# The Impacts of Representational Fluency on Cognitive Processing of Cryptography Concepts

Joe Beckman, *Purdue University* Sumra Bari, *Purdue University*
Yingjie Chen, Ph.D., *Purdue University* Melissa Dark, Ph.D., *Purdue University*
Baijian Yang, *Purdue University*

## Abstract

fMRI presents a new measurement tool for the measurement of cognitive processing. fMRI analysis has been used in neuroscience to determine where cognitive processing takes place when people are exposed to environmental stimuli and has been used to determine where students and experts process basic mathematical functions. This research sought to understand where cryptography was processed in the brain, how representational translation impacts cognitive processing, and how instruction focused on teaching representational fluency in cryptography concepts impacts cognitive processing of cryptography. Subjects were given a multiple-choice pretest, instructed during the semester in the concepts of interest to this research, given a multiple-choice post-test, then subjected to the fMRI scan while prompted to process these concepts. Results of the study show that cryptography is processed in areas indicative of the representational forms in which they were presented, as well as engaging the executive processing areas of the brain. For example, cryptography presented visually was processed in the brain in similar areas as other concepts presented visually, but also engaged the areas of the brain that organize and process complex concepts. However, the research team did not find significant results related to the cognitive processing of translating among representations, nor did we find significant changes in cognitive processing of cryptography for topics in which the focus of instruction was teaching representational fluency. Pre and post test results showed subject performed better on concepts instructed using representational fluency against concepts instructed without a focus on representational fluency, but the difference was not significant at α=.05.

## 1. Introduction

Cybersecurity is considered a top priority by the US government to defend its virtual borders. A shortage of qualified IT security professionals has long been a problem nationally and internationally [13, 15, 17]. Furthermore, the workforce shortfall is widening. According to a 2015 workforce study, 62% of respondents stated that their organizations have too few information security professionals compared to the 56% in 2013 [17].

Cybersecurity education has been and continues to be a primary focus for fortifying the workforce. The implications are many and include: the need for more students to become aware of and interested in cybersecurity; the need for a higher proportion of the students who are interested in cybersecurity to convert to a declared cybersecurity major in college; and the need to retain students in that major to boost graduation numbers so that more enter the workforce. However, quantity is not the only challenge in cybersecurity workforce development. It is equally, if not more, important that the workforce have the breadth and depth of skills needed to perform in the workforce. Cybersecurity education needs breadth that covers both technical and nontechnical skills spanning computer science, computer engineering, information systems, psychology, business and management, and many other related disciplines [3]. According to [7] we "have a shortage of the highly technically skilled people required to operate and support systems we have already deployed, we also face an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute systems after an attack" [7]. [9] and [16] also emphasize that cybersecurity experts need deep technical skills coupled with capabilities to recognize and respond to complex and emergent behavior, mastery in using abstractions and principles, assessing risk and handling uncertainty, problem-solving, and reasoning; coupled with facility in adversarial thinking.

It is a challenge to educate cybersecruity graduates to assure that they: 1) have broad and deep technical skills, 2) are facile in abstraction, problem-solving, reasoning, and adversarial thinking, and 3) able to learn and perform in this complex and emergent domain. Teaching cyberscurity requires the educator to present the abstract concept to students in a crystal clear way, and to extend the abstract concept to practice to let the students learn the knowledge in context.

Given the newness of the field, cybersecurity's pedagogical "best practices" have not yet been adequately investigated [19]. In the past 10-15 years,

articles focused on teaching practice have increased. For example, [4] discusses challenge based learning methodology to improve learning via a multidisciplinary approach which encourages students to collaborate with their peers, ask questions, develop a deeper understanding of the subject and take actions in
solving real-world challenges. [19] proposed a multifaceted hierarchical education framework to teach cybersecurity with the desired level of breath and depth [19]. [15] presents a unique teaching collaborative among 13 universities that intends to teach students agile research and development skills in cyberecurity. While there has been considerable growth in the investigation and reporting on cybersecurity teaching, we find that there is little to no substantive work on cybersecurity learning and thinking.

This work is grounded in cognitive theory and investigates students' mental models in one knowledge area of cybersecurity, i.e., cryptography. We developed Model-Eliciting Activities (MEAs), investigated students' representational fluency and the relationship of students' development of schema and changes in their cognitive processing and control when encountering cryptography concepts. In this paper, we report on students'mental models using functional magnetic resonnance imaging (fMRI) analysis of student's brain activities while solving complex security problems, as well as learning data from classroom tests.

The paper is organized as follows. Related work is reviewed in Section 2 and research methods are in Section 3. Results are presented and discussed in Section 4 and 5, respectively. Section 6 includes discussion and future work.

