Let students take the wheel: creating active learning modules for introducing quantum cryptography to STEM students

Ainaz Jamshidi, Khushdeep Kaur, Aryya Gangopadhyay, Lei Zhang
Department of Information Systems

Introduction

Quantum computing is not a promising future anymore but a coming reality. It can speed up the computations for drug design, machine learning, chemistry, etc. However, it is a double-bladed sword, which means it can also threatens existing encryption methods.

To mitigate this risk, the U.S. government and NSA urge all national security systems to migrate to **Post-Quantum Cryptography (PQC)** by 2035 [1]. As industry adapts to these changes, it is imperative to equip the next generation with the skills needed for the quantum era. Thus, we conduct this educational research to evaluate the most efficient and effective approaches to deliver PQC concepts to both undergraduate and graduate students.

Statement of the Research Problem

In this study, we assess the effectiveness of **active learning** methods, particularly **student-led seminars** [2], in delivering cutting-edge and interdisciplinary education on PQC.

Methods

We design a comparison test with and without student-led seminars for both undergraduate and graduate students. To assess the impact of active learning and student-led seminars and identify areas for improvement, we use Kahoot and surveys to evaluate learning outcomes and gather feedback from students.

Table 1. The overview of our lectures' structure

	Graduate (2.5 hours)	Undergraduate (1 hour)
Round 1	Coding + Kahoot	Coding + Kahoot
Round 2	Student-led Seminar + Coding + Kahoot	Student-led Seminar + Coding + Kahoot

Results

Table 2. The evaluation of student's performance in Kahoot quizzes (Kahoot scores, the higher the better) under the practice of student-led lectures (SLL) and faculty-led lectures (FLL) groups. The students' scores are reported as mean± standard deviation. The P-value is used to determine the statistical significance of the differences between the studied groups.

Subject		Mean ± SD	P-value
IS 471 (Undergraduate Lecture)	FLL	3540.84 ± 1006.96	0.367
	SLL	5216.84 ± 5954.70	
IS 636 (Graduate Lecture)	FLL	2759.2 ± 1159.96	0.046*
	SLL	3683.91 ± 1009.41	

*p < 0.05 is considered statistically significant.

Table 3. The evaluation of students' response time (the lower the better), measured in seconds, during Kahoot quizzes under the practice of SLL and FLL groups. The students' response time is reported as mean± standard deviation.

Subject		Mean ± SD	P-value
IS 471	FLL	4.93 ± 4.09	0.183
	SLL	3.09 ± 1.77	
IS 636	FLL	4.44 ± 5.09	0.318
	SLL	2.83 ± 1.51	

*p < 0.05 is considered statistically significant.

Table 4. P values of Chi-square test for students' course evaluations in SLL and FLL groups for undergraduate and graduate students, respectively.

Subject		Lecture pace	Amount of material presented	Difficulty of material presented	Is the topic interesting	Clarity of the presented materials by the instructor
IS 471 (Undergraduate Lecture)	FLL (RR = 100%)	0.498	1.0	0.964	1.0	0.089
	SLL (RR = 100%)					
IS 636 (Graduate Lecture)	FLL (RR = 87%)	0.641	0.320	0.319	0.162	0.709
	SLL (RR = 100%)					

*p < 0.05 is considered statistically significant. RR: Response Rate

Table 5. Semantic evaluation of students' general comments in SLL and FLL groups using DistilBERT model for semantic extraction and Chi-square test to assess sentiment differences.

Subject		Positive Comments	Negative Comments	P-value
IS 471 (Undergraduate Lecture)	FLL (RR = 92%)	10	1	0.498
	SLL (RR = 100%)	11	1	
IS 636 (Graduate Lecture)	FLL (RR = 60%)	6	3	0.638
	SLL (RR = 100%)	11	2	

*p < 0.05 is considered statistically significant. RR: Response Rate

Discussion

In this study, we propose an active learning approach for teaching both undergraduate and graduate students on PQC. We evaluate the effectiveness of our approaches in comparison tests and show that **active learning** approaches, such as **student-led seminars**, can be an effective method to deliver PQC to students with diverse backgrounds. We have extended this effort and received **NSF ExLENT Award**.

Acknowledgements

We would like to thank the Hrabowski Innovation Fund Seed Award for sponsoring this research and supporting our efforts to advance educational practices in PQC.

References

[1] White House. (2024, July). *Report on post-quantum cryptography*. The White House. https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[2] Minhas, Paras Singh, Arundhati Ghosh, and Leah Swanzy. "The effects of passive and active learning on student preference and performance in an undergraduate basic science course." *Anatomical sciences education* 5.4 (2012): 200-207.

Scan Me!