Grover's Search (1996): Quadratic Speedup

- **Search space of size 2^n using $2^{(n/2)}$ function evaluations vs. classical $(2^n)/2$**
- **Security implications: 256-bit key for ANY algorithm will have only 128-bit security level**
- **Simulation:**

```
for( iter = 1; iter <= k; ++iter)
{
 // apply f, i.e. flip sign of state m
 //
  q[m] = -q[m];

 // inversion about the average
 //
  avg = 0;  for( i = 0; i < N; ++i) avg += q[i];

  avg *= 2.0/N;  for( i = 0; i < N; ++i) q[i] = avg - q[i];
}
```