CERIAS

Representational Fluency and the Cognitive Processing of Cryptography Concepts

Joe Beckman, Ph.D. Candidate

PURDUE UNIVERSITY

CERIAS

The Problem

Educate cybersecurity students to be cybersecurity “experts”

- Experts can do more than operate tools, they:
  - …have deep technical skills
  - …but are also facile in abstractions
  - …can think like their adversaries
  - …are able to adapt solutions to emergent problems

PURDUE UNIVERSITY

CERIAS

Our Approach

Apply cognitive theory to cryptography instruction by investigating cognitive processing of cryptography concepts using fMRI.

PURDUE UNIVERSITY

CERIAS

Previous Work: Cognitive Control System

The cognitive control system (CCS) is located in the prefrontal areas of the frontal lobe.

- The CCS is associated with verbal and design fluency, handling novel situations, reasoning, problem solving, working memory and abstract thinking.

(Alvarez, Emory, and Emory, 2006)

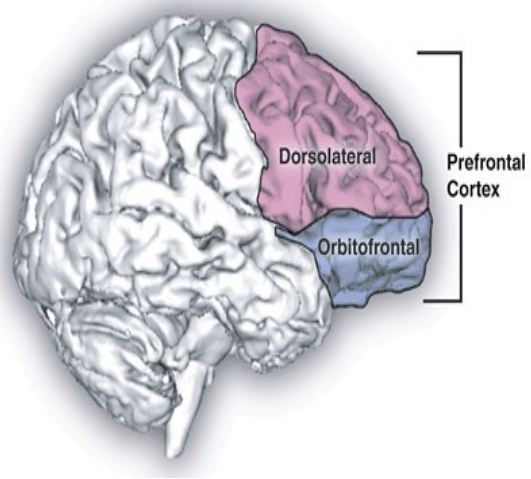


Image credit: NIH

PURDUE UNIVERSITY

CERIAS

Previous Work: Schemas

Cognitive Load Theory says that people develop schemas (Sweller, 1988) to process new information.

Schemas organize before information is transferred to working memory

(Merrienboer and Sweller, 2005, p. 149)

Schemas are part of the CCS.

PURDUE UNIVERSITY

CERIAS

Previous Work: Representational Fluency

Schemas are composed of multiple representational forms.

The ability to transform concepts form one representation to another (representational fluency) connotes depth of understanding.

PURDUE UNIVERSITY

CERIAS

Hypothesis

fMRI measures blood flow to areas of the brain over time.

By knowing which areas of the brain are active when students process cryptography concepts, we can test the effects of various instructional methods on cognitive processing.

Over time, we hypothesize that we will demonstrate that MEA instruction elicit executive control function.

PURDUE UNIVERSITY

CERIAS

Research Questions

1) Where does cognitive processing of different cryptography representations occur in the brain?

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

3) How does instruction focusing on representational fluency impact classroom learning results?

PURDUE UNIVERSITY

CERIAS

Methods

- We studied one section of a grad-level InfoSec “Network Security” course.
- Students were taught selected cryptography via traditional lecture, and others focused on representational fluency.
- 10 students (n=9 finally) from the course volunteered to answer cryptography questions during an fMRI scan of the brain.

PURDUE UNIVERSITY

CERIAS

Methods

- Pretest and post-test of cryptography concepts taught in class
  - Pencil & Paper
  - Concepts were tagged by instructional method (topic)
  - Statistical comparison of pre/post difference (learning gain) by topic not statistically significant at $\alpha=0.05$ ($t=1.19$, $p=0.24$)

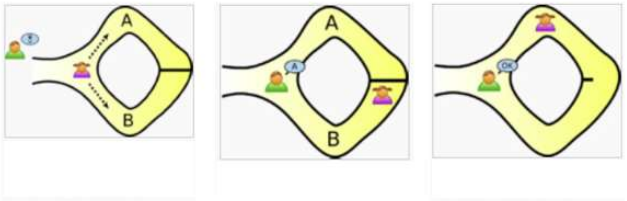
PURDUE UNIVERSITY

CERIAS

Methods

- Block design by topic
- Questions were delivered visually using individual and multiple representations.
- Subjects asked to assess conceptual congruence

Oblivious Transfer: A sender sends information to a receiver, but remains unaware of what the receiver actually received.



$$p \equiv q \equiv 3(mod\ 4)\ ; n = pq$$

PURDUE UNIVERSITY

CERIAS

Study Variable and Data Analysis

- Variable: Cognitive processing of cryptography concepts.
- Operationalization: Increases in blood oxygen levels while students answer cryptography questions.