## 2. Previous Work

### 2.1 The Importance of Conceptual Understanding of Cryptography in Cybersecurity

Cryptography is an important subject in cybersecurity. And while cryptography is important for everyone in the field to understand, it can be an especially challenging subject to learn. The domain includes several key concepts, such as symmetric key cryptography, asymmetric key cryptography, types of ciphers, cryptanalysis and attacks, hashing, digital signatures, etc. Each of these concepts is comprised of sub concepts, which build with other sub concepts to form conceptual understanding of a key concept. Furthermore, the conceptual understanding of these concepts and sub concepts requires mathematical, language, and analytic thinking. Both breadth and depth of cryptography knowledge must be considered.

Conceptual understanding is defined as the abstract mental representation of given phenomena. Conceptual understanding occurs in the mind and the mind continuously (re)forms mental representations. The veracity of learners' conceptual understanding is the fidelity of the conceptual understanding to the external world. If conceptual understanding matters, then conceptual learning is where we need to start.

### 2.2 Cognitive Theory, Conceptual Learning and Measurement Thereof

Cognitive theories of conceptual learning are grounded in Piaget's work on logical mental frameworks (also called schemas and mental models) as structures in the brain that organize information and interactions among information. Interacting with new information, according to Piaget, modifies these schema, which is learning [12]. Conceptual learning is the acquisition of information about concepts and their interactions, and the ongoing modification about the body of conceptual knowledge as new concepts and their interactions are encountered [10].

Correct categorization involves making links to prior knowledge and so may require adjustment or correction of prior knowledge. Assimilation theory presented in [1] contrasts rote learning (temporary acquisition of disorganized or poorly understood isolated or arbitrarily related concepts) with meaningful learning (long-term acquisition of organized, interrelated concepts into existing cognitive structures). Conceptual learning is the process of identifying and correctly categorizing concepts such that they can later be used to make predictions or decisions [2, 11].

[10] has shown that providing learners with instruction in representational fluency can build conceptual understanding. Representations are the different forms in which a concept, principle, or phenomenon can be expressed and communicated. Common representations include graphic, pictorial, verbal, mathematical, and concrete. Each representation presents the phenomenon it is intended to describe in a different mode. Deep(er) understanding of the given concept requires understanding of and among various representations. Beyond comprehending representations, even deeper understanding means being fluent in shifting back and forth among the variety of relevant representations.

The concept of fluency is often associated with the ability to express oneself in the spoken and written word, and to move effortlessly (automatically) between the two representations. A person who is fluent in a language has this ability; they can translate from English to Chinese and back, and from written to spoken word and back (where written may be in English and spoken in Chinese).

The idea of fluency has been extended to other fields such as physics, chemistry, engineering, and mathematics. For example, a study by [8] on experts and novices found that physics problem solvers who are fluent in their use of different representations can easily translate between them, and can assess the usefulness of a particular representation in different situations. Similarly, [16] found that when learners develop multiple representations they are better able to transfer knowledge to new domains with increased cognitive flexibility.

Representational fluency in the STEM fields can include: a) visualizing and conceptualizing transformation processes abstractly; b) understanding systems that do not exhibit any physical manifestations of their functions; c) transforming physical sensory data to symbolic representations and vice versa; d) quantifying qualitative data, e) qualifying quantitative data; f) working with patterns; g) working with continuously changing qualities and trends; and h) transferring principles appropriately from one situation to the next [5]. Regardless what the transformation, representational fluency connotes continuous adaptation and flexibility of the conceptual model, and the ability to perform with facility, adeptness, and expertise. Representational fluency is an important aspect of deep conceptual understanding that has been shown to promote transfer of learning and the development of "expertise".

[18] advocates for the role of neuroscience in the study of mental models. The "mental frameworks" theorized by Piaget in [10] would require activity in the brain [18]. As learners' mental schema change to incorporate new information derived from experiences, brain function in the learners' brains changes. That is, learning changes the structures of the brain.

Advances in neuroscience offer researchers new tools, such as fMRI, to measure brain activity. To date, fMRI has been used in studies of cognitive processing of mathematics. [12] sought to understand what areas of the brain are involved in mathematical computation while [10] built on [12] by using fMRI to measure changes in cognitive processing after instructing students in multiplication in one and two digit numbers. These studies are examples of how neuroscience is being used to understand cognitive processing, so that later it can be applied to evaluate the impacts of instruction on learning.

Our study seeks to understand where cryptography is processed in the brain as a basis for understanding what instructional methods maximize cryptography learning in students.

