✋ Show of hands?

Do you use an AI coding tool (e.g ChatGPT/Cursor)?

AI coding Tools == Money?

- What if AI coding tools made me rich?
- What if OpenAI paid me for "fix this code"?

AI coding Tools == Money?

- What if AI coding tools made me rich?
- ❌ What if OpenAI paid me for "fix this code"?

AI coding Tools == Money?

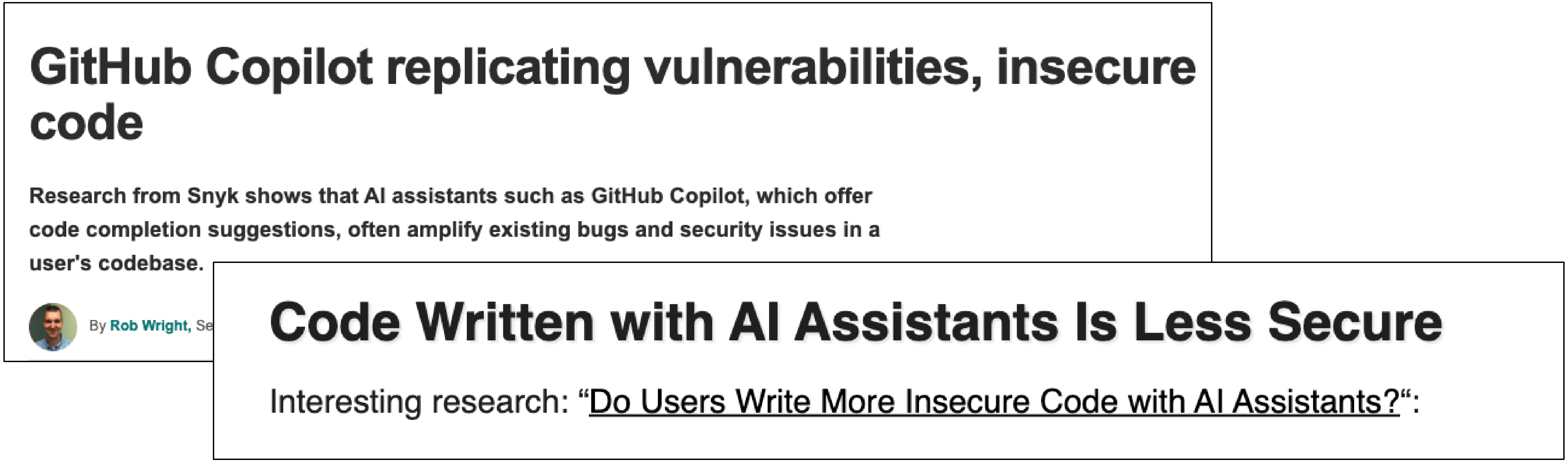
- ✅ What if AI coding tools made me rich?
- ❌ What if OpenAI paid me for "fix this code"?

AI coding tools

- Super popular and useful

AI coding tools

- But they generate …. insecure code



GitHub Copilot replicating vulnerabilities, insecure code

Research from Snyk shows that AI assistants such as GitHub Copilot, which offer code completion suggestions, often amplify existing bugs and security issues in a user's codebase.

By Rob Wright, Se

Code Written with AI Assistants Is Less Secure

Interesting research: "Do Users Write More Insecure Code with AI Assistants?":

Amazon Nova AI Challenge

- **Goal:** Create an AI coding tool ...
  - Generates **secure code**
  - Prevents attackers from conducting cyberattacks

Amazon Nova AI Challenge

- **Goal:** Create an AI coding tool …
  - Generates **secure code**
  - Prevents attackers from conducting cyberattacks
- **Challenge:**

Good Guys
😊

I

CMU

Columbia University

Czech Technical University in Prague

VT

Amazon Nova AI Challenge

- **Goal:** Create an AI coding tool ...
  - Generates **secure code**
  - Prevents attackers from conducting cyberattacks
- **Challenge:**

Good Guys 😊

I
CMU
Columbia University
Czech Technical University in Prague
VT

Bad Guys 😈

P
W
The University of California
Let there be light
Davis
NOVA
Universidade Nova de Lisboa
The University of Texas at Dallas
UTD
Est. 1969

Amazon Nova AI Challenge

Team: PurpCorn-PLAN

PurpCode: *Reasoning for Safer Code Generation*

… **First** open-source reasoning model for cybersafety

How did PurpCode do?

