

# Modular Approach to Teaching Post-Quantum Cryptography

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 large-scale, general-purpose, fault-tolerant quantum computing (QC), significant effort is being made in the cybersecurity community to create viable long-term solutions mitigating the threat of quantum computers breaking classical public-key based security schemes. The current post-quantum cryptography (PQC) standardization process led by the National Institute of Standards and Technology (NIST) has standardized cryptographic protocols designed to be resistant to QC. PQC education is still in its early stages, with limited curricular materials available for broad distribution in an appropriate academic format. Another challenge is developing curricula for students with different levels of computing and cryptographic preparedness. The modular approach to curriculum development has been proven to be an effective method for introducing new concepts. The authors of this work have several years of experience teaching cryptography and PQC courses at two academic institutions. We introduce two types of PQC instruction modules at varying levels of complexity: *Awareness* and *Proficiency*. The suggested contents, learning outcomes, and duration for each module are presented.

## CCS Concepts

• **Security and privacy** → Cryptography.

## Keywords

post-quantum cryptography, course design, quantum-resistant cryptography, cybersecurity, modular curriculum development

## ACM Reference Format:

Thomas J. Borrelli, Sumita Mishra, Monika Polak, and Stanisław Radziszowski. 2026. Modular Approach to Teaching Post-Quantum Cryptography. In *Proceedings of the 57th ACM Technical Symposium on Computer Science Education V.2 (SIGCSE TS 2026)*, February 18–21, 2026, St. Louis, MO, USA. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3770761.3777201>



This work is licensed under a Creative Commons Attribution 4.0 International License. *SIGCSE TS 2026, St. Louis, MO, USA*

© 2026 Copyright held by the owner/author(s).  
ACM ISBN 979-8-4007-2255-4/2026/02  
<https://doi.org/10.1145/3770761.3777201>

## 1 Motivation and Modular Approach

The development of large-scale, general-purpose, fault-tolerant quantum computing is gaining momentum [10, 11]. Quantum computing is expected to impact several of the currently used public-key cryptosystems (PKC) such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve DSA (ECDSA), and Diffie-Hellman Key Exchange (DHKE), thus impacting cybersecurity in a very significant way [7]. Post-quantum cryptography (PQC) or quantum-resistant cryptography (QRC) refers to cryptographic algorithms that ensure the security and privacy of data and users in the presence of quantum computers.<sup>1</sup>

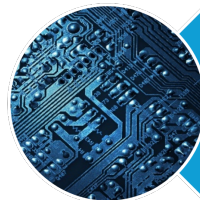
The current PQC standardization process led by NIST has already selected some new cryptographic protocols widely believed to be resistant to threats from quantum computers [4, 5]. Governments and industries around the world rely on secure encryption and authentication to protect critical infrastructure and sensitive information. As industries begin transitioning to quantum-resistant cryptographic systems, the demand for skilled professionals in PQC is growing.

Recent efforts focused on the design of a comprehensive curriculum for PQC for undergraduate and graduate computer science students [1, 2]. Others have also begun to incorporate PQC topics into cryptography courses [6]. However, there is a need to develop expertise in PQC at a broader scale.



### Awareness Modules

- A-1 Role of Public Key Cryptography
- A-2 NIST Standardization and Digital Protection
- A-3 QC Threats to Cybersecurity



### Proficiency Modules

- P-1 Role of NIST Standards in PQC
- P-2 Quantum Computing Basics
- P-3 Lattice-based PQC
- P-4 Hash-based PQC
- P-5 Code-based PQC
- P-6 Hybrid Models

<sup>1</sup>Although PQC and QRC are used interchangeably in the literature, in this work we use the more common term, PQC.

We recognize that PQC must be understood at different levels of depth depending on the audience - ranging from foundational awareness for high school students and undergraduate/graduate students with limited cryptographic preparedness, to advanced technical skills for computing students with a cryptographic background and cybersecurity professionals. A *course module* is a distinct unit of course materials, such as a laboratory or a teaching component, that can be incorporated into existing courses in the curriculum without requiring any significant changes in the course or degree program, and thus not requiring any curricular approval. The work addresses the need for PQC instruction at the undergraduate and graduate levels and the need for PQC awareness at the high school level by developing modular pedagogical approach. Such approach to instruction has been successfully used in computing and other disciplines [3, 8, 9]. We propose using course modules to embed relevant PQC material into existing courses, with the flexibility to create new courses by gluing two or more modules together. Our key contributions include the design of PQC Awareness and Proficiency modules for instruction, along with recommended student learning assessment strategies tailored to students with varying levels of computing and cybersecurity preparedness.