- Colors represent separate areas and structures of the brain that experienced statistically significant blood oxygen gain.

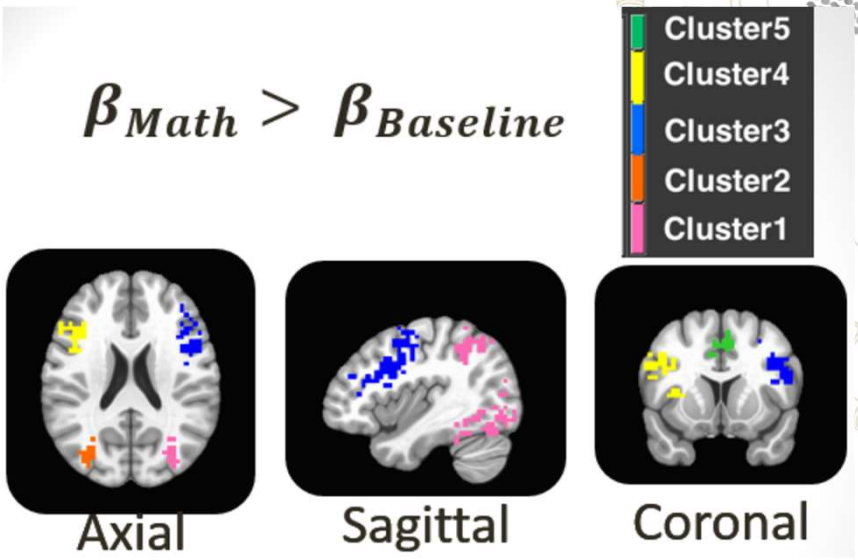
PURDUE UNIVERSITY

CERIAS

Results

- Math

$$\beta_{Math} > \beta_{Baseline}$$



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

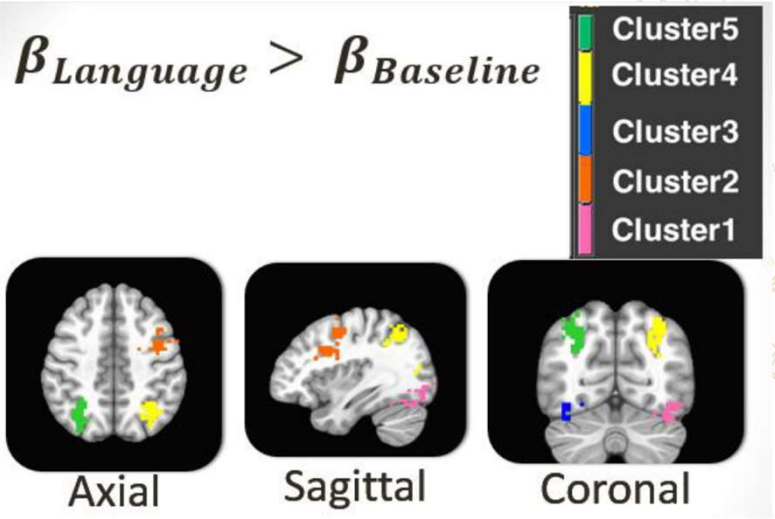
PURDUE UNIVERSITY

CERIAS

Results

- Language

$$\beta_{Language} > \beta_{Baseline}$$



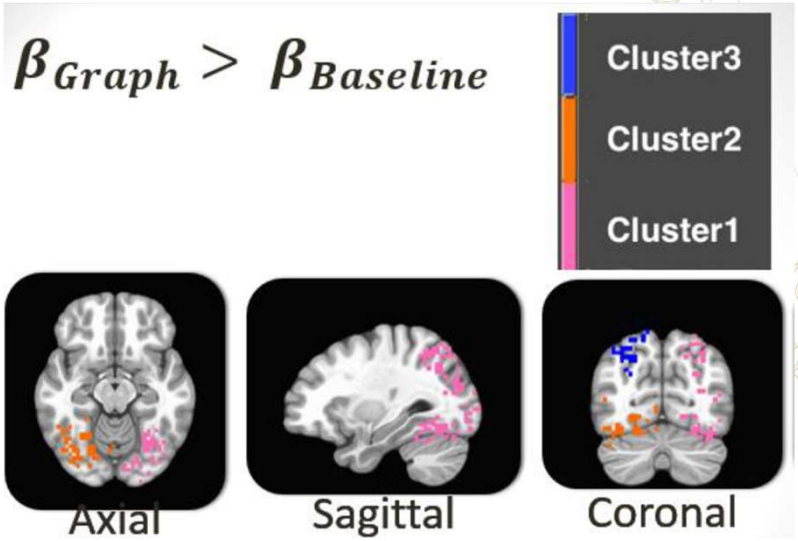
Cluster	Broadmann Area	Gyrus	Usage
1	Left 17	Left Inferior Occipital	Visual Processing
2	Left 44	Left Inferior Frontal	Executive Language Processing
3	Right 37	Right Lingual Gyrus	Visual Processing
4	Left 3	Left Inferior Parietal	Somatosensory Processing