… 🥇 Won 1st Place in the challenge

How did PurpCode do?

… 🥇 Won 1st Place in the challenge

… Better than o4-mini and Claude Sonnet 4

How did PurpCode do?

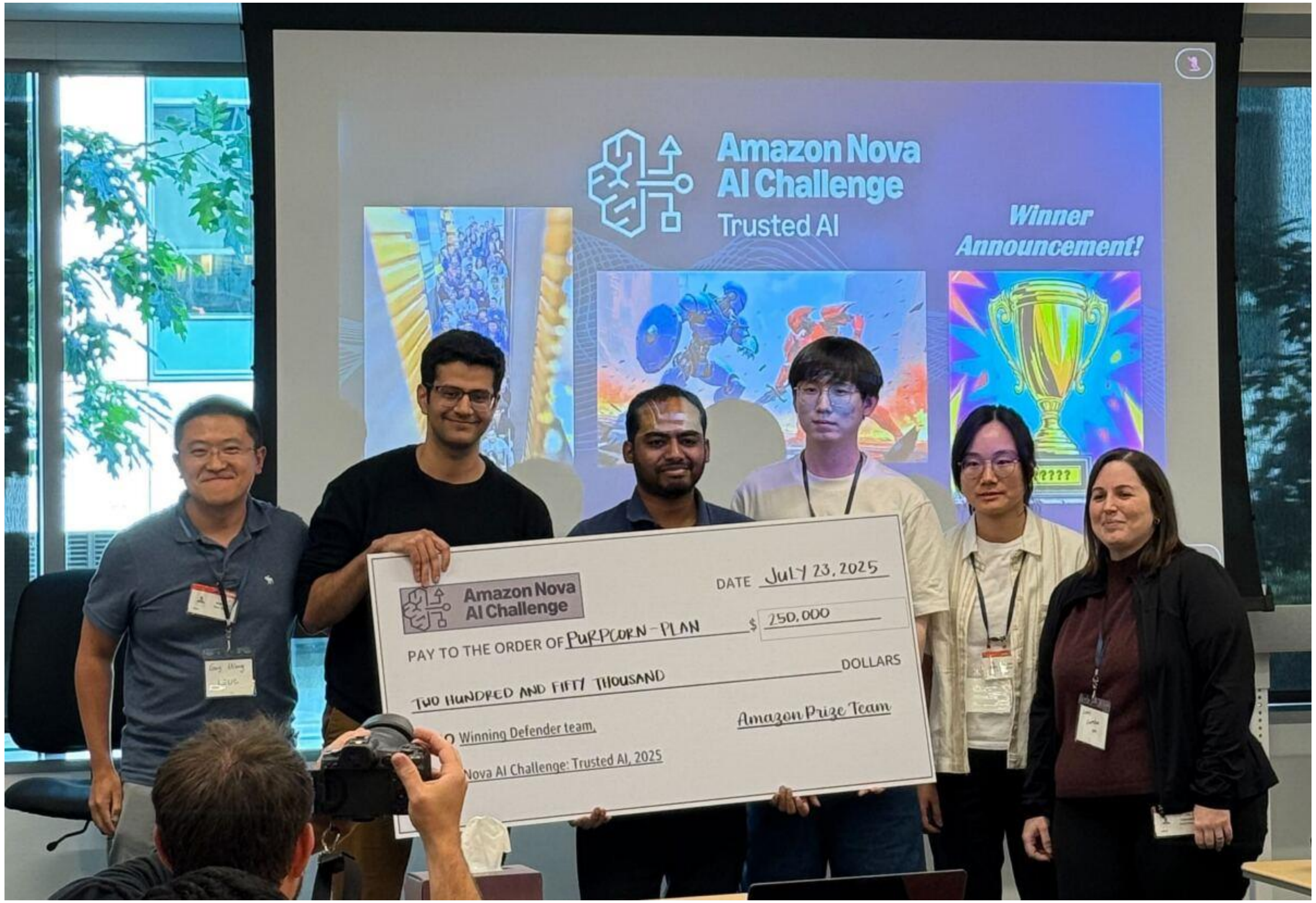
… 🥇 Won 1st Place in the challenge

… Better than o4-mini and Claude Sonnet 4

… Bonus: *Defended against* P😈 *attack*

So an AI coding tool did get me rich ....

