Cognitive Processing of Cryptography Concepts: An fMRI Study

Mr. Joseph William Beckman, Purdue University

Joseph Beckman is a Ph.D. student in information security at Purdue University researching cognitive processing as it applies to learning in information security.

Ms. Melissa Jane Dark, Purdue University

Melissa Dark is W.C. Furnas Professor of Technology in the College of Technology at Purdue University. Her work is in cybersecurity teaching, learning and thinking.

Mr. Pratik Kashyap, Purdue University

Pratik Kashyap is a PhD student in Electrical Engineering at Purdue University whose field of research is in biomedical signal and image processing.

Ms. Sumra Bari, Purdue University, School of Electrical and Computer Engineering

Sumra Bari received the Bachelor's degree in Electrical Engineering in 2011 from the University of Engineering and Technology, Lahore, Pakistan and the Master's degree in 2015 from Purdue University, West Lafayette, IN where she is currently working towards the Ph.D. degree in School of Electrical and Computer Engineering. Her research interests include functional neuroimaging, statistical biomedical imaging and signal processing and model based image processing.

Prof. Samuel S. Wagstaff Jr, Purdue University

Sam Wagstaff is a computer science professor at Purdue University. He works in cryptography and computational number theory. He has published four books and more than sixty papers. He taught the cryptography class on which some of the research of this article is based.

Dr. Yingjie Chen, Purdue Polytechnic Institute

Dr. Yingjie Chen is an assistant professor in the Department of Computer Graphics Technology of Purdue University. He received his Ph.D. degree in the areas of human-computer interaction, information visualization, and visual analytics from the School of Interaction Arts and Technology at Simon Fraser University (SFU) in Canada. He earned the Bachelor degree of Engineering from the Tsinghua University in China, and a Master of Science degree in Information Technology from SFU. His research covers interdisciplinary domains of information visualization, visual analytics, digital media, and human computer interaction. He seeks to design, model, and construct new forms of interaction in visualization and system design, by which the system can minimize its influence on design and analysis, and become a true free extension of human's brain and hand.

Dr. Baijian Yang, Purdue Polytechnic Institute

Dr. Yang is current an Associate Professor at Department of Computer and Information Technology, Purdue University

Cognitive Processing of Cryptography Concepts: An fMRI Study

Joseph Beckman, Melissa Dark, Ph.D.,
Pratik Kashyap, Sumra Bari,
Yingjie Victor Chen, Ph.D.,
Samuel Wagstaff, Ph.D., Justin Yang, Ph.D.

Purdue University

Abstract

This study investigated the effects of using Model Eliciting Activities that build representational fluency on the cognitive processing of selected cryptography concepts. The study used an experimental design where in the control group the cryptography concepts were taught to 5 participants using two representational forms (language and mathematics) and in the treatment group the same concepts were taught to 5 participant using four representational forms (language, mathematics, graphic and concrete). Cognitive processing was measured using Functional Magnetic Resonance Imaging (fMRI) to determine where in the brain cryptography concepts are processed and whether the use of MEAs focused on representational fluency impacted cognitive processing of cryptography concepts. fMRI image data were gathered from five volunteers by presenting multiple choice questions to the students visually and recording their responses while they were undergoing fMRI scanning. fMRI image analysis from the post-course scans showed common areas of brain activation among the ten fMRI participants that differed based on whether the questions were presented using language, math, or graphical representational forms. This paper discusses the differences in brain activation patterns resulting from each representation, as well as a direction for future work measuring cognitive processing of cryptography concepts in multiple representational forms.

