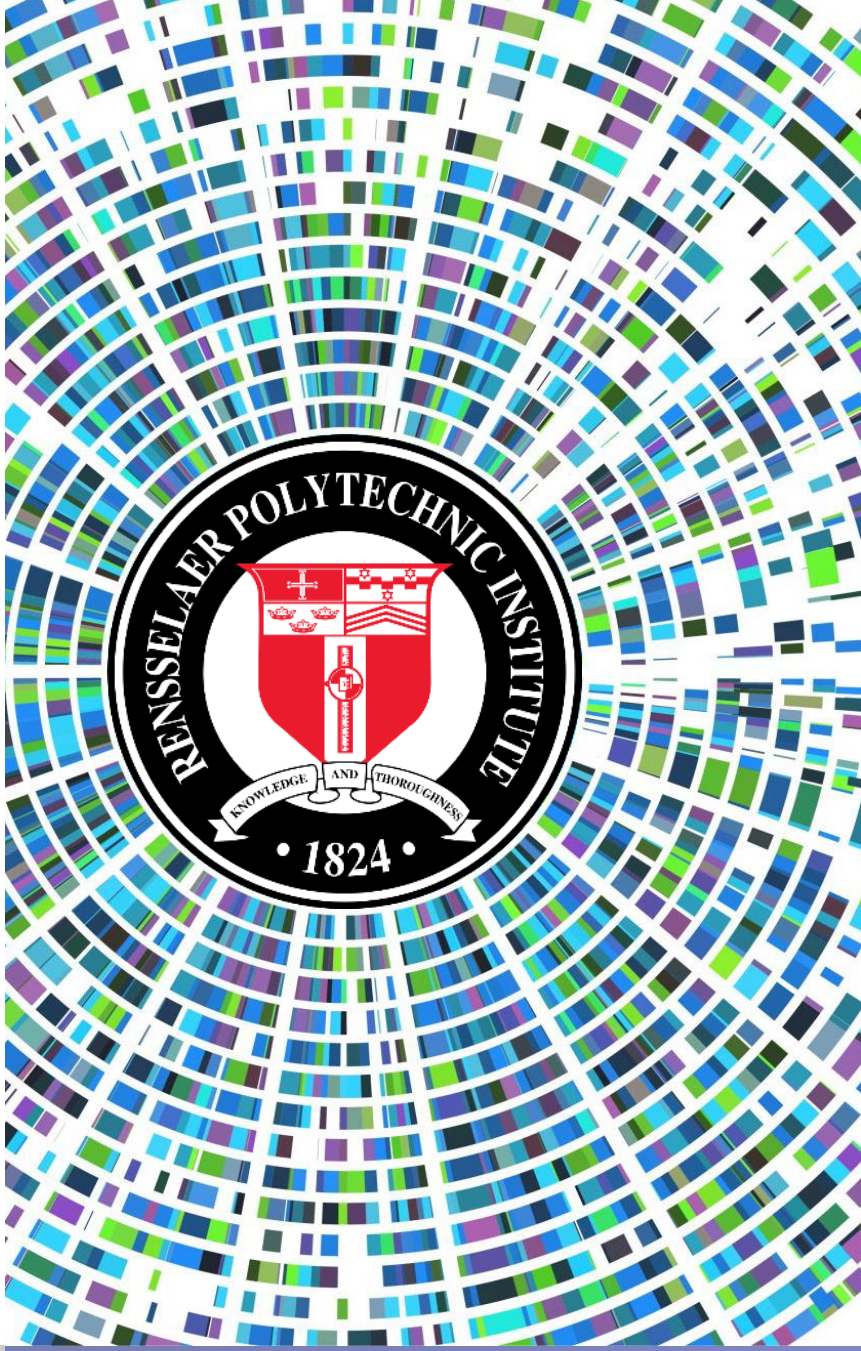
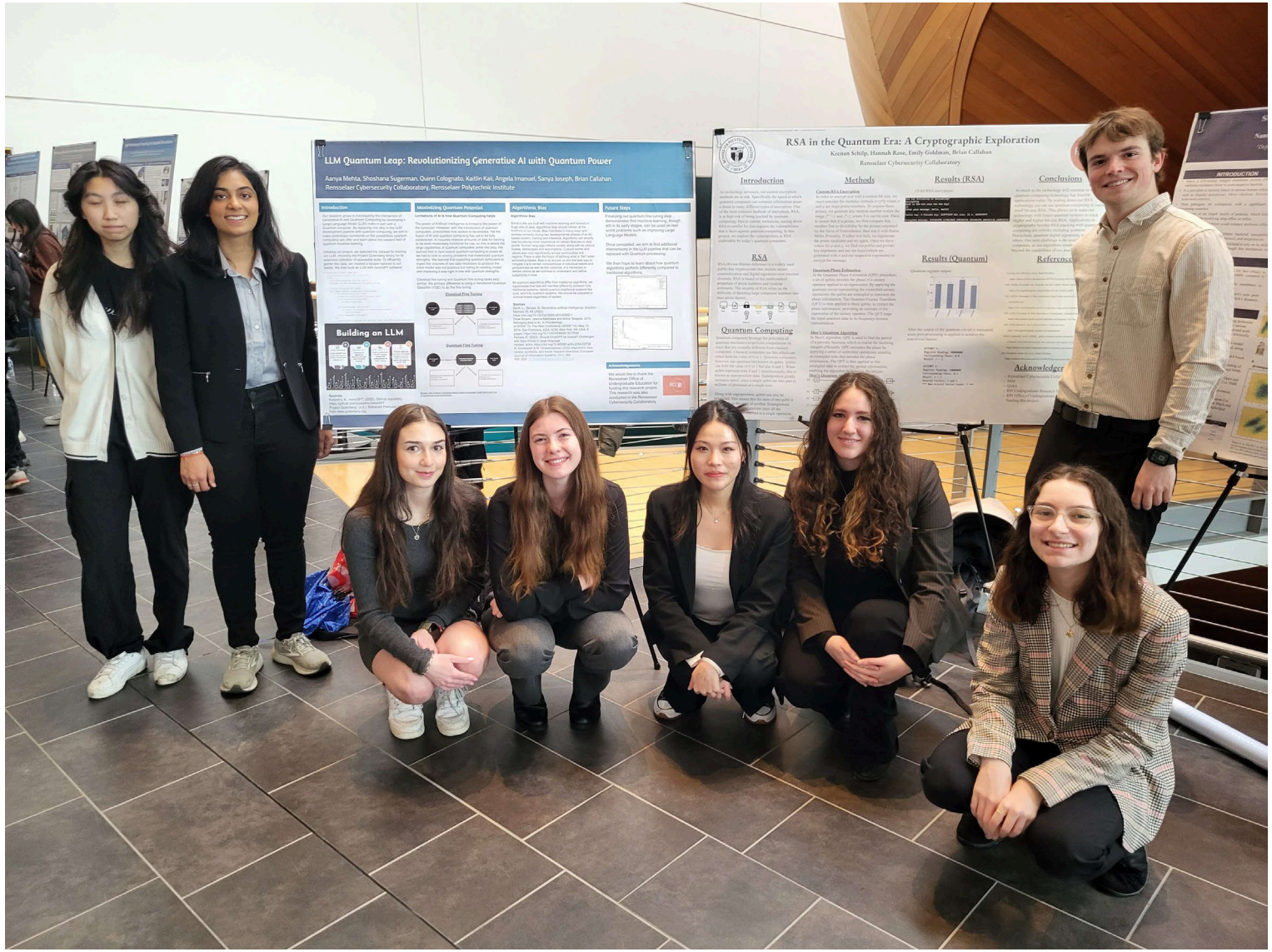
MULTIDISCIPLINARY QUANTUM CYBERSECURITY RESEARCH FOR THE UNDERGRADUATE LABORATORY