# 3. Methods

### 3.1 Research Questions

This exploratory study first investigated where in the brain cryptography is processed. Second, we investigated the impact of representational form on cognitive processing. More specifically, we investigated whether cognitive processing increased when students were asked to translate cryptography concepts between representational forms (language to math, math to graphical, etc.) in comparison to cognitive processing of concepts using the same representational form (language to language, math to math, etc.). Third we investigated whether teaching cryptography using multiple representations changed how and/or where cryptography concepts were processed in the brain in comparison to instruction that was not focused on generating representational fluency.

The research team used fMRI scans of students to answer the research questions. In order to investigate impact of teaching using multiple representations, learners were taught five cryptography topics using multiple representations, and four topics were taught using single representations to convey concepts. Data gathered from learners' classroom performance were used in support of the fMRI analysis, as discussed below.

### 3.2 fMRI Component

### 3.2.1 Variables and Operationalization

### 3.2.1.1 Independent Variables

As a descriptive question, determining where cryptography concepts are processed in the brain did not have an independent variable. When considering whether translation between representational forms in the context of cryptography impacted cognitive processing, the research team defined a binary variable, Representational Translation. Either the students had to make a translation between representations, or they did not. We implemented this variable as questions that the students were asked to answer while under fMRI scanning. Students were required to make a Representational Translation when, as shown in Figure 1, Representation 1 and Representation 2 were presented in different representational forms.

Questions asked of students during fMRI were generated from material that was taught using both the representational fluency-focused instructional method, as well as the method that did not focus on the use of multiple representations in instruction. Instructional Method was defined as the independent variable in terms of our third research question regarding the impact of instruction focused on representational fluency on cognitive processing of cryptography concepts.

#### 3.2.1.2 Dependent Variables

For our research questions, the dependent variable was Cognitive Processing of Cryptography Concepts, which illustrates where in the brain and with what intensity cryptography is processed. The variable was analyzed in different ways based on the question asked, but was implemented by comparing different periods of activity in the fMRI scan based on the question being considered against brain activity measured as the subject observed the crosshair pattern following each question as shown in Figure 1.

### 3.2.2 Population and Sample

Nine out of the 12 students from a graduate-level, semester-long network security course participated in fMRI scans.

### 3.2.3 Setting

Scans were administrated at the University MRI Facility using 3T GE Discovery MR750 and a 32-channel brain array (Nova Medical). Scans consisted of a high-resolution (1mm isotropic) T1-weighted anatomical scan for registration and tissue segmentation purposes and six functional scans (TR/TE=1500/28msec; flip angle=72°; 35 slices at 3.5mm; field of view (FOV)= 24 cm and matrix= 64x64). Each functional run focused on one topic and consisted of nine yes/no matching questions (nine blocks) using three different representational forms. The functional runs were presented in random order. The subjects were able to see the questions inside the scanner through fiber optic goggles (NordicNeuroLab; Bergen, Norway) and responded with their answers through a four-button keypad. Subject's responses were directly transmitted to a computer for storage. Each block began with 15 seconds of crosshair display during which subjects were instructed to relax and focus on the display. The subjects were then presented with a question in one of the representational form for nine seconds, the ISI was of 1.5 seconds and then they were presented with another slide consisting of a question in the same or different representation form for nine seconds. After the second representation subjects then had nine seconds to decide if both the representations (R1 and R2) presented the same concept or not and answered yes or no by pressing one of the designated buttons on the keypad.

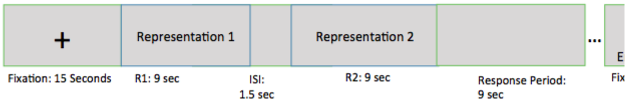


*Figure 1: The protocol of a block.*

### 3.2.4 Data Analysis

fMRI scans were processed with an in-house MATLAB code adapted from *afni_proc.py*, using AFNI and FSL. The pipeline consisted of brain extraction, outlier detection, de-spiking, slice timing correction, motion correction, alignment to the T1-weighted anatomical scan, tissue segmentation into gray matter, white matter and cerebral spinal fluid (CSF), and spatial smoothing within each tissue type (isotropic Gaussian filter with Full Width Half Maximum (FWHM) of 4mm). Anatomical and fMRI scans of all subjects were aligned to a standard template (skull stripped $1mm^3$ ICBM152) so that brain activation patterns from different subjects could be grouped together for analysis. Data were motion corrected using three motion parameters (three translational and three rotational for each x-y-z axes) and their derivatives as regressors in General Linear Model (GLM). Block regressors were used for each of the nine transitions and crosshairs in GLM.