Introduction

Producing a highly skilled IT security workforce is vital to protect the interests of the US and her allies. Recent reports (Rowe, 2011; Suby, 2013) indicate a shortage of qualified cybersecurity professionals exists, even though it is one of the highest paid technology jobs and has been enjoying double digits job growth in the recent years. McGettrick (2011) and Schneider (2013) have emphasized that cybersecurity experts need deep technical skills coupled with capabilities to recognize and respond to complex and emergent behavior, as well as a "security mindset", which includes mastery in using abstractions and principles, assessing risk and handling uncertainty, problem-solving, and reasoning; coupled with facility in adversarial thinking. However, producing graduates with deep technical skills who are facile in abstraction, problem solving, reasoning, and adversarial thinking and able to learn and perform in this highly complex and emergent domain is not easy. Grounded in cognitive theory, this project developed model-eliciting activities (MEAs) for cryptography concepts using and translating among multiple representations, and investigated students' cognitive processing. Our investigation of learning in cryptography introduced the use of fMRI as a measure of cognitive processing of cryptography concepts.

Previous Work

Cognitive theory is the study of mental processes. Cognition refers to conscious mental activities and more specifically to the activities of thinking, remembering, understanding, learning, reasoning, problem solving, decision-making, and creating. These cognitive activities both use existing knowledge and generate new knowledge. One area of study in cognitive science is cognitive control, also known as executive function and supervisory attentional system. Cognitive control refers to the regulation, management, and control of mental processes. The cognitive control system, located in the prefrontal areas of the frontal lobe (Alvarez, Emory

and Emory, 2006) has been found to be associated with verbal fluency, design fluency, cognitive flexibility (the mental ability to think about multiple concepts), planning, response inhibition, handling novel situations, working memory, reasoning, problem solving, and abstract thinking (Alvarez, Emory and Emory 2006; Lezak, Howieson, and Loring, 2004; Monsell, 2003). Norman and Shallice (1980) outline five types of situations where routine activation of behavior would not be sufficient for optimal performance:

1. Those that involve planning or decision making
2. Those that involve error correction or troubleshooting
3. Situations where responses are not well-rehearsed or contain novel sequences of actions
4. Dangerous or technically difficult situations
5. Situations that require the overcoming of a strong habitual response or resisting temptation.

Cognitive control is important for cybersecurity professionals because, more often than not, they are planning, decision making, trouble shooting, correcting errors, and dealing with novel and technically difficult situations. Cognitive control system abilities develop and mature over time as the brain continues to mature and develop connections, often well into adulthood. The cognitive control system is shaped by physical changes in the brain, and molded by experiences in and out of the classroom (De Luca, Leventer, and Richard, 2008; Anderson, 2002). If cognitive control is important for cybersecurity professionals, the instructional experiences that enhance cognitive control are important for cybersecurity education.

An area of cognitive science that links to education is cognitive load theory (CLT). Cognitive load theory focuses on the amount and nature of information and the interactions that

must be processed for meaningful learning to occur. According to cognitive load theory, people develop schemas (Sweller, 1988) in order to handle the processing of new information. Schemas are especially critical for handling complex information and technically challenging materials. “Schemas act as a central executive, organizing information or knowledge that needs to be processed into working memory” (Merrienboer and Sweller, 2005, p. 149); in other words, schemas are part of the cognitive control system.

Schemas (also called mental models) have described as: 1) mental structures of preconceived ideas, 2) a framework representing some aspect of the world, or 3) a system of perceiving and organizing new information. As a representational system, a schema is composed of multiple representations. We can think of representations as the different forms in which a concept, principle, or problem can be expressed and communicated, such as graphically, pictorially, verbally, mathematically, by example, etc. Each representation presents a different mode of the system it is intended to describe. Deep(er) understanding of a given concept (conceptual system) 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 Hsu, Brewe, Foster, and Harper (2004) 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, Spiro (1992) found that when learners develop multiple representations they are better able to transfer knowledge to new domains with increased cognitive flexibility (Spiro, 1992). 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 (Dark, 2003). Regardless what the transformation, representational fluency connotes continuous adaptation and dynamism, 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".