5	Right 1,2	Right Superior Parietal	Somatosensory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

PURDUE UNIVERSITY

CERIAS

Results

- Graphical



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

PURDUE UNIVERSITY

CERIAS

Conclusion (RQ #1)

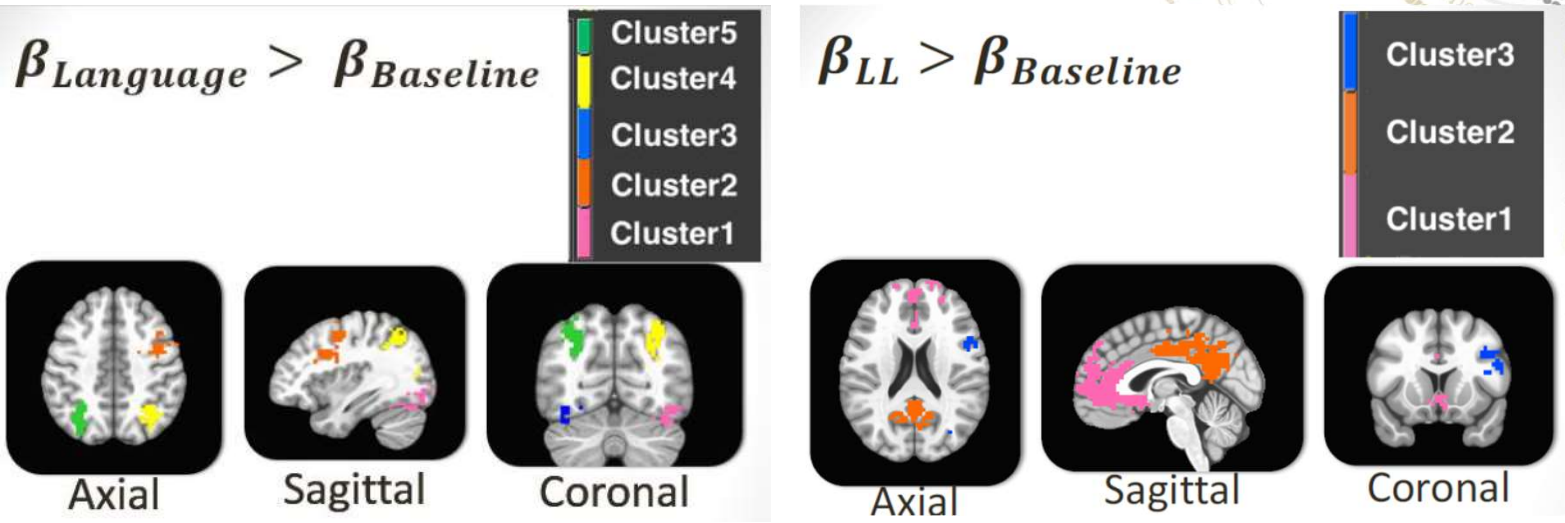
- In this study, cryptography was processed similarly to other visual stimuli represented graphically.
- Cryptography processed from mathematical representations produced areas of activation in executive areas, as well as areas consistent with (Delazer, et al., 2006)
- Cryptography processed from text produced areas of activation in executive language, visual processing, and somatosensory areas of the brain.