Brain activations obtained from crosshair slides were treated as Baseline activations. Brain activations for each representation were obtained by comparing the $\boldsymbol{\beta_{Representation}}$ versus $\boldsymbol{\beta_{Baseline}}$ obtained from GLM of all subjects and all runs, using paired voxel-wise 3D t-tests followed by voxel-wise False Discovery Rate (FDR) correction. Adjacent voxels with $p_{FDR}$<0.05 and cluster size greater than 100 voxels were considered as significant brain activations against the baseline and are as shown in the figures.

fMRI data gathered was analyzed differently for dependent variable, Cognitive Processing of Cryptography Concepts, based on which question was being investigated. When investigating where in the brain cryptography concepts are processed, activation patterns were gathered during the presentation of the first representation of each question. Activation present during the resting period following the question (noted as the second crosshair pattern in Figure 1) was subtracted from activation patterns noted during Representation 1. Data were separated based on the representation presented in Representation 1 in Figure 1, then the data were aggregated for all student participants (n=9) by representation n=18 per student), for a total of 162 individual data points per representation.

Evaluating whether translation between representations within questions impacted cognitive processing of cryptography, the period of time during the presentation of Representation 2 and the Response Period (as shown in Figure 1) was used to gather cognitive processing data and activation noted during the second crosshair pattern was subtracted from the gathered cognitive processing data. Data were grouped by the independent variable Representational Translation and aggregated for all students. In this case, three questions per topic did not require Representational Translation. So, the total number of data points for non-translation was n=18. Six per topic did require translation for a total translation n=36. Each student answered questions on the same six topics.

Finally, cognitive processing data were gathered and analyzed by the Instructional Method independent variable. In this case, the same data gathering process was used as for analysis of Representational Translation, except that the data were grouped by the instructional method in which the topic was taught. In terms of this comparison, each student was given questions from three topics that were taught using the treatment instructional method that focused on representational fluency and three topics that were taught with the control instructional methodology. This analysis consisted of nine questions over three topics aggregated for nine students, or n=243. However, the research team delimited these comparisons by comparing only questions with the same structure to each other. For example, the fMRI results for all questions on a topic that required the subject to translate a concept from language to math (or vice versa) were aggregated to determine cognitive processing of cryptography concepts during that translation process. Therefore, the effective n=27 (three translations per topic, nine subjects in total) treatment data points and n=54 control data points.

### 3.3. Classroom Component

#### 3.3.1 Research Question

Classroom data were used only in support of analysis of the fMRI results produced from this study; therefore, the research questions are the same as those discussed as part of the fMRI component earlier.

#### 3.3.2 Variables and Operationalization

#### 3.3.2.1 Independent Variable

The independent variable in this experiment was the method of instruction. Instructional methods were assigned by the researchers to the following topics taught in class: Zero-Knowledge Proof (ZKP), Pohlig-Hellman Ciphers (PH), Rivest Shamir Adleman Cryptosystems (RSA), Digital Cash (DC), and Public Key Infrastructure (PKI). All other content taught during the semester was taught using two representational forms not focused on representational fluency.

#### 3.3.2.2 Dependent Variable

The dependent variable was students' pre to post-test learning gain. Learning gain was determined by normalizing students' points scored on the pre and post- tests into a percentage interval variable, subtracting the pretest score from the post-test score, and averaging the differences of the twelve students for each question. Pre to post-test score differences were aggregated by instructional method and compared using a t-test.

#### 3.3.3 Populations and Samples

Twelve of twelve students from a graduate-level, advanced network security course offered in the Spring 2017 semester at a large university in the Midwestern United States consented to allow their pre and post-test exam scores to be used in this research.

#### 3.3.4 Setting

Data for this experiment were gathered in one section of a graduate-level advanced networking course at a large public university in the Midwestern United States. The course was not a required course. The control topics were taught using a combination of lectures delivered by projecting slides containing individual representational forms (language, graphics, or math) to deliver concepts to learners. Instruction of the treatment topics taught: Zero-Knowledge Proof (ZKP), Pohlig-Hellman Ciphers (PH), Rivest Shamir Adleman Cryptosystems (RSA), Digital Cash (DC), and Public Key Infrastructure (PKI) using activities consisting of multiple representations and focused on representational fluency. No other aspects of the instruction or scored evaluation of the students in the classroom differed between the control and treatment groups. Student performance was evaluated using a pretest and post-test, which also served as the students' final exam.