To recap, the relationship between the cognitive control system and learning is co-adaptive; the cognitive control system shapes learning, and learning stimulates and hones the cognitive control system. And schemas are critical to this co-adaptation. Schemas shape how and what new information is assimilated. Schemas influence how and what stored knowledge will be retrieved and used. Developing representational fluency contributes to the development of robust schema. This team has developed and used educational materials aimed at building learners' representational fluency and schema in cryptography.

Using fMRI, this study identifies active areas of cognitive processing when learners engage in cryptography concepts of various representational forms. When neurons in a certain

areas of the brain become active, local blood flow to those brain regions will increase, which are captured by fMRI. Thus we are able to find out which part of brain is actively charged when students encounter cryptography concepts. By knowing which areas of the brain are active when processing cryptography concepts, we can later test the effects of various methods of instruction on cognitive processing. We hypothesize that over time we will demonstrate that MEAs elicit executive control functioning.

Methods and Procedures

The questions to be answered in this study are 1) where does cognitive processing of different cryptography representations occur in the brain, and 2) does the location change based on method of instruction? This investigation of learning in cryptography introduced the use of fMRI as a measure of cognitive processing of cryptography concepts. The study was set in one undergraduate computer science class entitled "Introduction to Cryptography" that was split into two separate class sections. Both sections were taught the same topics by the same instructor. The control section was taught using a lecture format with slides containing text and math formulae. In the treatment section, concepts necessary to understand: Simple Ciphers, Diffie-Hellman Key Exchange, Oblivious Transfer, Zero Knowledge Proof, and Digital Cash were taught using text, math, graphical, and example representations in MEA instruction focused on building representational fluency. Five subjects from each class section participated in an fMRI scan while responding to cryptography questions that required conceptual understanding of the five topics using multiple representations. Using this design, our team sought to aggregate data from all ten fMRI participants following classroom learning in order to determine where in the brain cryptography concepts are processed, if common areas of processing exist, and compare differences in fMRI image data from the control and treatment groups (five participants from

each section) in order to measure the impact on student learning of instruction delivered using MEAs focused on representational fluency compared to instruction focused on math-based lecture.

Study Variables

The variable being studied is brain activation during cognitive processing of cryptography concepts. Increases in blood oxygen levels in subjects' brains as they answered the questions were used to represent increases in cognitive processing activity. In order to stimulate cognitive processing of the concepts in question, subjects were presented visually with cryptography questions related to Simple Ciphers, Diffie-Hellman Key Exchange, Oblivious Transfer, Zero Knowledge Proof, and Digital Cash while being scanned in the MRI machine, and instructed to answer the questions using a four-button response box given to the them prior to the start of the scan. The cryptography questions delivered during the scan served to stimulate cognitive response to cryptography concepts in support of our goal of determining where cryptography concepts are processed in the brain and, through the selection of these particular cryptography questions, by presenting content that students learned under different instructional methods. Because representational fluency has been determined to be a proxy for deep conceptual understanding and because the instructional method used in the treatment focused on teaching representational fluency, questions presented during the fMRI scans were presented using multiple representational forms. Examples of the different representational forms as

presented during the scans are shown in

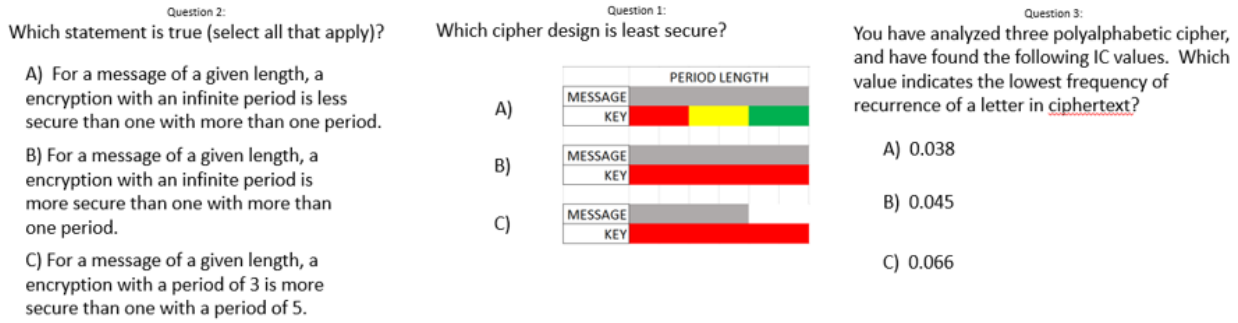

Figure 1: Examples of language, graphical, and mathematical representations of cryptography questions.

