors should provide a compelling motivation for cryptography instructors to include QRC in both undergraduate and graduate curricula.

REFERENCES

- [1] Frank Arute, Kunal Arya, Ryan Babbush, et al. 2019. Quantum supremacy using a programmable superconducting processor. *Nature* 574 (October 2019), 505–510. <https://doi.org/10.1038/s41586-019-1666-5>
- [2] Debzani Deb, Muztaba Fuad, and Keith Irwin. 2019. A Module-based Approach to Teaching Big data and Cloud Computing Topics at CS Undergraduate Level. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (Minneapolis, MN, USA) (SIGCSE ’19). Association for Computing Machinery, New York, NY, USA, 2–8. <https://doi.org/10.1145/3287324.3287494>
- [3] National Institute for Standards and Technology (NIST). 2022. *Post-Quantum Cryptography Standardization*. NIST. Retrieved Jul 16, 2024 from <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>
- [4] National Institute for Standards and Technology (NIST). 2024. *Fifth PQC Standardization Conference*. NIST. Retrieved July 15, 2024 from <https://csrc.nist.gov/Events/2024/fifth-pqc-standardization-conference>
- [5] Kelsey Houston-Edwards. February 1, 2024. *Quantum-Proof Secrets*. Scientific American. Retrieved July 5, 2024 from <https://www.scientificamerican.com/article/tomorrows-quantum-computers-threaten-todays-secrets-heres-how-to-protect-them-2/>
- [6] Sumita Mishra, Carol J. Romanowski, Rajendra K. Raj, Trudy Howles, and Jennifer Schneider. 2013. A curricular framework for critical infrastructure protection education for engineering, technology and computing majors. , 1779-1781 pages. <https://doi.org/10.1109/FIE.2013.6685144>
- [7] Michael A. Nielsen and Isaac L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press, New York.
- [8] Christof Paar and Jan Pelzl. 2010. *Understanding Cryptography*. Springer, Berlin.
- [9] Christof Paar, Jan Pelzl, and Tim Güneysu. 2024. *Understanding Cryptography* (2 ed.). Springer, Berlin.
- [10] Eleanor G. Rieffel and Wolfgang Polak. 2000. An Introduction to Quantum Computing for Non-Physicists. arXiv:quant-ph/9809016 [quant-ph]
- [11] P.W. Shor. 1994. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE, Santa Fe, NM, USA, 124–134. <https://doi.org/10.1109/SFCS.1994.365700>
- [12] Blair Taylor and Siddharth Kaza. 2011. Security injections: modules to help students remember, understand, and apply secure coding techniques. In *Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education* (Darmstadt, Germany) (ITICSE ’11). Association for Computing Machinery, New York, NY, USA, 3–7. <https://doi.org/10.1145/1999747.1999752>