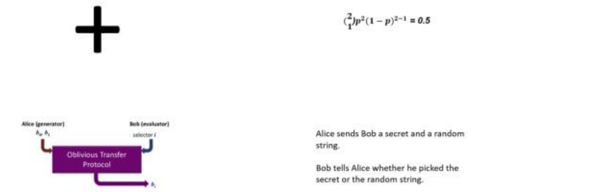
#### 3.3.2 Population

The population from which subjects were drawn for this experiment consisted of all students enrolled in the University's graduate advanced network security course offered by the college of Technology in the Spring of 2017. Enrolled students were predominantly 18-24-year-old. Because the experiment required subjects to consent to the use of their scores on course homework, projects, and exams, those students who gave their signed consent to release their scores to the research team comprised the sample in each class section. All 12 students in the course consented to allow use of their classroom scores in this study.

## 4. Results

### 4.1 Brain Location: Cognitive Processing of Cryptography

In order to answer the question, "Where in the brain are cryptography concepts processed?", the research team analyzed blood oxygen level data (BOLD) of participants, representing brain activity, taken during the fMRI while the participants were processing cryptography questions. Measurement of blood flow to the bran, the measurement on which fMRI is based, serves as a proxy for changes in brain activity. Increased blood flow to an area of the brain indicates increased brain activity, cognitive processing, where decreased activity is signaled by reduced blood flow to areas of the brain. In this research, questions were presented using graphical, language, and mathematics representations as shown in Figure 1, which generated distinct patterns of brain activation, so we address the research question by representation.


$(\binom{2}{1})p^2(1-p)^{2-1} = 0.5$

Alice sends Bob a secret and a random string.

Bob tells Alice whether he picked the secret or the random string.

Figure 1: Representations used in fMRI questions (clockwise top to bottom): crosshair pattern, mathematic, language, graphical

This analysis used brain activation detected during the presentation of the first of two slides in each question, and the resting crosshair pattern following the question as illustrated in Figure 2.

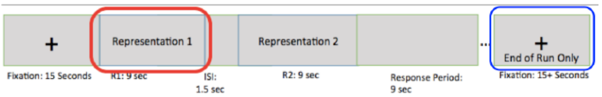


Figure 2: Activation Comparisons by Representation

The research team aggregated the BOLD signal data for all questions by the type of the first representation, that is math, graphical, or language, across the nine student participants. Cryptography concepts presented using a mathematical representation with mathemtics produced BOLD activation patterns shown in Figure 3.

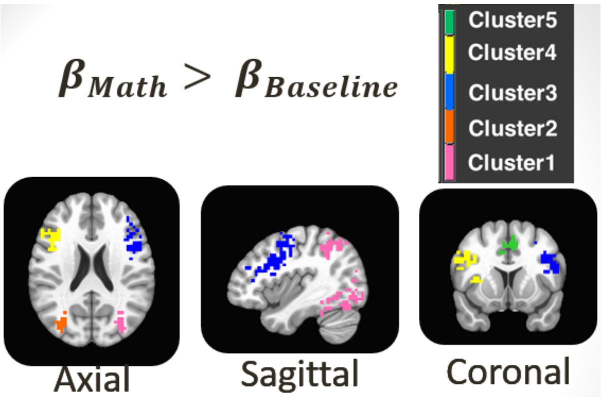


Figure 3: Brain Activation of Cryptography Concepts Presented using Matematical Representations

Five clusters of activation were noted at a significance level of α=0.05. Corresponding Broadmann Areas and usages are listed in Table 1 below.

| Cluster | Broadmann Area | Gyrus | Usage |
|---|---|---|---|
| 1 | Left 39 | Left Middle Temporal | Accessing word meaning |
| 2 | Right 39 | Right Middle Temporal | Accessing word meaning |
| 3 | Left 9 | Left Inferior Frontal | Representation of numbers |
| 4 | Right 44 | Right Inferior Frontal | Executive processing |
| 5 | Left 9 | Left Medial Frontal | Executive processing |

Table 1: Math Processing Areas of Activation

Cryptography concepts presented using English language stimuli activated five areas of the brain, which are shown in Figure 4 and detailed in Table 2.

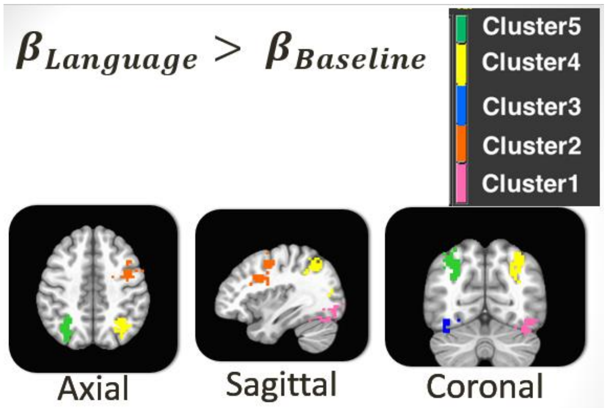


Figure 4: Brain Activation of Cryptography Concepts Presented using English Language Representations