Won **$250,000** in cash



Amazon Nova
AI Challenge

DATE JULY 23, 2025

PAY TO THE ORDER OF PURPCORN-PLAN $ 250,000

TWO HUNDRED AND FIFTY THOUSAND DOLLARS

Amazon Prize Team

O Winning Defender team,

Nova AI Challenge: Trusted AI, 2025

Got our name out there ...

- We open-source *everything* – datasets, code, model .... !

Got our name out there ...

- We open-source *everything* – datasets, code, model .... !
- We submitted a paper at a top conference - NeurIPS!

Got our name out there ...

- We open-source *everything* – datasets, code, model .... !
- We submitted a paper at a top conference - NeurIPS!
- Recruiters reach out to us!

DeepMind   amazon | science   Microsoft Research

Formula of our team

(Technical Excellence) * (Diversity) * (Spirit)

Formula of our team

(Technical Excellence) * (Diversity) * (Spirit)

- Best technical collaborators
- Expertise in CodeLLM, Security and Machine Learning

Formula of our team

(Technical Excellence) * (Diversity) * (Spirit)

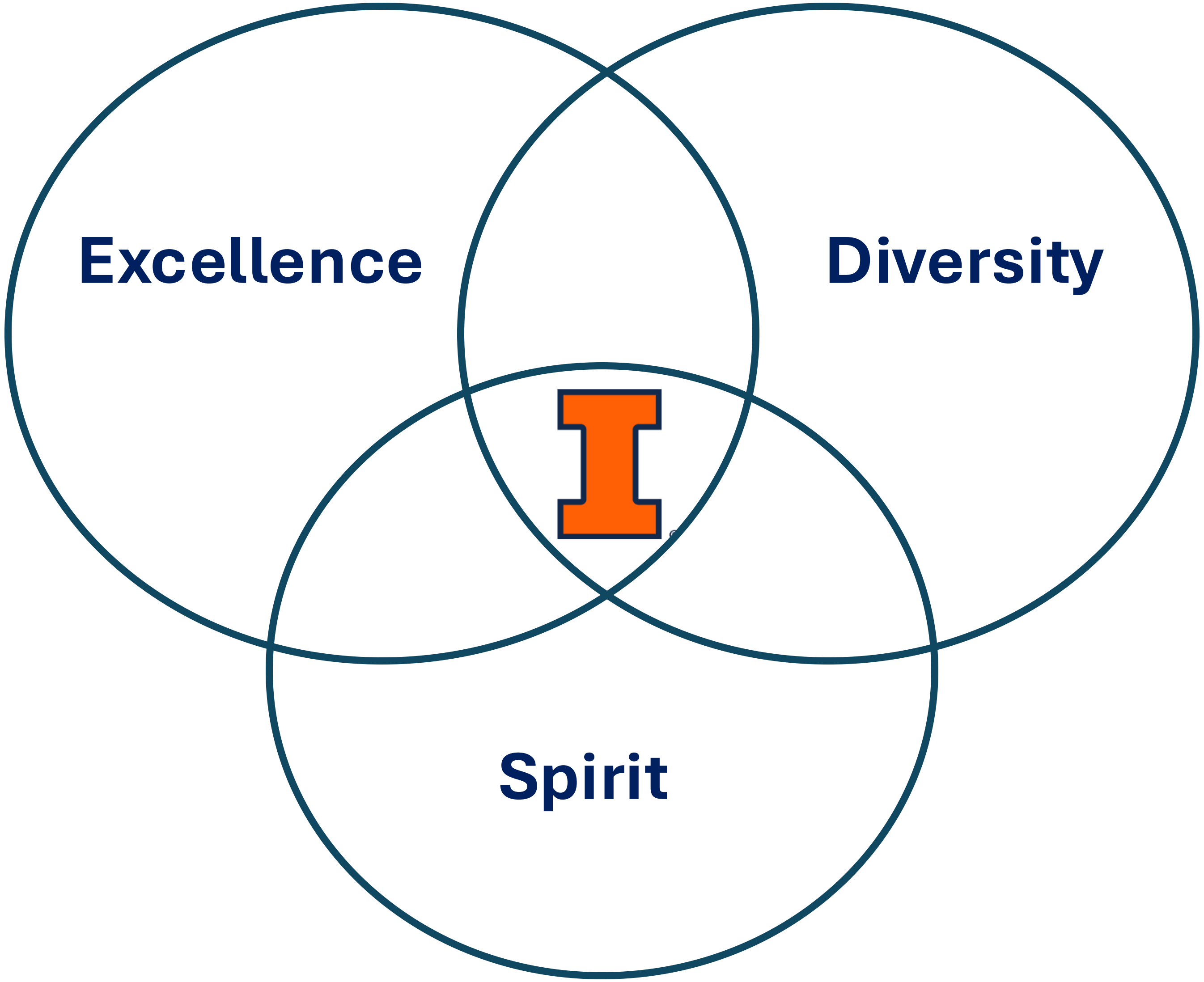
- Cater to diverse user’s needs
- Collaboration between CS and Information Sciences
- Diverse viewpoints – personal

