MATH REU
&
ZERO KNOWLEDGE PROOFS

Emily Sundberg

October 28, 2022

Clemson University

WHAT IS AN REU?

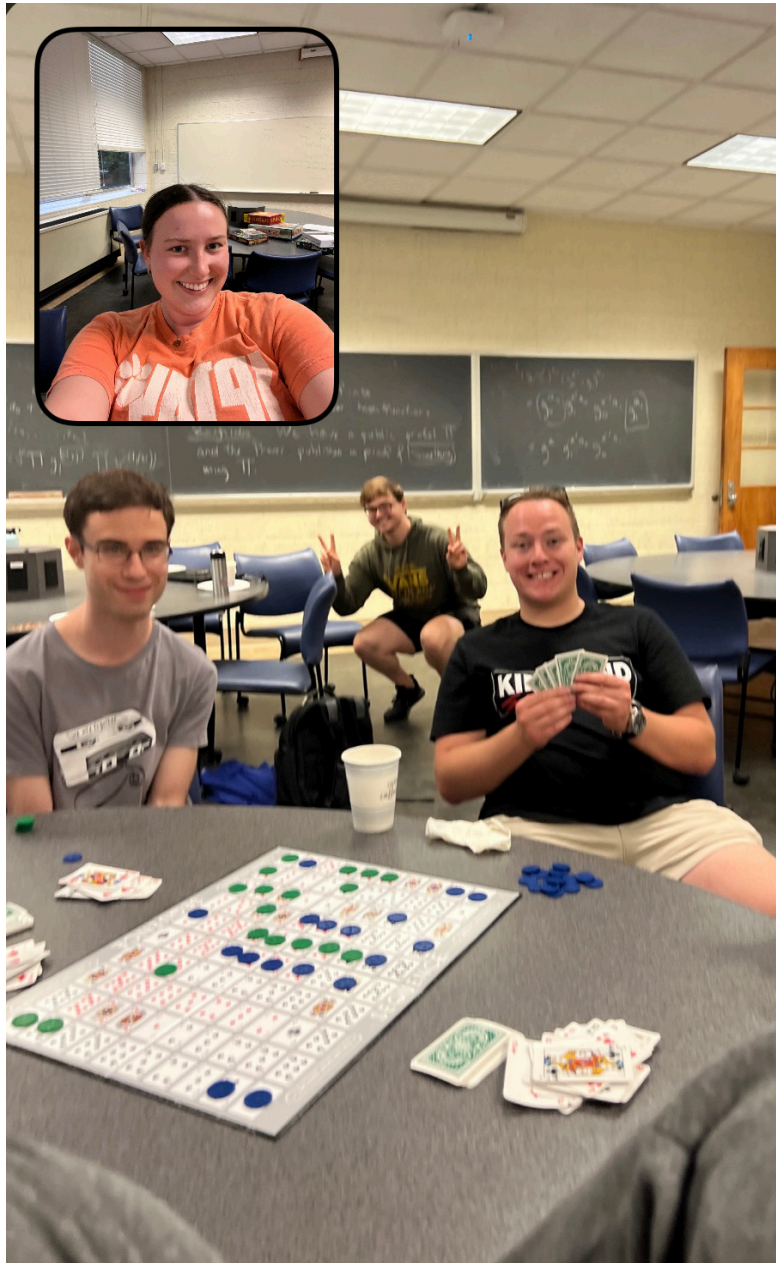
- A research experience for undergraduates
- An opportunity to conduct unique research in small groups or individually
- An opportunity to get a feel for research in a non-committal setting
- Sponsored by the NSF, NSA, or another grant - usually paid with stipend
- Looks really great on grad school applications!

MY EXPERIENCE IN AN REU - A DAY IN THE LIFE

- We were provided housing in Thornhill Village on campus
- We would wake up and walk over to Martin at 9am
- Usually, we would eat breakfast that we brought and go over what we wanted to accomplish in the day
- Get started on the project for the day
- Lunch! an hour or so
- Afternoons were normally spent talking to our mentors and presenting what we've figured out.
- Go home around 5pm
- Hang out, game nights, work on project a little bit, do some readings before the next day, sleep!