Five clusters of activation were noted at a significance level of α=0.05. Corresponding Broadmann Areas and usages are listed in Table 2 below.

| Cluster | Broadmann Area | Gyrus | Usage |
|---|---|---|---|
| 1 | Left 17 | Left Inferior Occipital | Visual Processing |
| 2 | Left 44 | Left Inferior Frontal | Executive Language Processing |
| 3 | Right 37 | Right Lingual Gyrus | Visual Processing |
| 4 | Left 3 | Left Inferior Parietal | Somatosensory Processing |
| 5 | Right 1,2 | Right Superior Parietal | Somatosensory Processing |

Table 2: Language Processing Areas of Activation

Graphical representations of cryptography concepts produced two areas of brain activation. These areas are shown in Figure 5 and decribed in Table 3 below.

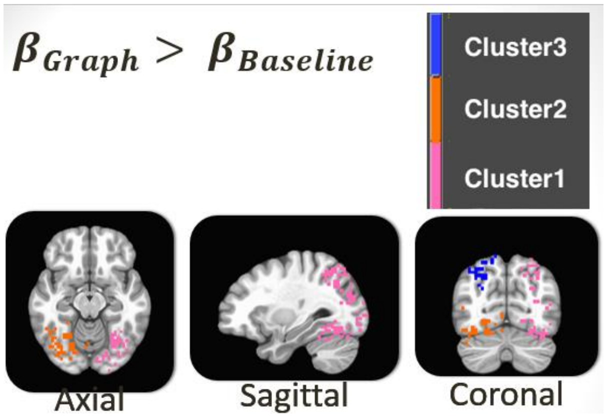


Figure 5: Brain Activation of Cryptography Concepts Presented using Graphical Representations

Three clusters of activation were noted at a significance level of α=0.05. Corresponding Broadmann Areas and usages are listed in Table 3 below.

| Cluster | Broadmann Area | Gyrus | Usage |
|---|---|---|---|
| 1 | Left 30 | Left Middle Occipital | Visual Processing |
| 2 | Right 7 | Right Superior Parietal | Facial Stimuli |
| 3 | Right 37 | Right Lingual | Visual and Letter Processing |

Table 3: Graphica Processing Areas of Activation

### 4.2 Brain Activation in Cryptography Processing During Translation of Representational Forms

The research team compared students' cognitive processing on cryptography questions in which they were forced to make a translation between representational forms in order to answer the question against cognitive processing activity on questions in which no such translation was necessary. We had hypothesized, based on Thomas, Wilson, Corballis, Lim, and Yoon (2010), that questions requiring such a translation would produce more intense cognitive activity in similar brain regions than those that did not require representational translation. Our comparison of brain activation in this study did not support this hypothesis. Only brain activation patterns in the Language to Language questions, the Language to Math, and the Math to Graphical analyses showed significant activation beyond baseline. Figures 6, 7, and 8, respectively, show the brain areas of significant activation in this comparison.

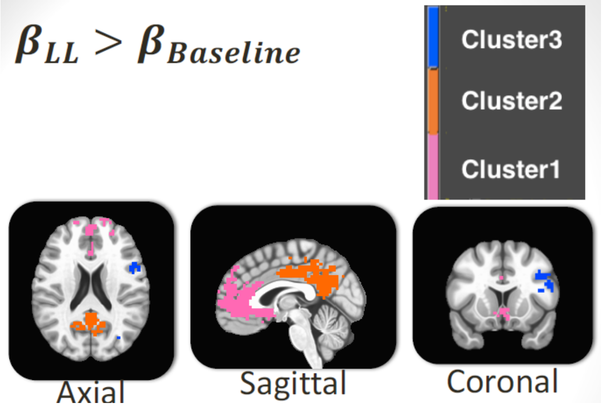


Figure 6: Brain Activation for Language to Language Comparisons of Cryptography Concepts

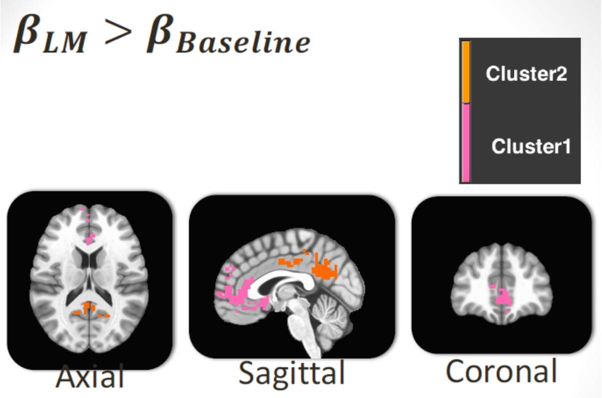


Figure 7: Brain Activation for Language to Math Comparisons of Cryptography Concepts