Population and Samples

The population of this study was drawn from all students enrolled in the university's undergraduate introductory cryptography course offered through the Computer Science department in the Fall semester, 2016. The course was required for graduation only of students seeking a Bachelor's Degree in Computer Science within the Security track. Enrolled students were predominantly male in the morning section, and exclusively male in the afternoon section. Students were predominantly 18-24-years old in both sections. Five members from each classroom section were sampled from the class population for the study's fMRI component. The research team solicited volunteers to participate in this component, then screened out volunteers who were not in the 18-24-year-old age range. None of the female students volunteered to participate.

Settings

Scans were administered at a facility and using a 3-Tesla General Electric MRI machine with a 16-channel receive-only head coil. Each subject was briefed about duration and format of the scans, and how to operate the equipment that they were asked to use. The subject was

then fitted with visual display goggles by placing them over subject's eyes and adjusting until the subject reported seeing one clear image through the goggles. The subject's head was landmarked in the MRI machine before advancing the subject into the machine for scanning.

Scans consisted of a localizer scan, which configured the machine to scan the specific subject's head, an anatomical scan (1mm isotropic T1 weighted), which created a detailed image of the subject's head and was used to map areas of the brain that were active during particular portions of the scan, and a series of nine functional scans (task-based echo-planar images), which scanned the subject while he responded to cryptography questions about the five topics previously discussed. Each functional scan run focused on a single cryptographic concept, contained questions using different representational forms, and were four minutes in duration. Runs began with a one-minute display of a crosshair, during which subjects were to relax and focus on the crosshair. Four questions followed about one of the five selected cryptography topics, each of which the subject was given 30 seconds to answer using a four-button keypad that he held during the scan. Subjects' responses were transmitted directly to a computer for storage. Each run ended with the same one-minute display of the crosshair pattern that started the run.

Some of the questions presented during the scan were presented with one correct answer choice, while for other questions, multiple correct answers were shown as choices. Subjects were asked to choose all responses to a question that they believed to be correct, and were instructed that some questions may have more than one correct answer choice. By giving subjects the option to select multiple answers, the research team sought to reduce subjects' ability to deduce answers by eliminating answer choices based on the strength of their understanding of a particular representational form. If a subject selected more than one answer to a question, he was asked over the MRI's intercom system immediately following the run if he

intended to change his initial answer, if he had inadvertently hit a button, or if he believed that all of the choices he selected were correct. Appropriate adjustments were made to participant responses based on subjects' feedback.

Data Analysis

fMRI scans were pre-processed using a standard pipeline consisting of brain extraction, de-spiking, slice timing correction, volume registration, alignment to the T1 weighted anatomical, tissue segmentation into gray matter, white matter and cerebral spinal fluid (CSF), and spatial smoothing (isotropic Gaussian filter with Full Width Half Maximum (FWHM) of 4mm). These processes interpreted the numeric data that measured the brain activation response, analyzed it to produce a regression model, and translate the numeric data into color-coded levels that appear on the brain images in the figures below. Anatomical and fMRI scans of all subjects were warped to a standard template (skull stripped $1mm^3$ ICBM152) so that brain activation patterns from the different individual subjects could be grouped together for analysis. fMRI data were motion corrected by using six motion parameters (3 translational and 3 rotational for each x-y-z axes) and their derivatives. Significant brain region activations for each representational form in which questions were presented were obtained by linear regression of the data against a block design. These activations were then averaged across all nine runs and across each representation type for each subject. Paired voxel-wise 3D t-tests of the ten subjects were conducted between baseline activations and activations during processing of the questions. The brain regions activations with a p-value < 0.05 (corrected for false positive cluster detection) were considered significantly different activations among the two scans.