HOW TO APPLY TO AN REU

- mathprograms.org
- Really convenient! You can apply to almost all math REUs on this one website!
- Go to "View Programs" and in the search bar look up REU.
- You'll need a transcript, CV/Resume, 2 letters of recommendation, cover letter.
    - Your recommendation writers only need to submit letters once to the website and you can apply to as many as you'd like!
- They're pretty competitive so I recommend starting the applications early.
- Most applications close in February so I would start applying in the December/January time frame.
- Some REUs may have specific applications on their websites, this is much less likely.



QUESTIONS ABOUT THE REU

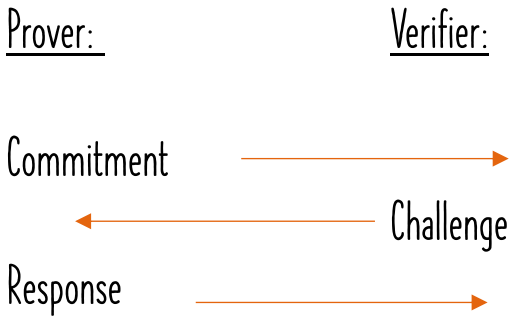
before I move on to math stuff

SOME DEFINITIONS

- Group: a set with one operation (usually multiplication or addition)
- Field: a set with two operations
  - Example: Group 1 consists of integers (mod 5) under addition, Group 2 consists of integers (mod 5) under multiplication
    - Then, the Field consists of integers (mod 5) under both addition and multiplication
- Relation: A relation R consists of elements (s ; w) where s and w satisfy a certain predicate. An element of R is considered a statement-witness pair where s is the statement, and w is the witness (knowledge).
  - We will use this relation notation in further definitions

SOME MORE DEFINITIONS

- Interactive Protocol: A system that demonstrates an exchange between a Prover and Verifier where the Prover is trying to convince the Verifier that a statement is true.
  - 2 Properties:
    - Completeness: If the statement is true, the Prover will always be able to convince the Verifier.
    - Soundness: If the statement is false, the Prover will never be able to convince the Verifier that it is true (except by an incredibly small possibility)



DISCRETE LOGARITHM ASSUMPTION AKA DECISIONAL DIFFIE-HELMAN (DDH) ASSUMPTION

- Suppose g and y are elements of a group G with order p (prime). It is computationally hard to find an integer x such that

$$y = g^x$$

Interactive protocol using discrete log (Shnorr Protocol)

Showing knowledge of x such that $y = g^x$

Prover $(g, y; x)$

Verifier (g, y)

1. Choose a random t in the group such that $g^t = r$

r (commitment) →

← c (challenge)

2. Pick a random c in the group

z (response) →

3. Compute $z = t + xc \pmod p$

4. Confirm iff $g^z = r\, y^c$

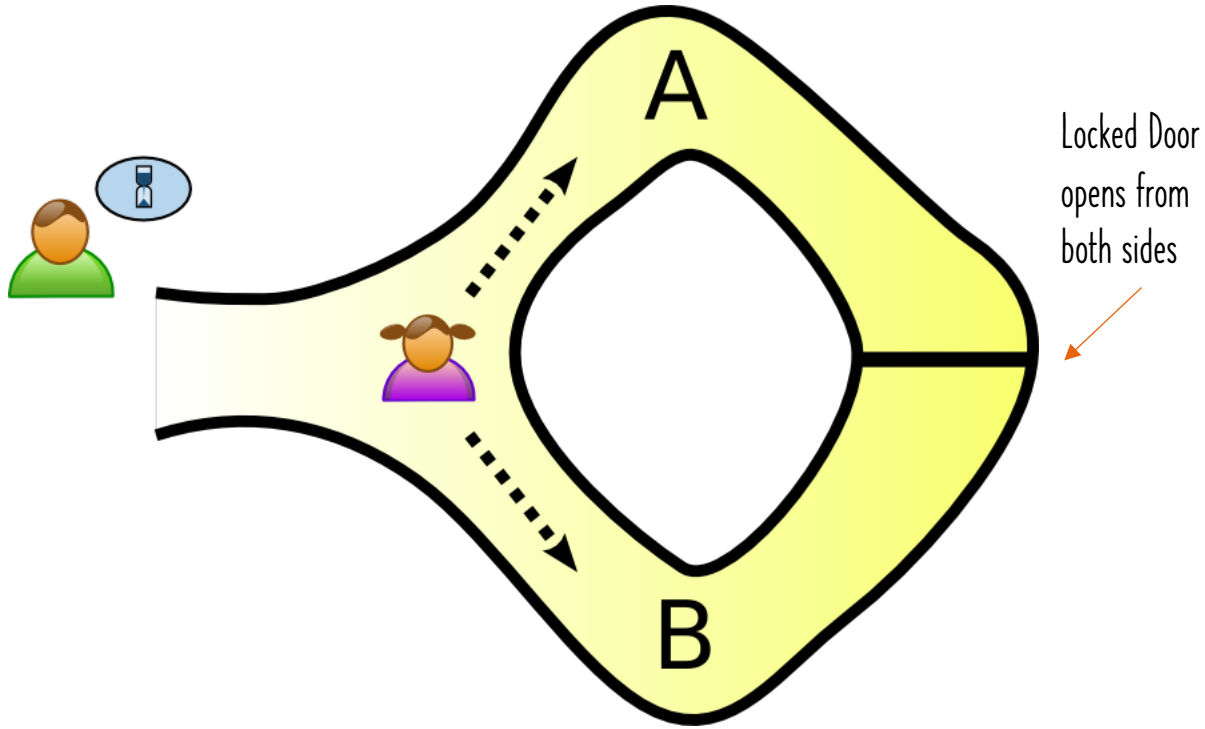
WHAT IS A ZERO KNOWLEDGE PROOF?