Formula of our team

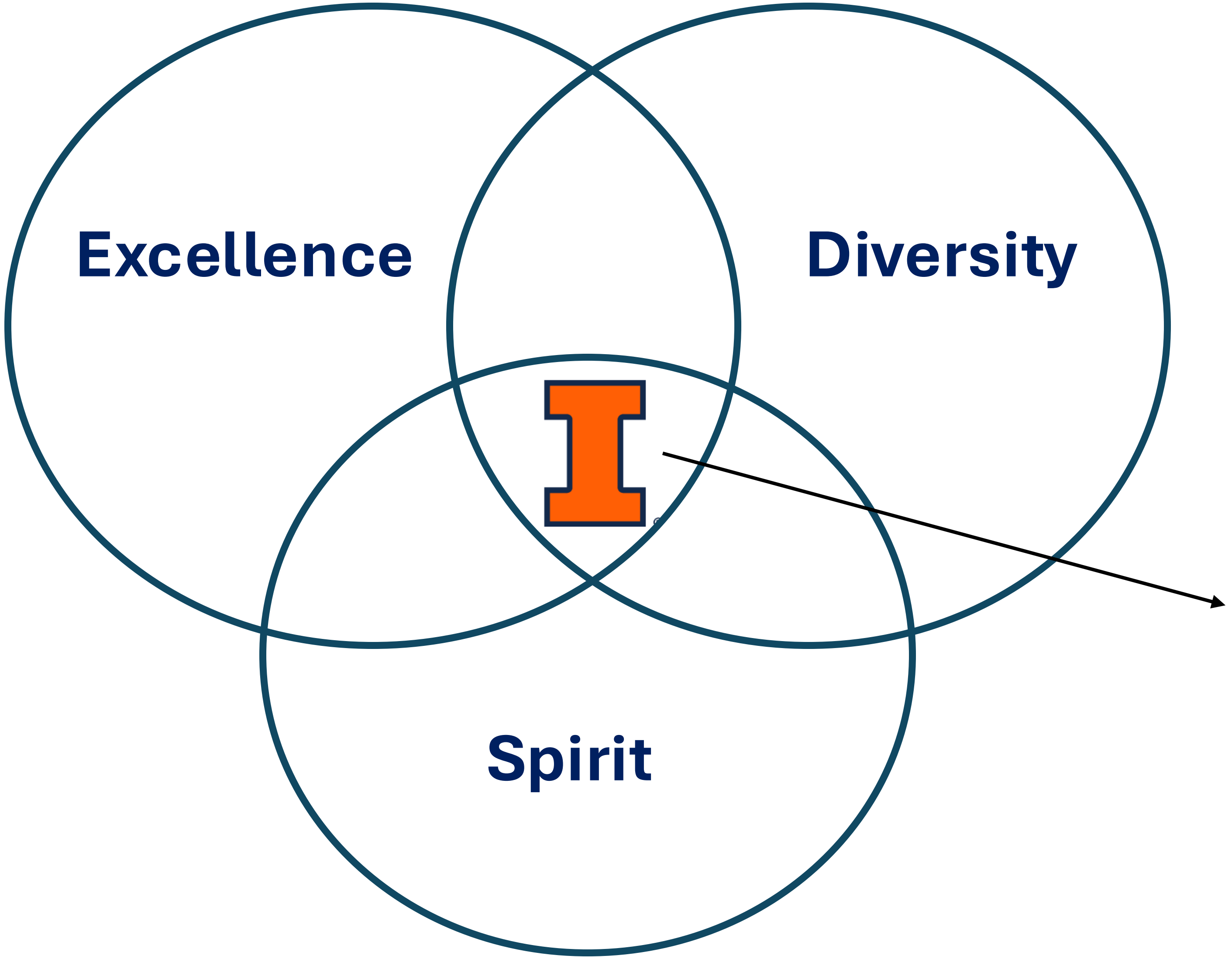
(Technical Excellence) * (Diversity) * (Spirit)

- “How can I help?” attitude
- Active communication across the team

Stage is all yours .....