Results

The research team analyzed the image data produced during the study by aggregating images from the five treatment subjects and comparing it to aggregate of the images from the

control group in order to investigate cognitive processing in terms of the classroom instructional method used, and by aggregating images from all ten fMRI participants in order to determine where in the brain cryptography concepts are processed. No statistically significant results at $\alpha=0.05$ were noted when comparing images between the treatment and control groups. Thus, we were unsuccessful in noting any differences in cognitive processing that would have provided evidence of a difference in cognitive processing of cryptography concepts based on the instructional method used to deliver the cryptography concepts. Analysis of the aggregate image data from all ten fMRI subjects did provide significant activation that differed based on the representational form in which the questions were presented. Details of that analysis follow. All colored areas of the brain are significant at $\alpha=0.05$. Activation differences become more significant as the colors become warmer. Green represents p-values that are less significant than p-values represented in yellow, which are less significant than those represented in red.

Graphical:

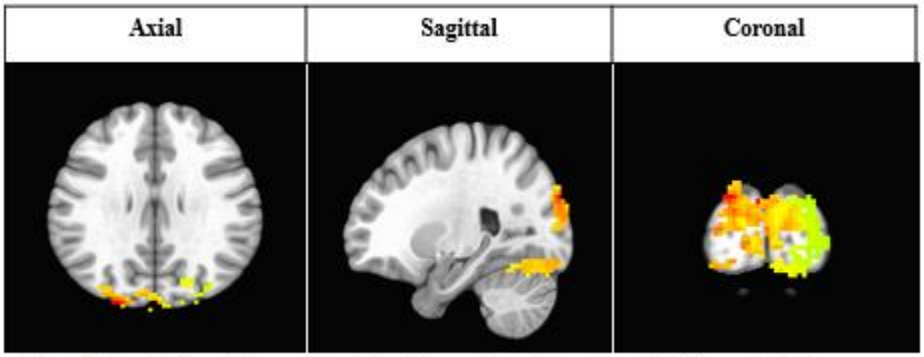

Figure 2: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using Graphical Representations (n=10)

The activated voxels in questions presented graphically were primarily in Broadmann area 19 (associated visual cortex) and near Broadmann area 18 (secondary visual cortex), the focus point of the cluster is in Right Superior Occipital Gyrus. These areas are located in occipital lobe of the brain and respond to visual stimuli. The associated visual cortex processes

visual properties like orientation, spatial frequency, and color and intermediate complexity of object features like geometric shapes.

Language:

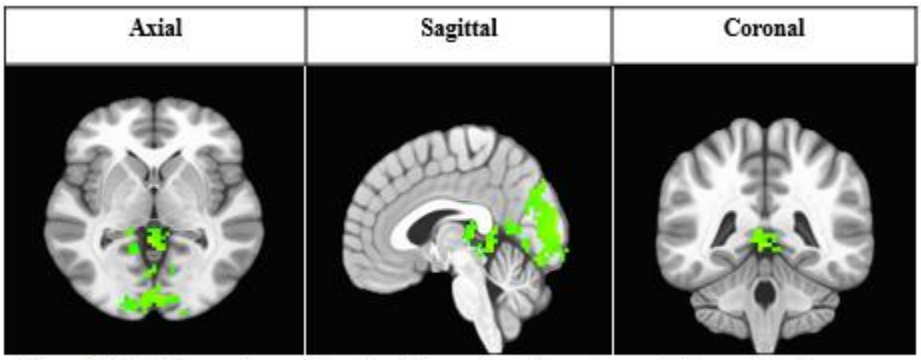

Figure 3: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using English Language Representations (n=10)