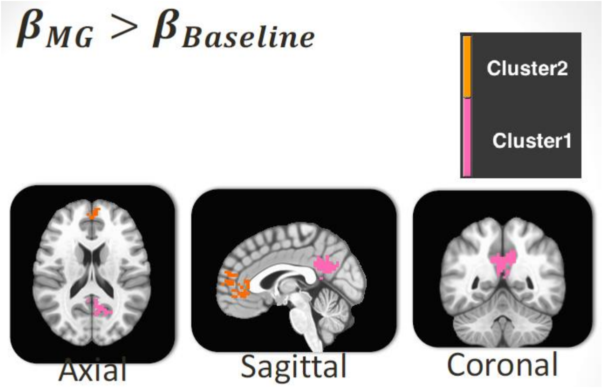


Figure 8: Brain Activation for Math to Graphical Comparisons of Cryptography Concepts

### 4.3 Cryptography Learning by Instructional Method

In support of the fMRI brain activation data comparison between topics instructed using MEA and focused on representational fluency and those taught using traditional lecture-based instruction, the research team also compared learning gains using the course pre-test and post-test. We hypothesized that teaching cryptography concepts using representational fluency would produce different patterns of cognitive activation compared against topics taught without a focus on representational fluency. For this comparison, pre and post-test scores were aggregated from the twelve students in the class, and across all topics that were instructed using MEA and compared to those that were instructed using the traditional method of instruction not focused on representational fluency. This analysis showed an average learning gain of 10.83% on topics instructed using MEA and 3.56% on topics instructed using methods not focused on representational fluency. These learning gains are not significant at $\alpha$=0.05 (t=1.19, p=0.24). Comparing pre-test scores based on instructional method indicated a similar level of knowledge, on average, of material that would be instructed using MEA ($\mu$: 0.57, $\sigma$: 0.23) versus topics that would be instructed using other methods ($\mu$: 0.57, $\sigma$: 0.25)

## 5. Discussion and Conclusion

The purpose of this work is to design and evaluate if and how representational fluencies are related to cognitive learning. The team specifically examined the following research questions:

1) Where does the cryptography occur in the brain?

The fMRI scan analyses showed that cryptography concepts, if represented using different formats, i.e. language, graph, and math notations, activate different parts of the brain. The results were statistically significant, even when the sample size was merely 9. The activation maps also echo similar distributions as the previous study on math and physics concepts. This may suggest that from cognitive perspective, cryptography is fundamentally not very different from math and physics. Or put it differently, brain activations are directly related to the form of the representations rather than the underlying complex cryptography concepts or algorithms.

2) Where do the transitions of different representations occur in the brain?

Among nine possible representation fluencies, the research team discovered that three of them are statistically significant. They are from language to language, from language to math, and from math to graph. This suggest for the group of students that participated fMRI scans, longer and stronger brain activities were recorded when students were asked to translate the same concept from language to language, from language to math, and from math to graph. Interestingly, the translation from math to language and the translation from graph to math were not shown the same statistical significance. If the research results are reliable, it can be inferred that representation translations are uni-directional. That is the brain reacts differently when translating language to math than translating math to language. If we further assume stronger or longer brain activations are related to more difficult tasks, then it may suggest the three transitions that showed statistically significance might be the ones that students having trouble with.

3) How does representational fluency impact the classroom learning results?

The classroom learning results showed an average of 10.38% gains between pretests and posttests when the instructional methods were delivered using MEAs that were specifically designed to train students on the representational fluencies. In contrast, the gains were merely 3.56% when conventional instructional methods were adopted in the classroom. However, the p value of the paired t-test was 0.26: too large for the research team to declare the findings are statistically significant. There were two major reasons accounted for this "non-significance". The first was due to small sample size of 12. They second was the very high average pretest scores. More specifically, students averaged 56.8% ($\sigma$ = 23.4%) on topics to be instructed using MEA and 57.2% ($\sigma$ = 25.3%) on topics to be taught not using MEA. Students participated in this study were all graduate students and may possess strong prior knowledge of cryptography. If high levels of prior knowledge contributed to the relatively high pretest scores, the large standard deviations in both pre and posttest scores indicate that very different levels of prior knowledge were present among the students (posttest $\sigma$, MEA: 23.8%, non-MEA: 24.2%). Further study is needed with a bigger sample size, and preferably at undergraduate level to fully understand the impact the representational fluencies on the classroom learning results. Adding more questions to the pre and posttests at each Bloom level of learning would add clarity to how instruction impacted understanding of the cryptography concepts being researched.