Based on our years of experience teaching classical and post-quantum cryptography, we propose a set of instructional modules instead of a ready-made curriculum, that we delivered at two institutions with good learning outcomes. We propose an *embeddable* set of PQC learning modules at both basic and advanced levels.

**Table 1: Learning Outcomes for PQC Awareness Modules**

No.	Learning Outcomes for Awareness
1	Students will understand the basics of currently used symmetric and asymmetric cryptosystems. (A-1, A-2)
2	Students will explain the need for encryption in day-to-day computing. (A-1, A-2)
3	Students will explain the need for standards. (A-2)
4	Students will understand the threats of quantum computing on currently used cryptosystems. (A-3)
5	Students will understand the need for PQC. (A-3)

**Table 2: Learning Outcomes for PQC Proficiency Modules**

No.	Learning Outcomes for Proficiency
1	Students will explain the need for PQC. (P-1, P-2, P-6)
2	Students will explain limitations of existing quantum computers and how they affect classical cryptography. (P-2, P-6)
3	Students will explain the principles of PQC. (P-1, P-6)
4	Students will describe & implement PQC algorithms and explain their security. (P-1, P-3, P-4, P-5)
5	Understanding the pros/cons of NIST recommendations. (P-3, P-4, P-5, P-6)

## 2 Conclusions

The background needed to truly understand post-quantum cryptography is broad and often quite challenging, even for people experienced in cryptography and mathematics. In this work, we aim to provide clear guidance on how to teach the core concepts that explain the risks of quantum computing to data security, and how PQC algorithms can help mitigate these threats. The proposed modular approach helps students to develop a strong understanding of how to protect personal data and critical infrastructure against emerging quantum threats, while facilitating the integration of these topics into existing curricula. Having separate modules makes it possible to teach only selected topics by incorporating them into existing courses.

As large-scale, fault-tolerant quantum computers become more accessible, PQC education will only grow in importance. These modules can be taught by instructors in computer science, cybersecurity, or related fields looking to incorporate PQC topics into their courses. Beyond classroom learning, engaging undergraduate and graduate students in PQC can spark research interests that lead to better testing of existing protocols, white-hat hacking efforts, and overall progress in the field.

## References

- [1] Thomas J. Borrelli, Sumita Mishra, Monika Polak, and Stanislaw Radziszowski. Towards a Quantum-Resistant Future: Experiences in Post-Quantum Cryptography Education. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education*, SIGCSE 2025. ACM, 2025. doi:10.1145/3641555.3705271.
- [2] Thomas J. Borrelli, Monika Polak, and Stanislaw Radziszowski. Designing and Delivering a Post-Quantum Cryptography Course. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, SIGCSE 2024, page 137–143, New York, NY, USA, 2024. ACM. doi:10.1145/3626252.3630823.
- [3] Debzani Deb, Muztaba Fuad, and Keith Irwin. 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*, SIGCSE '19, page 2–8, New York, NY, USA, 2019. ACM. doi:10.1145/3287324.3287494.
- [4] National Institute for Standards and Technology (NIST). Post-Quantum Cryptography Standardization, 2022. URL: <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>.
- [5] National Institute for Standards and Technology (NIST). PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates, 2022. URL: <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>.
- [6] Joshua Holden. Work in Progress: Dilithium/2 = Lithium? Post-quantum signatures for undergraduate classes. *2025 ASEE IL-IN Section Conference*, 2025. URL: <https://www.rose-hulman.edu/asee-conference/>.
- [7] Kelsey Houston-Edwards. Quantum-proof secrets, February 1, 2024. URL: <https://www.scientificamerican.com/article/tomorrows-quantum-computers-threaten-todays-secrets-heres-how-to-protect-them-2/>.
- [8] Darakhshan J. Mir, Sumita Mishra, Paul Ruvolo, Lori Pollock, and Sam Engen. How do faculty partner while teaching interdisciplinary CS+X courses: Models and experiences. *J. Comput. Sci. Coll.*, 32(6):24–33, June 2017. URL: <https://dl.acm.org/doi/10.5555/3069658.3069665>.
- [9] Sumita Mishra, Carol J. Romanowski, Rajendra K. Raj, Trudy Howles, and Jennifer Schneider. A curricular framework for critical infrastructure protection education for engineering, technology and computing majors. In *2013 IEEE Frontiers in Education Conference (FIE)*, pages 1779–1781, 2013. doi:10.1109/FIE.2013.6685144.
- [10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2000.
- [11] Eleanor G. Rieffel and Wolfgang Polak. An Introduction to Quantum Computing for Non-Physicists, 2000. arXiv:quant-ph/9809016.