Results show that peak activation for questions presented using the language representational form was focused in the Right Culmen and near Brodmann area 31 (Posterior Cingulate Cortex). The Posterior Cingulate Cortex is involved in emotional memory retrievals and configuring learning. It is connected to a wide range of intrinsic control networks such as the Default Mode Network (DMN). The DMN is the network active during day dreaming, effortless mind wandering and gets deactivated in tasks with external stimuli and controlled awareness. The center of the persistent activation cluster, though, is in the Right Cuneus and most of the activation is located in occipital lobe in Brodmann area 17 (Primary Visual Cortex). The Primary Visual Cortex processes simple visual information regarding edge detection of the objects and helps to distinguish object boundaries from the background.

Mathematical:

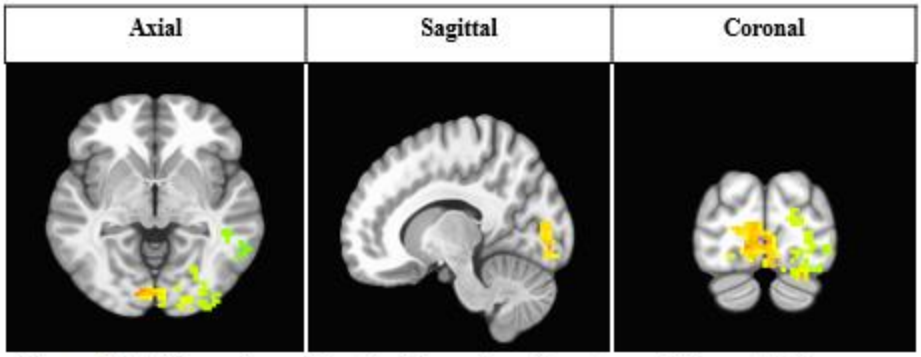

Figure 4: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using Mathematical Representations (n=10)

The activated voxels are predominately located in Brodmann area 17 (Primary Visual Cortex) and the focus point of the cluster of activation is in Right Lingual Gyrus. The Primary Visual Cortex, again, is located in the occipital lobe of the brain and processes simple visual information regarding edge detection of the objects and helps to distinguish object boundaries from the background.

Discussion

Though cryptography is an applied discipline of mathematics, brain activation patterns noted in our results are not consistent with the areas of activation noted in prior fMRI studies of cognitive processing of basic mathematical operations (Delazer, et al., 2006) or simple linear and quadratic functions (Thomas, et al., 2010), even when questions were represented mathematically. The results of this analysis show that most of the activation in response to the stimuli of different representations is in the visual cortex. These results were expected because questions were displayed as visual stimuli and this activation generalizes to the presentation of visual stimuli. We also anticipated activation in prefrontal cortex, which is the region central to working memory, the executive network and the processing of ideas. The lack of activation in the prefrontal cortex was surprising, but may have been influenced by several aspects of the fMRI scan protocol. The presentation order of the questions may have impacted the activation

by adding noise to the scans. Because questions with the same representational forms were not presented together, subjects' brains may have had to switch modes of processing without sufficient time to return to a baseline state. The amount of effort subjects used in processing is also unclear. The average percentage correct on the final scan questions was low at 44.44%. Individual scores ranged from 30.56% to 63.89%. Based on these scores, subjects may have found the questions to be too difficult to solve in 30 seconds and reduced their effort to match a task that they felt was futile. Finally, ten is a small sample size, especially when the difference in instructional method based on class section may make the sample of ten behave more like two samples of five.

The unexpected lack of prefrontal activation may also have roots in the fMRI measurement itself. fMRI signals arise from the contrast of cerebral blood flow known as BOLD (blood oxygen level dependence), which is coupled with neuronal activity. When neurons in an area of the brain become active, oxygenated blood flow to these areas is increased. The contrast of oxygenated to de-oxygenated blood gives rise to BOLD signal. This BOLD signal lags the neuronal activity. With continuous stimuli of different representations being presented to subjects without intermediate rest/crosshair period might result in overlap of BOLD signal, corrupting or averaging out the results.