## 6. Future Work

The results of this study present several avenues for future research. Given the limitations of this experiment, future work could validate our findings regarding where cryptography concepts are processed in the brain. Our failure to find significant results relating to cognitive processing activation during representational translations or cognitive processing related to representational fluency leave these areas open for additional research. In particular, it is possible that different types of classroom instruction or classroom measures of that instruction could also be performed in order to evaluate the effects on cognitive processing and learning. With a cognitive processing baseline set in this work for processing of cryptography, many aspects of learning can be compared against these baselines toward the goal of increasing cryptography learning in information security students.

## References

[1] Ausubel, D. P., Novak, J. D., & Hanesian, H. (1978). Educational Psychology: A Cognitive View, 2nd edn (New York: Holt, Rinehart and Winston). *Reprinted (1986). New York: Warbel and Peck.*

[2] Brown, A. L., Cocking, R. R., & Bransford, J. D. (2000). How people learn. JD Bransford (Ed.).

[3] Burley, D. L. (2014). Cybersecurity education, part 1. *ACM Inroads*, *5*(1), 41–41.

[4] Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the 2011 International Conference on Security & Management* (Vol. 1).

[5] Dark, M. J. (2003). A models and modeling perspective on skills for the high performance workplace. Beyond constructivism: Models and modeling perspectives on mathematics problem solving, learning, and teaching, 279-293.

[6] Delazer, M., Domahs, F., Bartha, L., Brenneis, C., Lochy, A., Trieb, T., & Benke, T. (2003). Learning complex arithmetic—an fMRI study. Cognitive Brain Research, 18(1), 76-88.

[7] Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. CSIS.

[8] Hsu, L., Brewe, E., Foster, T. M., & Harper, K. A. (2004). Resource letter RPS-1: Research in problem solving. American Journal of Physics, 72(9), 1147-1156.

[9] McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014). Toward curricular guidelines for cybersecurity. In *Proceedings of the 45th ACM technical symposium on Computer science education* (pp. 81–82). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2538990

[10] Moore, T. J., Miller, R. L., Lesh, R. A., Stohlmann, M. S., & Kim, Y. R. (2013). Modeling in engineering: The role of representational fluency in students' conceptual understanding. *Journal of Engineering Education*, *102*(1), 141-178.

[11] Özdemir, G., & Clark, D. B. (2007). An Overview of Concep-tual Change Theories. Eurasia Journal of Mathematics, Sci-ence & Technology Education, 3(4).

[12] Piaget, J. (1964). Part I: Cognitive development in children: Piaget development and learning. *Journal of research in science teaching, 2*(3), 176-186.

[13] Pierce, A. O. (2016). *Exploring the Cybersecurity Hiring Gap*. Walden University. Retrieved from http://scholarworks.waldenu.edu/dissertations/3198

[14] Rickard, T. C., Romero, S. G., Basso, G., Wharton, C., Flitman, S., & Grafman, J. (2000). The calculating brain: an fMRI study. Neuropsychologia, 38(3), 325-335.

[15] Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113–122). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2047628

[16] Schneider, F. B. (2013). Cybersecurity education in universities. IEEE Security & Privacy, 11(4), 3-4.

[15] Sherman, A., Dark, M., Chan, A., Chong, R., Morris, T., Oliva, L., ... & Wetzel, S. (2017). The INSuRE Project: CAE-Rs Collaborate to Engage Students in Cybersecurity Research. *arXiv preprint arXiv:1703.08859*.

[16] Spiro, R. J. ea (1992). Cognitive flexibility, constructivism and hypertext: Random access instruction for advanced knowledge acquisition in ill-structured domains. Duffy, Thomas M. und David H. Jonassen (Hg.): Constructivism and the Technology of Instruction: A Conversation. Hillsdale, NJ, 57-75.

[17] Suby, M., & Frank Dickson. (2015). The 2015 (ISC) 2 Global Information Security Workforce Study. *Frost & Sullivan in Partnership with Booz Allen Hamilton for ISC2*.

[18] Szűcs, D., & Goswami, U. (2007). Educational neuroscience: Defining a new discipline for the study of mental representations. *Mind, Brain, and Education*, *1*(3), 114-127.

[19] Wei, W., Mann, A., Sha, K., & Yang, T. A. (2016). Design and implementation of a multi-facet hierarchical cybersecurity education framework. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 273–278). https://doi.org/10.1109/ISI.2016.7745488