PURDUE UNIVERSITY

CERIAS

Results

- Language - Language

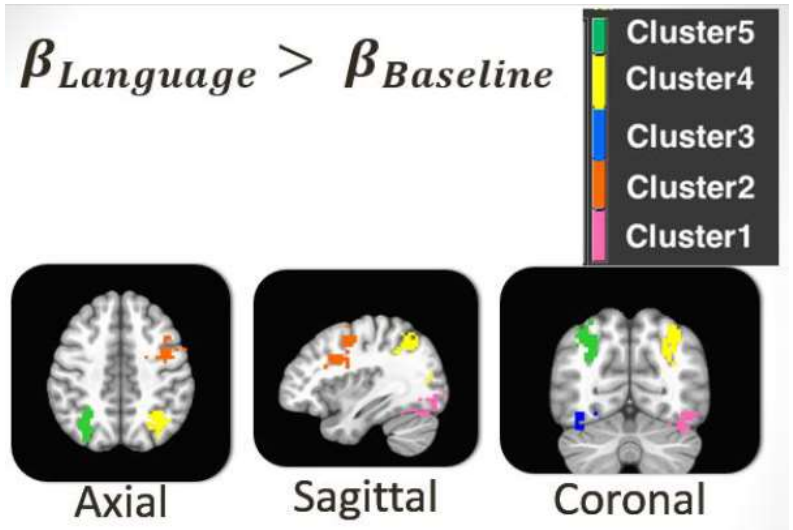


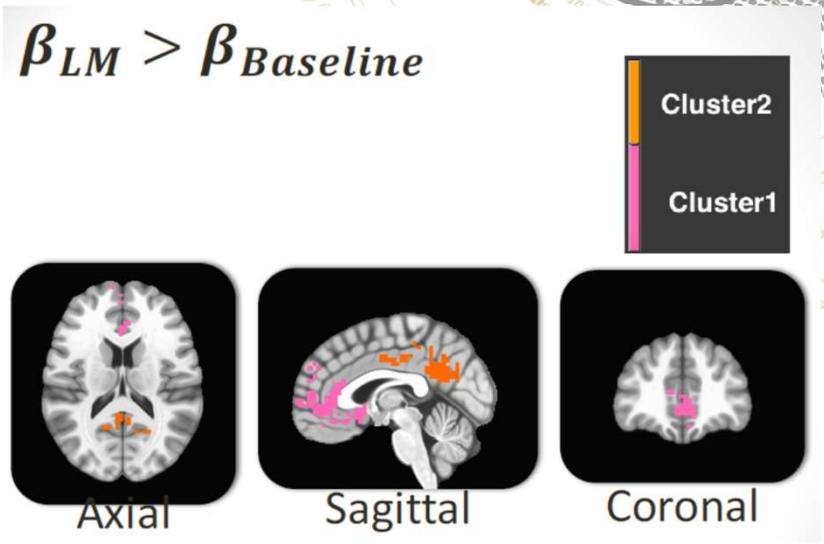
PURDUE UNIVERSITY

CERIAS

Results

- Language - Math



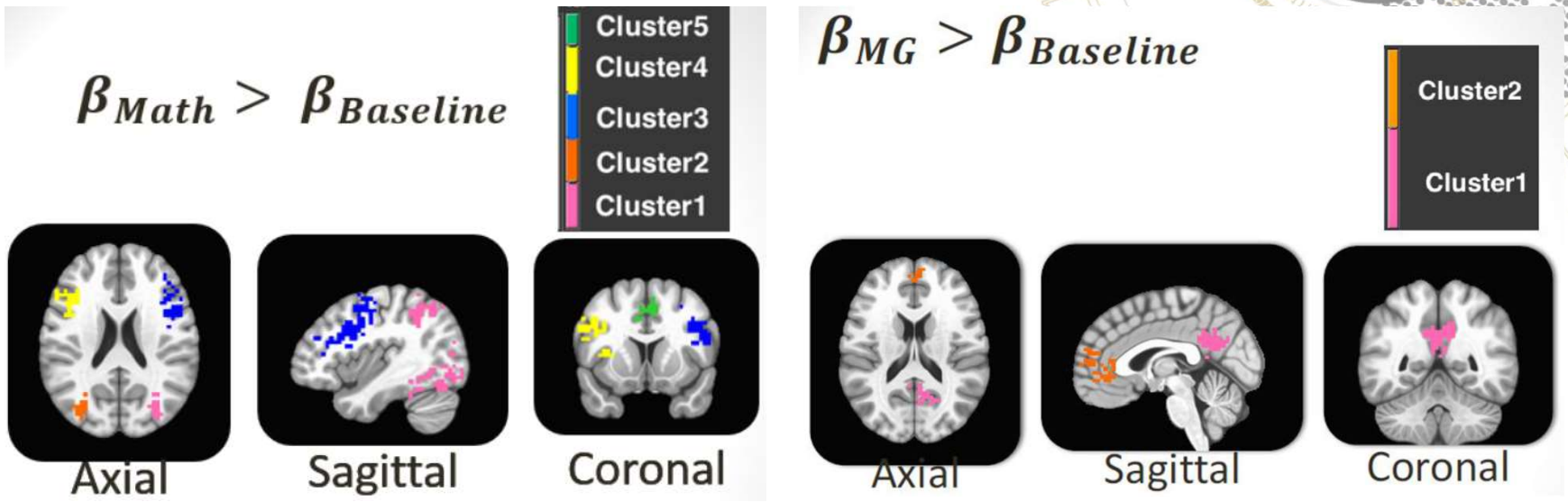


PURDUE UNIVERSITY

CERIAS

Results

- Math - Graphical



PURDUE UNIVERSITY

CERIAS

Conclusion (RQ #2)

- In this study, cryptography was processed similarly to other visual stimuli represented graphically.
- Cryptography processed from mathematical representations produced areas of activation in executive areas, as well as areas consistent with (Delazer, et al., 2006)
- Cryptography processed from text produced areas of activation in executive language, visual processing, and somatosensory areas of the brain.

PURDUE UNIVERSITY

CERIAS

Results - Classroom

- Learning Gains:
