CERIAS

The Center for Education and Research in Information Assurance and Security

Measuring Cryptography Learning using fMRI

Joe Beckman (beckmanj@purdue.edu), Victor Chen, Ph.D. (victorchen@purdue.edu), Melissa Dark, Ph.D. (dark@purdue.edu),
Pratik Kashyap (pkashyap@purdue.edu), Sam Wagstaff, Ph.D. (ssw@cerias.purdue.edu), Justin Yang, Ph.D. (byang@purdue.edu)

Problem

"…[a] 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" (Evans and Reeder, 2010).

Problem

Cybersecurity experts with not only deep technical skills, but also the 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. This study focuses on cryptography principles.

Research Questions

- What is the efficacy of model-eliciting activities (MEA) for developing representational fluency contextualized on cryptography concepts and practices? MEAs challenge students to build and test conceptual models using six principles: model construction, the Reality Principle, self-assessment, model documentation, model share-ability and reusability, and effective prototyping.
- Can fluency in cryptography concepts be measured in cognitive performance using fMRI and is cognitive processing of cryptographic concepts influenced by instructional method?
- If so, where does processing of cryptography concepts happen in the brain?

Results

Average Percentage Correct by Representational Form of Question: Treatment vs. Control (Percentage/Standard Deviation) during fMRI.

	Concrete (Graphical)	Symbolic – Language	Symbolic – Mathematics	Multiple	Total
Treatment	42.22% / 19.12%	53.33% / 16.33%	62.22% / 11.33%	48.89% / 8.89%	51.67% / 12.82%
Control	31.11% / 19.12%	44.44% / 12.17%	53.33% / 14.74%	20.00% / 10.89%	37.22% / 2.48%
Difference	11.11%	8.89%	8.89%	28.89%	14.45%

