Representational Fluency in Cryptography: An Eye-Tracking Study

Wenjie Wu, Zhenzhi Xu, Yingjie Chen, Baijian Yang*

Purdue University

West Lafayette, Indiana

{wu1116,xu933,victorchen,byang}@purdue.edu

ABSTRACT

To enhance and improve cryptography instructions, this study investigated how representational fluency is related to the cognitive process through a set of eye-tracking studies and interview questions. The results showed that multiple representations were helpful for students to comprehend a concept because the different representations supported each other and provided more comprehensive information. In addition, students who are not fluent in translating one representation to another perform poorer than students who are more capable in representational fluency. While students have their own favorite representations, math representation seems dominate the outcome of their performance. This may suggest that students who will be working on the technical side of the cybersecurity should better prepare their math skills.

CCS CONCEPTS

• Security and privacy → Cryptography; • Social and professional topics → Computing education;

KEYWORDS

MEA; Representational Fluency; Eye Tracking; Cryptography Education

1 INTRODUCTION

Representational fluency means the translation among representational forms, which was defined by Lesh [1] and based on Piaget's theories of learning[2]. The purposes of this study are to investigate how students read multiple representations and whether multiple representations are helpful for them to understand a cryptography concept. To achieve these purposes, we designed a study with two cryptography concepts using multiple representations based activities. Participants were asked to learn new concepts and take quizzes on a computer. We used eye tracker to record participants' eye movements, and we also used questionnaires to understand their opinions.

In Fall 2017, 19 participants were successfully recruited from this IRB approved study. 15 of them were native English speaker. The

study took about 30 minutes for each participant. Each participant received \$20 compensation. Two cryptography topics were chosen as the testing content. The first was Zero Knowledge Proof, and the second was LZ77 Compression. Both were advanced cryptography topics and were not included in their class curriculum. All participants claimed that they were not familiar with the two topics. The concepts of the two topics were presented in three different formats: language, graph, and mathematics. Three True/False questions were designed for each topic. The experiments were conducted at a research lab. A windows laptop was used together with Tobii Pro X3-120 eye tracker. Tobii Studio was the software used to track and analyze the gaze movement data.

2 PRELIMINARY RESULTS

We found that multiple representations are helpful for students to understand cryptography concepts. In the questionnaire, most participants ($n=17$) agreed that multiple representations were helpful for them to understand the concept. The most important reasons are that multiple representations can clarify and verify each other, and different representations provided different information. We also found that students have different preferences for representations, which was reflected by their reading sequence and time use. Most students prefer to read language first and spend more time on language. A few of them ($n=3$) prefer graph representation. Only one student prefer the mathematics representation. Most participants ($n=18$) mentioned that math representation was difficult, and about a half of them were unwilling to read math equations. However, we found that the knowledge of math and the willingness to figure out math equations are of great importance. The participants who spent more time to figure out the math representation had a significantly better performance ($p=0.043$) in the quiz than participants who avoid spending time on math. Also, the only participant who prefer mathematics in our study had a much higher accuracy than other participants. In addition, we found that some participants ($n=7$) would search answers in the concept area with the same format as the question. Their average accuracy was significantly ($p=0.035$) lower than other participants. This type of behaviors suggest that they are not fluent at translating one representation form another. We can further infer that not being able to translate representations may link to poorer performance in a cryptography course.

REFERENCES

- [1] Richard Lesh, Thomas R Post, and Merlyn Behr. 1987. Representations and translations among representations in mathematics learning and problem solving. In *Problems of representations in the teaching and learning of mathematics*. Lawrence Erlbaum.
- [2] Jean Piaget. 1964. Part I: Cognitive development in children: Piaget development and learning. *Journal of research in science teaching* 2, 3 (1964), 176–186.

*This study is supported by NSF Award 1500046

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SIGITE '18, October 3–6, 2018, Fort Lauderdale, FL, USA

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5954-2/18/10.

<https://doi.org/10.1145/3241815.3241840>