- DR. BRIAN CALLAHAN
- KEENAN SCHILP
- QUINN COLOGNATO
- EMILY GOLDMAN
- SHOSHANA SUGERMAN
- AANYA MEHTA
- ANGELA IMANUEL
- KAITLIN KAII
- HANNAH ROSE




RENSSELAER
CYBERSECURITY
COLLABORATORY

MEET THE TEAM



1. OVERVIEW & BACKGROUND
2. CRACKING PSEUDO-RSA
3. QUANTUM ALGORITHMIC BIAS
4. CONCLUSIONS

AGENDA

OVERVIEW & BACKGROUND

ORIGINS OF PROJECTS

CREATING THE TEAMS


IBM
IBM Quantum
System One

CRACKING PSEUDO-RSA

DESIGNING THE EXPERIMENT

EXECUTING THE EXPERIMENT

RESULTS

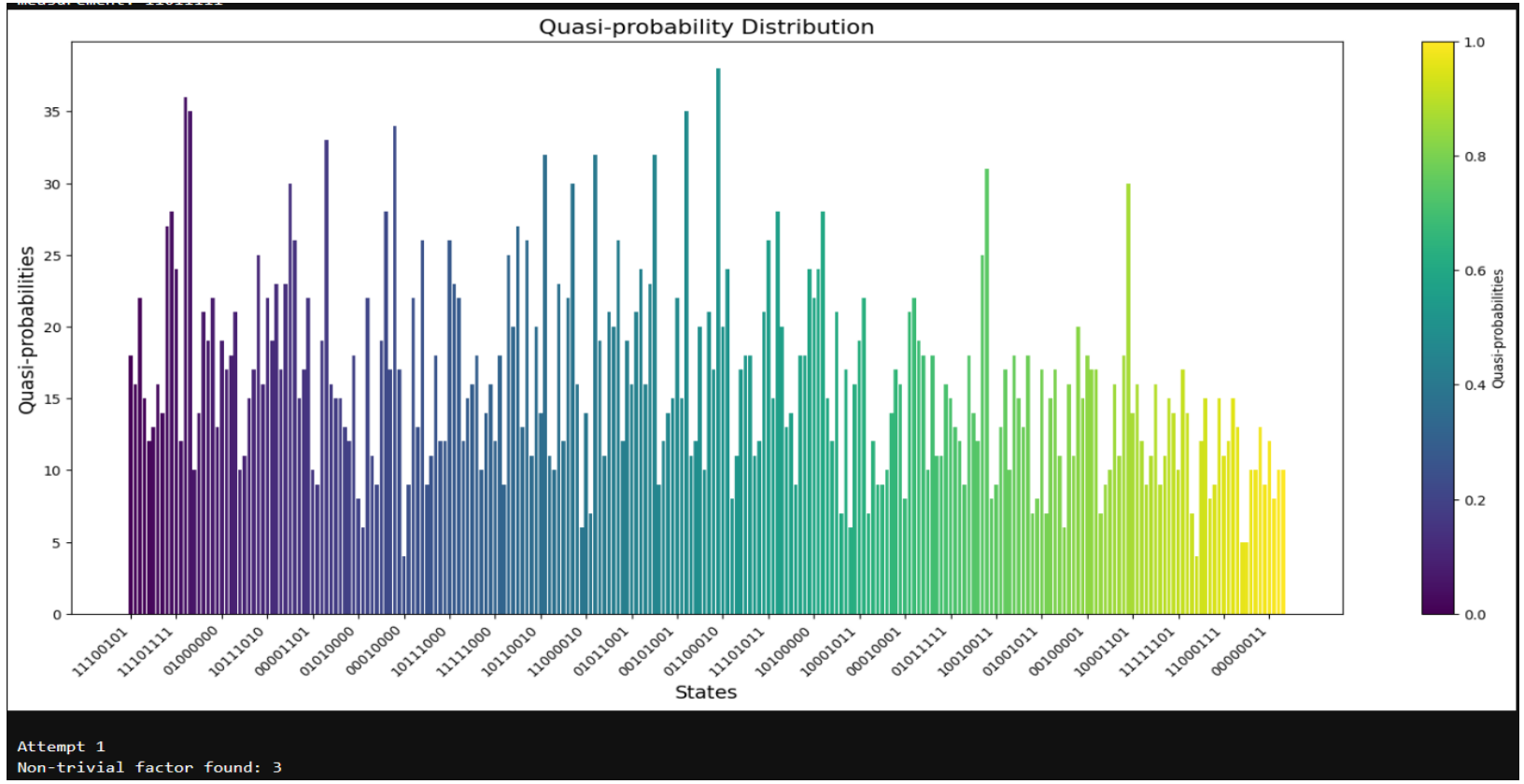
THE PROBLEM

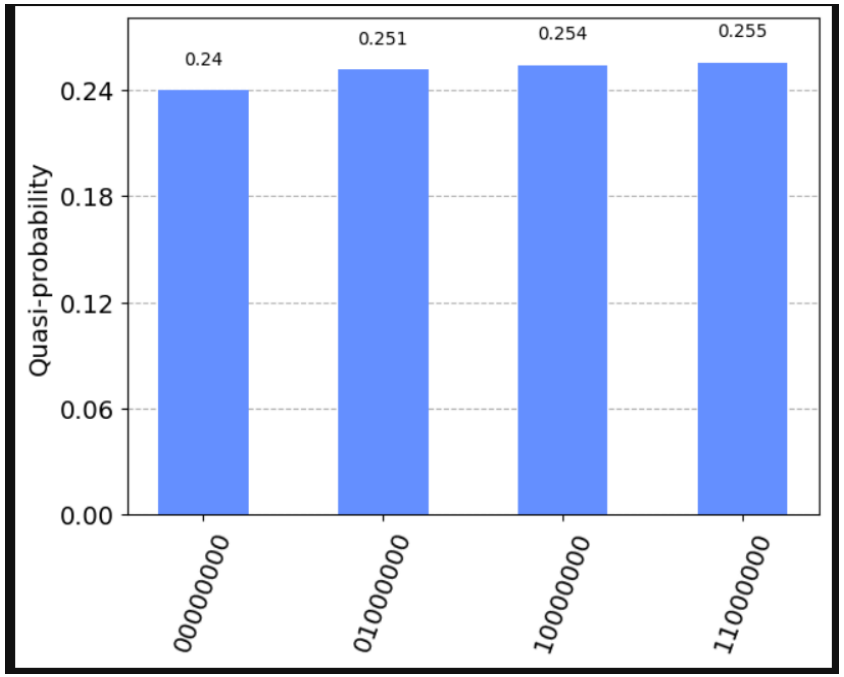
- Quantum computers are expensive!
- They don't have large enough bit-size computers to handle the task of cracking today's in-use RSA
- RPI has a quantum machine, though: how can we utilize it...?
- Enter pseudo-RSA

EXECUTION

- Wrote code for custom bit-size RSA to scale down key size to quantum computation levels applicable for our computer
- Used phase estimation and factoring to crack the RSA key
- Applied classical post-processing to acquire a non-trivial factor of the original "key"

RESULTS


Quasi-probability Distribution
Quasi-probabilities
States
Quasi-probabilities
Attempt 1
Non-trivial factor found: 3


Quasi-probability
0.24
0.251
0.254
0.255
00000000
01000000
10000000
11000000

QUANTUM ALGORITHMIC BIAS

DESIGNING THE EXPERIMENT

EXECUTING THE EXPERIMENT

RESULTS

WHAT IS ALGORITHMIC BIAS?

Our primary focus was to understand the limitations of quantum machine learning in aiding LLM development and refinement.

- LLMs are built with machine learning and trained on huge sets of data and bias can manifest in many ways throughout the developmental process.
- Comparison between quantum algorithmic bias and traditional computing algorithms.
- Occurrence of unfair discrimination against specific groups of people as a result of human influence on design and implementation.

METHOD

Initial experiment, developing LLMs to implement on both quantum and traditional computers

- Our goal was to replace one step in the LLM development pipeline with quantum computing.
- We built our LLM with nanoGPT software using Project Gutenberg books.

Revised experiment, part-of-speech analyzer

- Utilized a part-of-speech recognizer using Qiskit machine learning software.
- Created scripts to assist us with overall process.
- Used fine tuning with VQC to improve our recognizer and analyzed data with graph outputs.

R E S U L T S

- There is potential for quantum algorithms to be susceptible to the same algorithmic bias that is faced by classical algorithms.
- Such issues must be handled now while research in quantum computing is still new.

CONCLUSIONS

RESILIENCY & DIVERSITY

FUTURE DIRECTIONS

MULTIDISCIPLINARY QUANTUM CYBERSECURITY RESEARCH