- Suppose I have some information. I want to prove to you that I possess this information without revealing to you what this information is. I also don't want anyone else to know that I possess this information.
- An interactive protocol with an extra Zero Knowledge property. The Schnorr Protocol is a zero-knowledge interactive protocol

- Examples:
  - Colorblind friend
    - Say I am colorblind. You have two balls that look identical to me, but you can see they are different colors. I need to be convinced they are actually two distinct colors.
  - Ali Baba cave

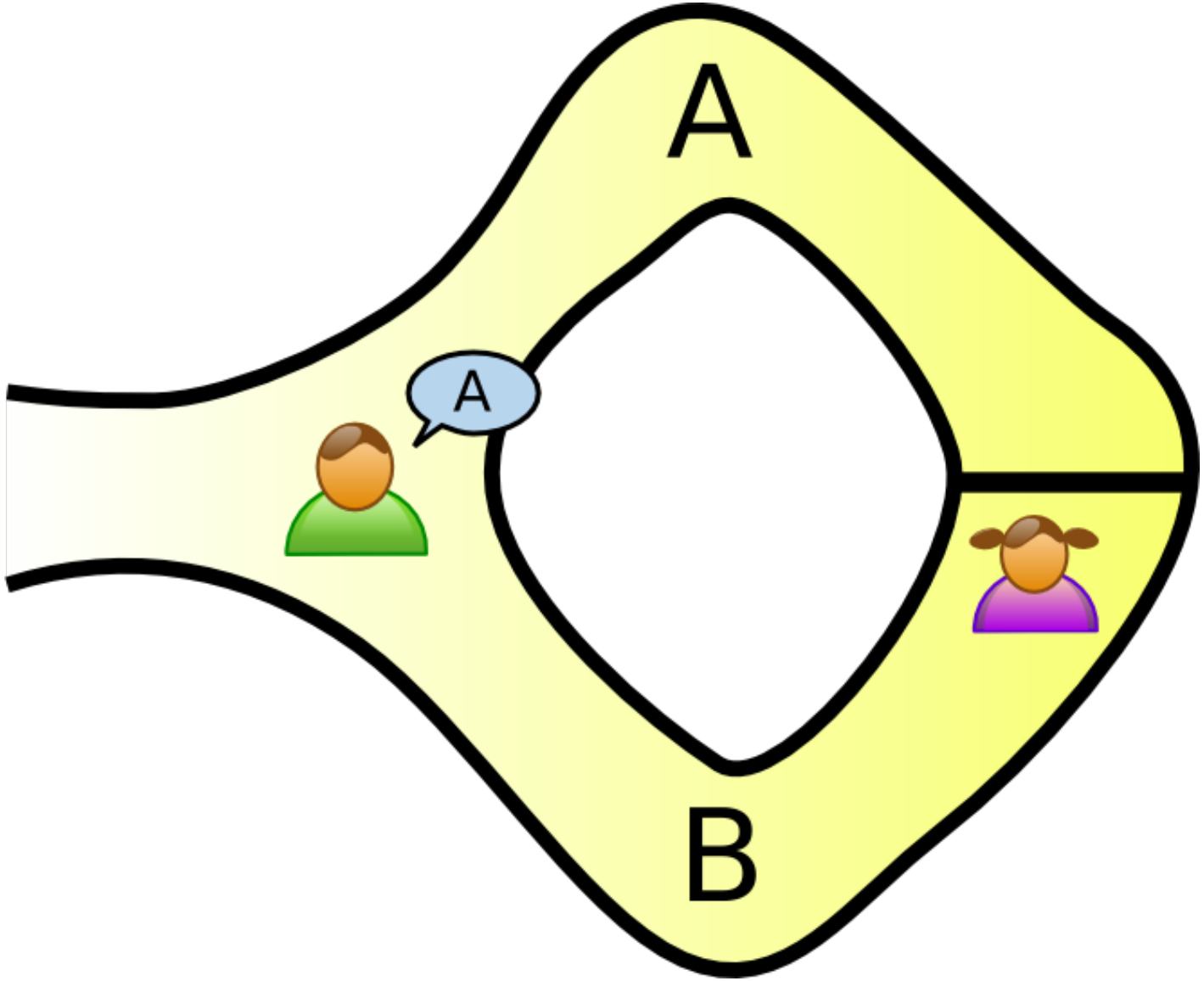