Conclusion and Future work

We sought to study student's cognitive process on cryptography concepts using fMRI. We examined how different ways of representing cryptography concepts (text, math, graphics, and the use of multiple representational forms) stimulate different regions of a brain then aggregated these analyses to determine where cryptography concepts are processed in the brain. Based on that analysis, we can conclude only that cryptography concepts, as operationalized in

this study, process similarly to other cognitive tasks presented visually. Based on the limitations and delimitations discussed in the results section, we have begun studying this question in a new section of students with a re-designed scan protocol. The questions from each representation will be presented together with rest period between two representations in order to allow the BOLD signal to reach baseline levels before presenting a new representational form. The questions are also re-designed in order to attempt to maximize activation related to cryptography concepts by maximizing the effort subjects exert to answer the question. We expect that these changes to the fMRI methods will add to our understanding of where cryptography concepts are processed in the brain.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1500046. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

Alvarez, J. A., & Emory, E. (2006). Executive function and the frontal lobes: a meta-analytic review. *Neuropsychology review*, *16*(1), 17-42.

Anderson, P. (2002). Assessment and development of executive function (EF) during childhood. *Child neuropsychology*, *8*(2), 71-82.

Arsalidou, M., & Taylor, M. J. (2011). Is 2+ 2= 4? Meta-analyses of brain areas needed for numbers and calculations. Neuroimage, 54(3), 2382-2393.

Bukach, C. M., Gauthier, I., & Tarr, M. J. (2006). Beyond faces and modularity: the power of an expertise framework. Trends in cognitive sciences, 10(4), 159-166.

Dark, M. (2003). A models and modeling perspective on skills for the high performance workplace. (279-296). In R. Lesh & H. Doerr (Eds.), *Beyond Constructivism: A Models and*

Modeling Perspective on Mathematics Teaching, Learning, and Problem Solving. Lawrence Erlbaum Associates: Hillsdale, NJ. ISBN 0-8058-3822-8.

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.

De Luca, C. R., & Leventer, R. J. (2008). Developmental trajectories of executive functions across the lifespan. *Executive functions and the frontal lobes: A lifespan perspective*, *3*, 21.

Hsu,L., Brewe, E., Foster, T.M., and Harper, K.A. (2004). Resource letter RPS-1: Research in problem solving, Am. J. Phys. 72, 1147.

Lezak, M. D., Howieson, D. B., & Loring, D. W. (2004). The behavioral geography of the brain. *Neuropsychological assessment*, *4*, 39-85.

Van Merrienboer, J. J., & Sweller, J. (2005). Cognitive load theory and complex learning: Recent developments and future directions. *Educational psychology review*, *17*(2), 147-177.

Monsell, S. (2003). Task switching. *Trends in cognitive sciences*, *7*(3), 134-140.

Norman, D. A., & Shallice, T. (1980). *Attention to action: Willed and automatic control of behavior* (No. CHIP-99). CALIFORNIA UNIV SAN DIEGO LA JOLLA CENTER FOR HUMAN INFORMATION PROCESSING.

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.

Spiro, R.J. (1992). "Cognitive flexibility, constructivism, and hypertext: Random access instruction for advanced knowledge acquisition in ill-structured domains, "Constructivism and the technology of instruction: A conversation, pp. 57-75.

Sweller, J., Cognitive load during problem solving: Effects on learning, Cognitive Science, 12, 257-285 (1988).

Thomas, M. O., Wilson, A. J., Corballis, M. C., Lim, V. K., & Yoon, C. (2010). Evidence from cognitive neuroscience for the role of graphical and algebraic representations in understanding function. ZDM, 42(6), 607-619.

Zago, L., Pesenti, M., Mellet, E., Crivello, F., Mazoyer, B., & Tzourio-Mazoyer, N. (2001). Neural correlates of simple and complex mental calculation. Neuroimage, 13(2), 314-327.