Grover's Algorithm:
Single Solution

By Michael Kontz

Application

- Grover's algorithm can identify an item from a list of N elements in $O(\sqrt{N})$
- What's this good for?

Unstructured database search

(virtual database)

  - breaking DES (Data Encryption Standard)
  - SAT (Satisfyability of boolean formula)
  - map coloring with 4 colors

Application: DES

- clear text + key = ciphertext
- “attackatdawn” + 3726495784 = “ojbevjewbvv”

- 56-bit key
- Best classical algorithm $\frac{2^{56}}{2}$
  - 36 quadrillion
- Grover’s algorithm
  - 118 million