ALI BABA CAVE - A CLASSIC EXAMPLE

- Two People: Peggy (Prover) and Victor (Verifier)
- Peggy claims she knows the secret password to a door in this cave
- Victor doesn't trust that Peggy is telling the truth and Peggy doesn't trust Victor with the secret password.
- Design a protocol to test this:
  - Step 1: Peggy goes into the cave and randomly commits to a route A or B.
  - Victor doesn't see this, as he is waiting outside



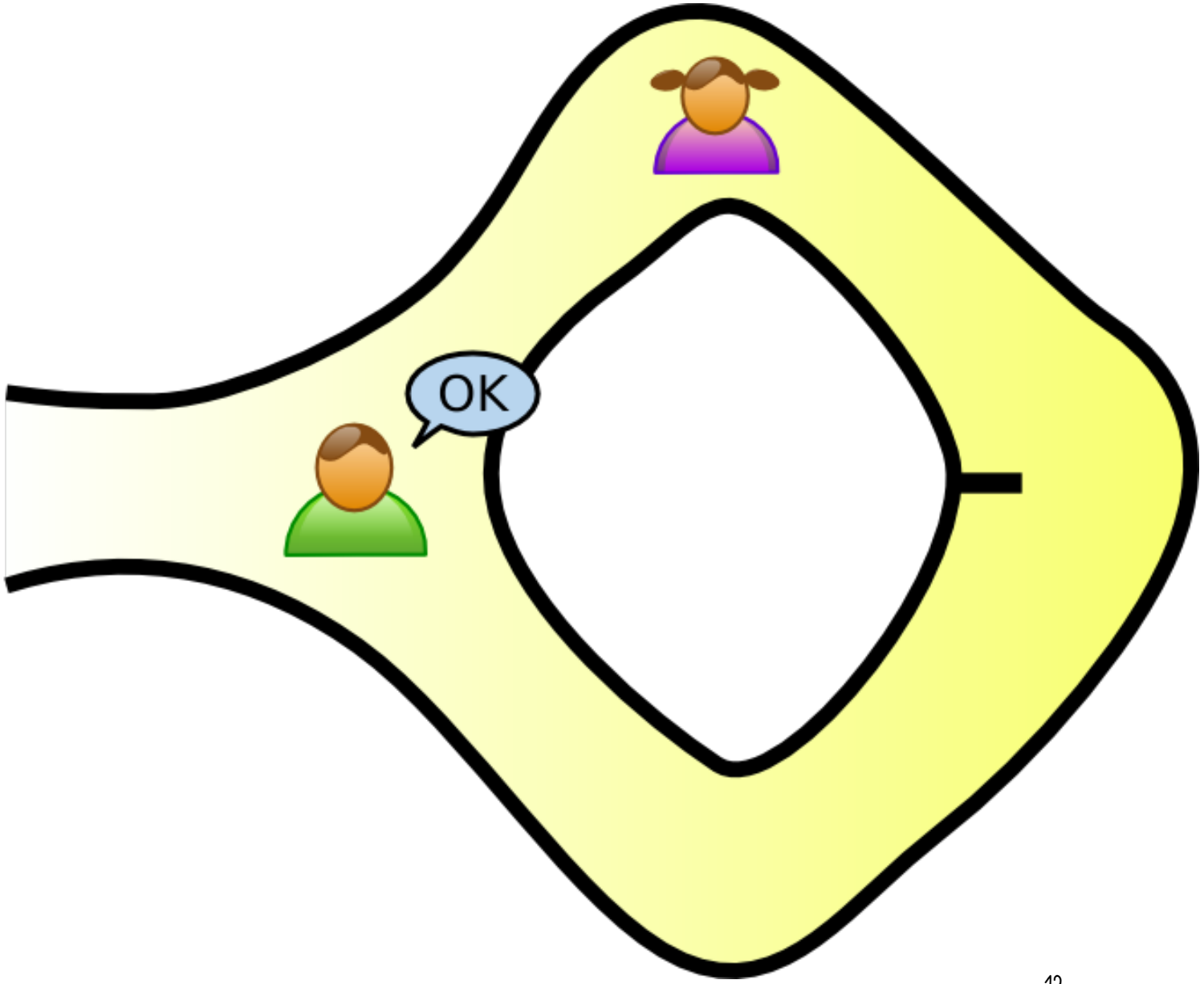
- Step 2: Victor enters the cave and calls out a challenge. i.e. he calls out a path he wants Peggy to exit from

