**BACKGROUND**
- MIT Tech. Rev.: “a quantum computer could break 2048-bit RSA encryption in 8 hours”.
- The Knapsack Problem is a potential basis for making secure quantum cryptosystems.
- The Knapsack Problem (KP):
  - Widely applicable in finance, eCommerce, online trading, material design.
  - The best existing KP solution runs in $O(nW)$ (dynamic programming).
  - Among 75 problems, the KP is the 3rd most in need of improvement.

Grover’s Algorithm:
- A quantum algorithm for efficient searching.
- PSU student Yiwei Li used Grover Search to create an efficient quantum algorithm for the difficult graph coloring problem.

**METHODS**
- Inspired by Yiwei’s graph coloring, I wondered if I could use Grover Search to design a Quantum Knapsack Algorithm (QKA).
- Unlike in existing quantum literature, I also implemented my algorithm and circuits with real gates in Microsoft Q#.

**ORACLE DESIGN**
- My algorithm’s core module was the Knapsack Oracle, a function of quantum gates that allows Grover Search to solve the KP.
- I also had to design custom circuits for necessary arithmetic functions that aren’t yet supported in Q# API.
- The Knapsack Oracle has the function of determining if a combination of box “amounts” satisfies bounds and yields optimal profits.

**TIME AND COST ANALYSIS**
- QKA Time Complexity: $O\left(\frac{n!}{M^{\frac{1}{2}}}\left(b+1\right)^{\frac{1}{2}}\log\left(l/\left(b+1\right)\right)\right)$
- Designed, implemented, and verified first ever quantum algorithm for the KP.
- The QKA yields significant speed-up relative to classical solution algorithms for the KP.
- Analyzed gate cost of Knapsack Oracle, rarely done in existing quantum literature.
- First step in creating quantum-resistant Knapsack cryptosystems in the future.

**CONCLUSION**