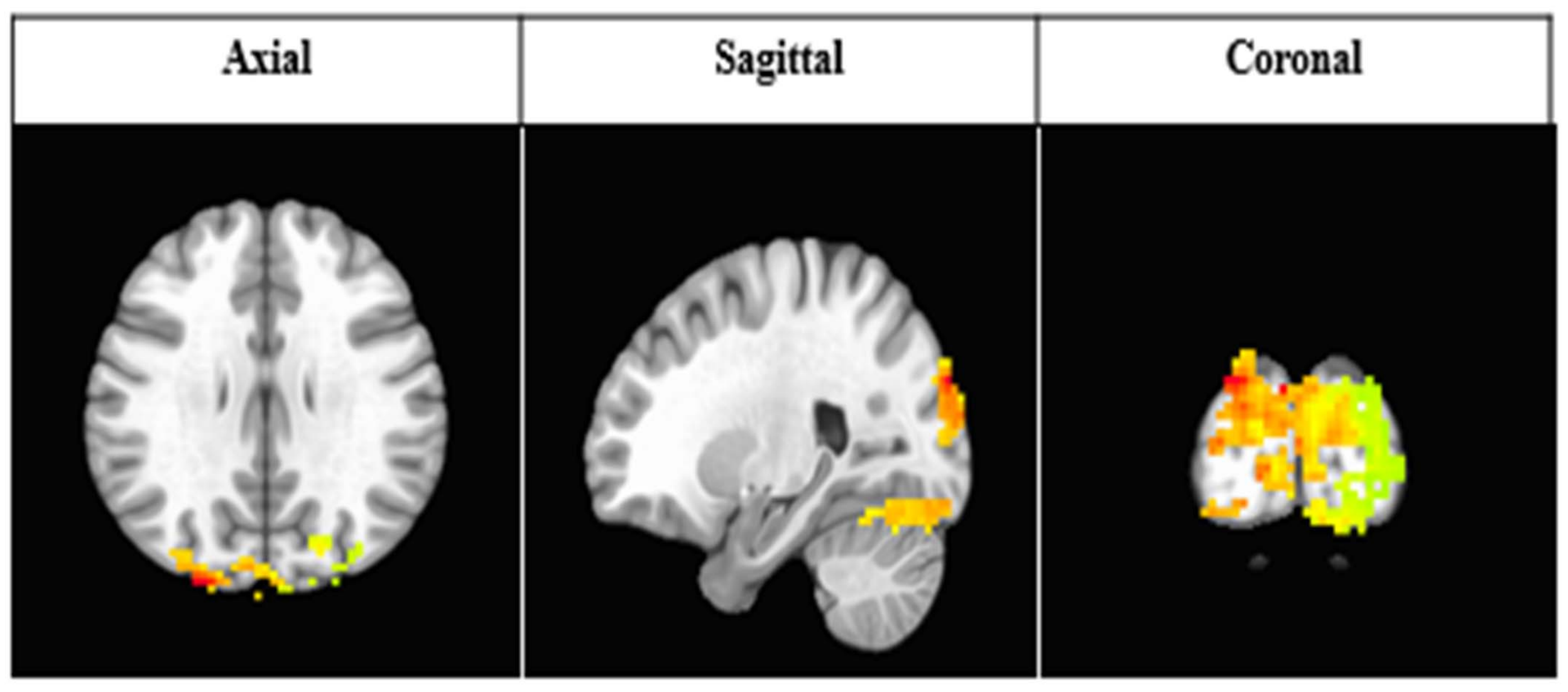


Figure 1: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using Graphical Representations (n=10)

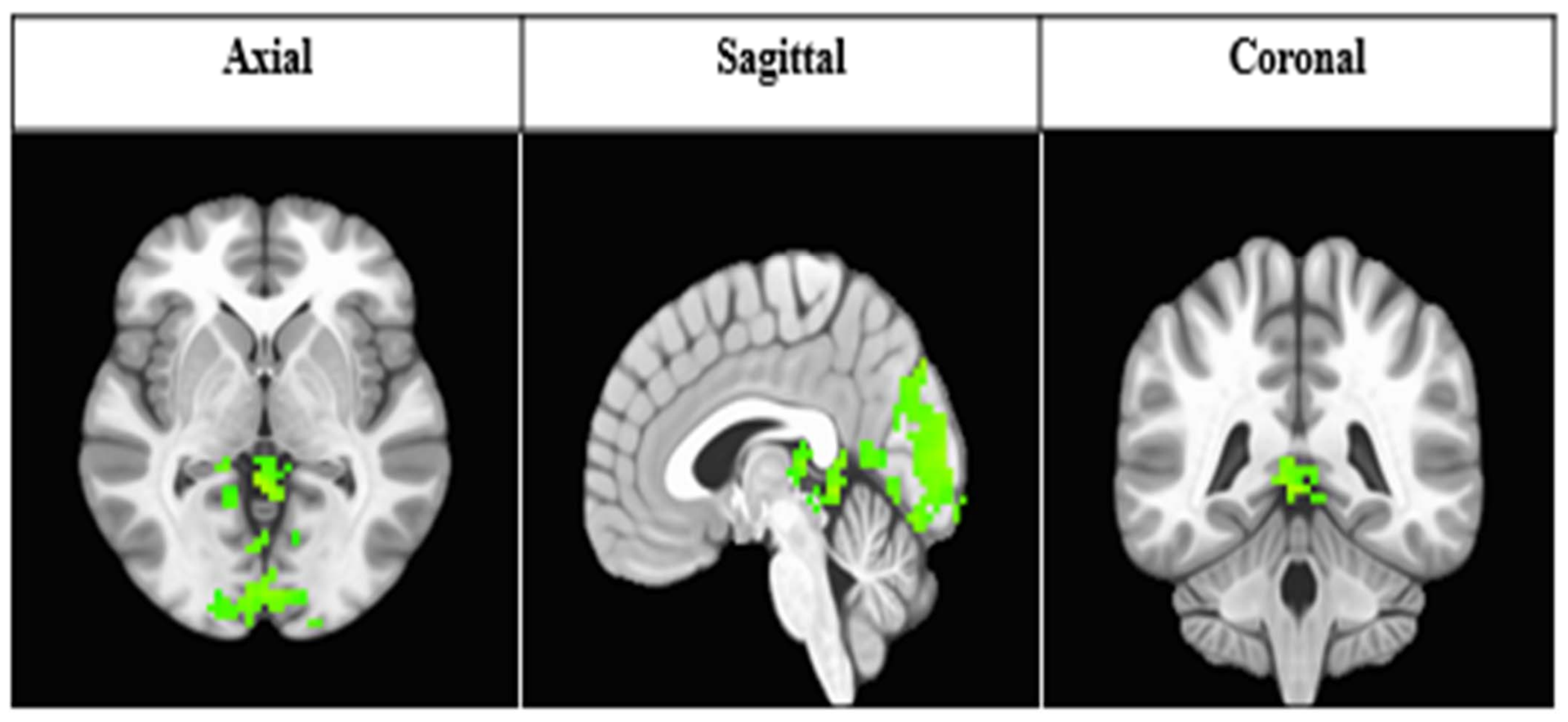


Figure 2: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using English Language Representations (n=10)