- Note: if she doesn't know the password, Peggy will only be able to exit from the route secretly entered through.



- Step 3: Peggy, knowing the secret password, exits through the path that Victor called out. This is her response

- Step 4: If the process is repeated, Victor will always be convinced by Peggy so long as she knows the password. If she didn't know the password, her odds of getting it right every time is roughly 1 in a million



PROPERTIES OF ZERO KNOWLEDGE PROOFS

- Completeness
  - If the statement is true, the Verifier will always be convinced by the Prover.
  - If Peggy knows the password, Victor will always be convinced because she will always come out the correct side.
- Soundness
  - If the statement is false, no dishonest Prover can convince the Verifier that it is true.
  - If Peggy doesn't know the password, she will not be able to convince Victor except with some very small probability.
- Zero Knowledge
  - The Prover's secret is never revealed to the Verifier and no third party observer could be convinced that the statement is true.
  - Victor never finds out the password, and if someone was watching this interaction, they would not be convinced because Peggy and Victor could be colluding!

PEDERSEN COMMITMENT / INNER PRODUCT

- A Pedersen commitment is used to encrypt two vector commitments using the inner product
- The relation used for the inner product is

$$\mathcal{R}_{\mathrm{IP}}(n) = \left\{ \begin{array}{l|l} (\mathbf{G}, \mathbf{H} \in \mathbb{G}^n, u, \alpha, \beta \in \mathbb{G}, c \in \mathbb{F}_p; & \alpha = \mathbf{G}^{\mathbf{A}} \wedge \beta = \mathbf{H}^{\mathbf{B}} \\ \mathbf{A}, \mathbf{B} \in \mathbb{F}_p^n) & \wedge c = \langle \mathbf{A}, \mathbf{B} \rangle \end{array} \right\}.$$

- The Pedersen commitments are α and β

MATRIX PRODUCT

- We created a zero-knowledge interactive protocol designed to verify the product of two matrices.
- The relation for this product is

$$\mathcal{R}(n,m,k) = \left\{ \begin{array}{l} (\mathbf{G} \in \mathbb{G}^{n\times m}, \mathbf{H} \in \mathbb{G}^{m\times k}, \mathbf{U} \in \mathbb{G}^{n\times k}, g_0, P \in \mathbb{G}; \\ \mathbf{A} \in \mathbb{F}_p^{n\times m}, \mathbf{B} \in \mathbb{F}_p^{m\times k}, r \in \mathbb{F}_p) \end{array} \middle| \; P = \mathbf{G}^{\mathbf{A}}\mathbf{H}^{\mathbf{B}}\mathbf{U}^{\mathbf{AB}} g_0^r \right\}.$$

- We carry this out by folding one parameter at a time
  - We start by folding the rows of A in half and the columns of B in half.

WHAT DOES THIS MEAN?

- If I send you a matrix C=AB encrypted in a Pedersen commitment, it is very hard to decrypt A and B.
- I can, however, prove to you that I know A and B such that AB=C without revealing to you what A and B are.
- We can do this through a very complicated zero-knowledge interactive protocol that was the bulk of my research this summer.

THANK YOU!