  - Instruction focused on representational fluency: μ: .104, σ: .237
    - Pretest score (μ: .568, σ: 0.23)
  - “Standard Instruction”: μ: .036, σ: .241
    - Pretest score (μ: .570, σ: 0.25)
  - learning gains are not significant at α=0.05 (t=1.19, p=0.24)

PURDUE UNIVERSITY

CERIAS

Discussion

- Areas of activation were consistent with previous fMRI studies of mathematics processing (Delazer, et al., 2006).
- Increased activity during representational translation is not supported by these results.
- Learning gains due to instructional methods were not significant.
- Small sample size (9-12)

PURDUE UNIVERSITY

CERIAS

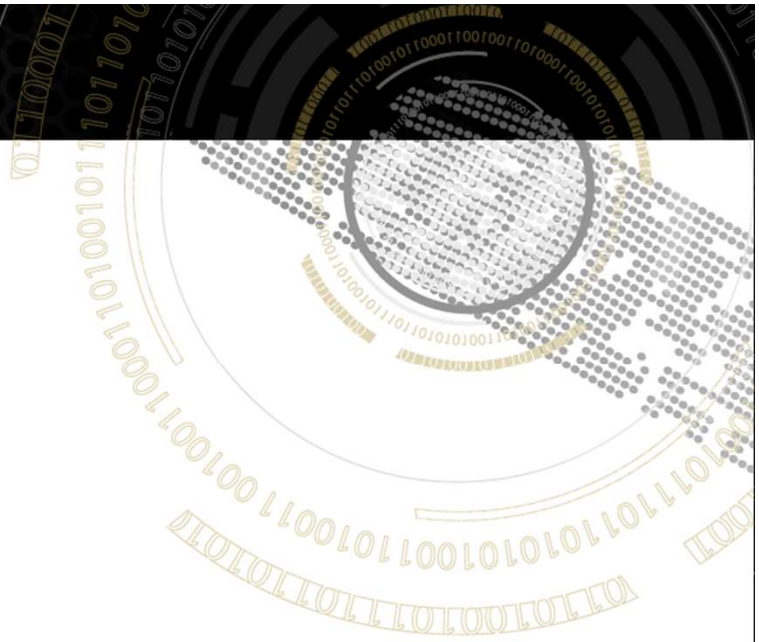
Future Work

- Use more consistent methods of instruction.
- fMRI: Experts vs. Novices

PURDUE UNIVERSITY

CERIAS

Questions?



PURDUE UNIVERSITY

CERIAS