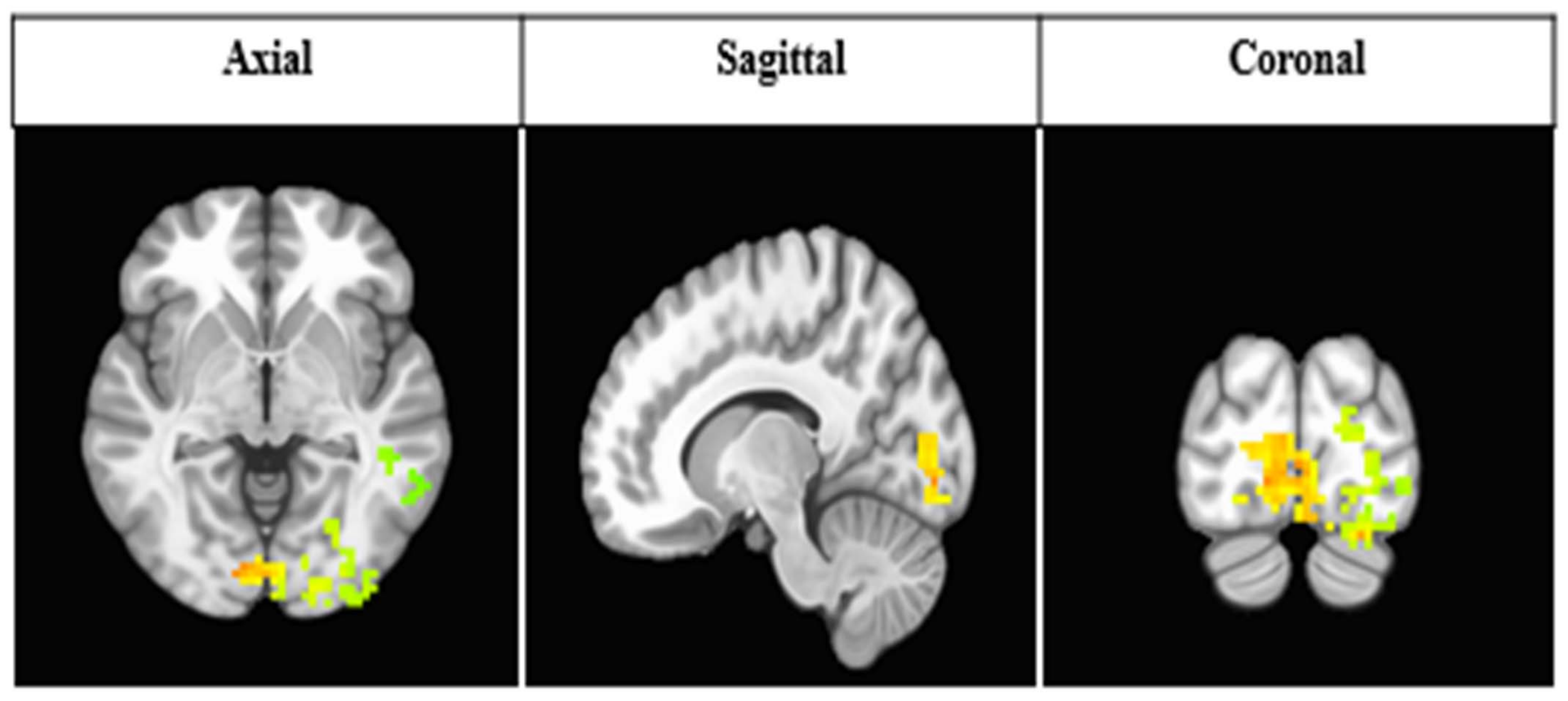
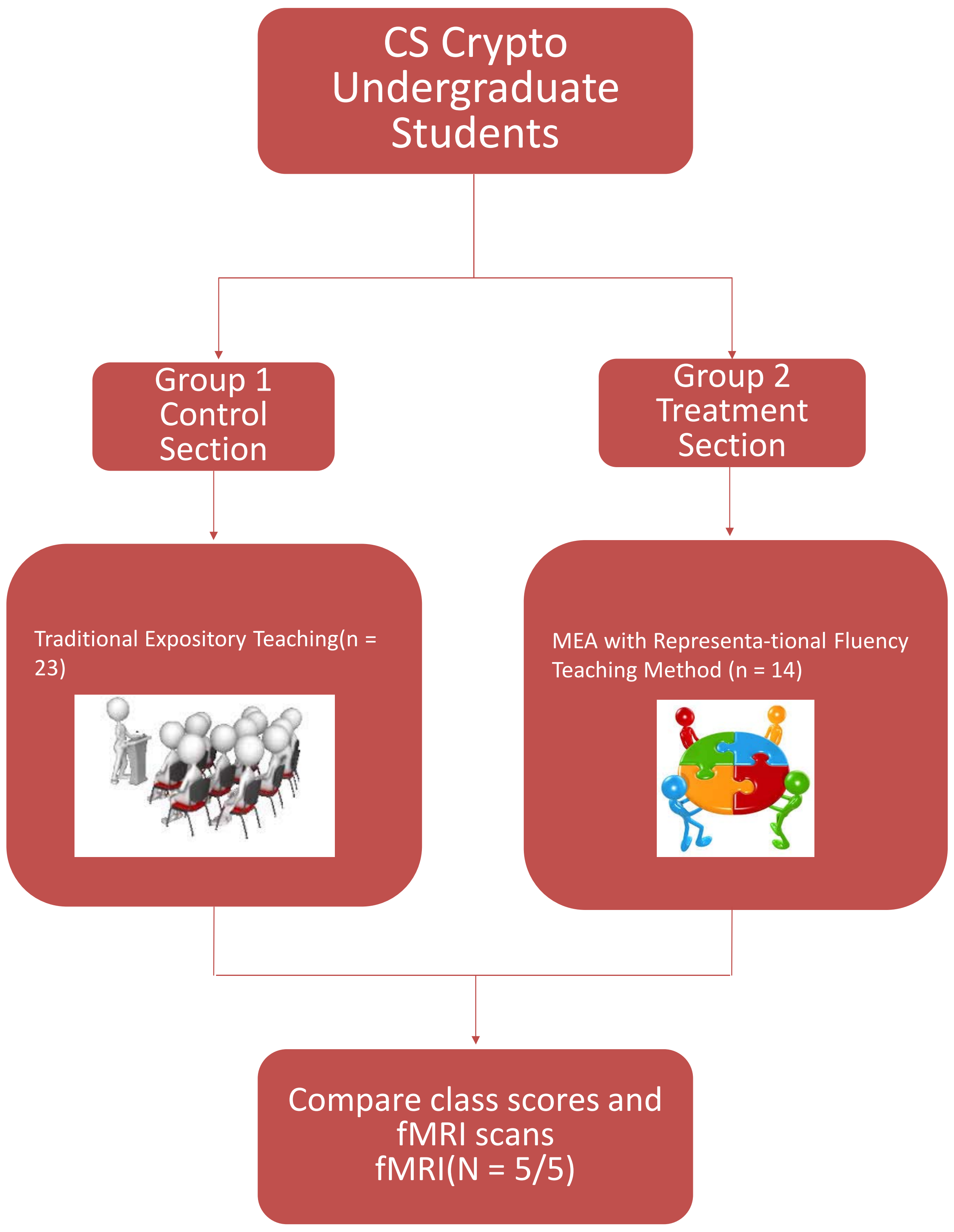


Figure 3: Post-Course Scan of Cognitive Processing of Cryptography Concepts Using Mathematical Representations (n=10)

Methods



CS Crypto Undergraduate Students

Group 1 Control Section

Group 2 Treatment Section

Traditional Expository Teaching(n = 23)

MEA with Representa-tional Fluency Teaching Method (n = 14)

Compare class scores and fMRI scans fMRI(N = 5/5)

References

- Lesh, R., Post, T., & Behr, M. (1987). Representations and translations among representations in mathematics learning and problem solving. Problems of representation in the teaching and learning of mathematics, 21, 33-40.
- Dark, M., & Manigault, C. (2006, June). Model eliciting activity for problem solving in information assurance. In Proceedings of the IA Symposium at SUNY Albany.
- 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.

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.

CERIAS

PURDUE UNIVERSITY