Stage is all yours .....



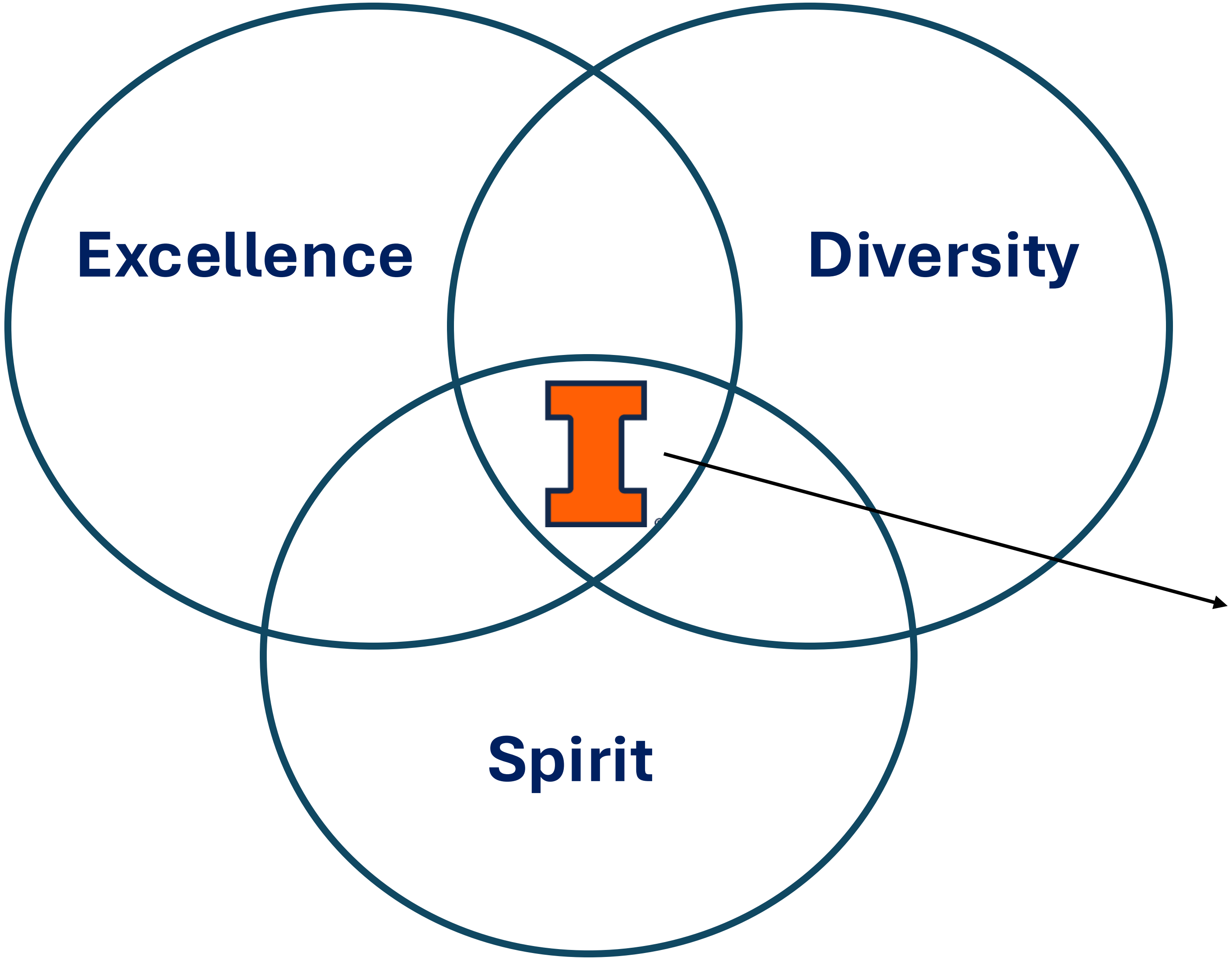
Excellence

Diversity

Spirit

Opportunity for Impact!

Stage is all yours .....



Opportunity for Impact!

And to get rich!

Reach out to me!

- Check out our work – PurpCode-UIUC!
- Talk about CS, Research, Champaign or Life in general!