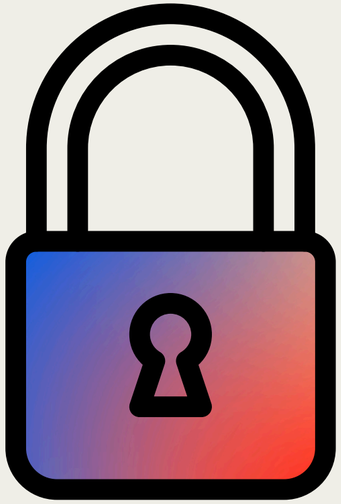
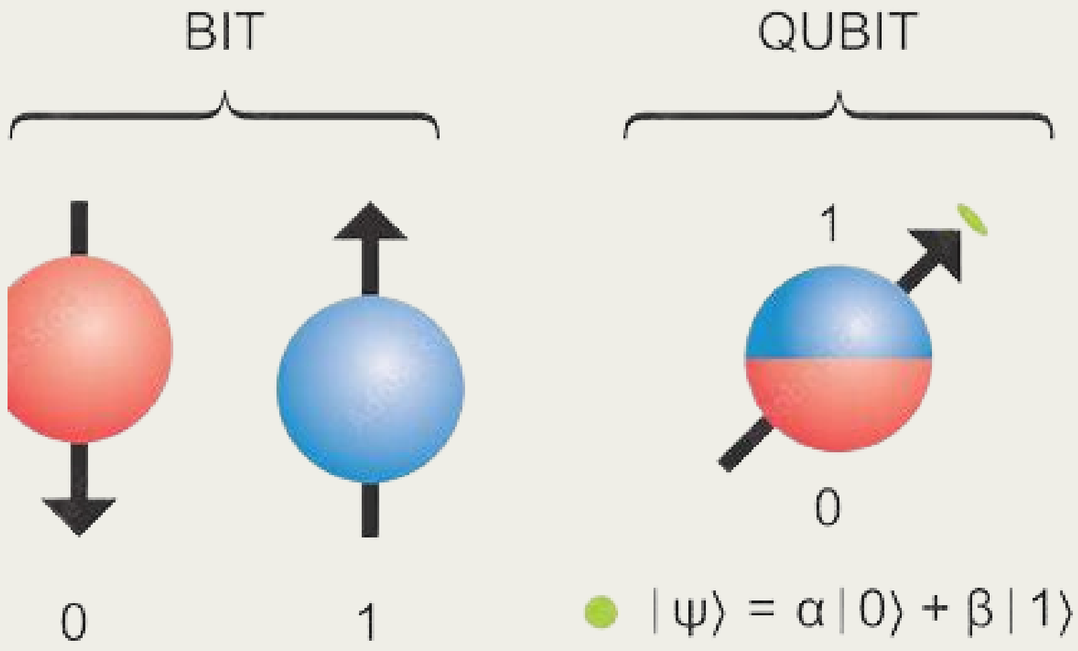
Quantum Resistant Cryptography Toolkit



MILES FRANCK

WHAT IS QUANTUM COMPUTING

- Classical Computers use bits 0 or 1
- Quantum uses qubits
- Qubits allow quantum computers to process vast amounts of information at once

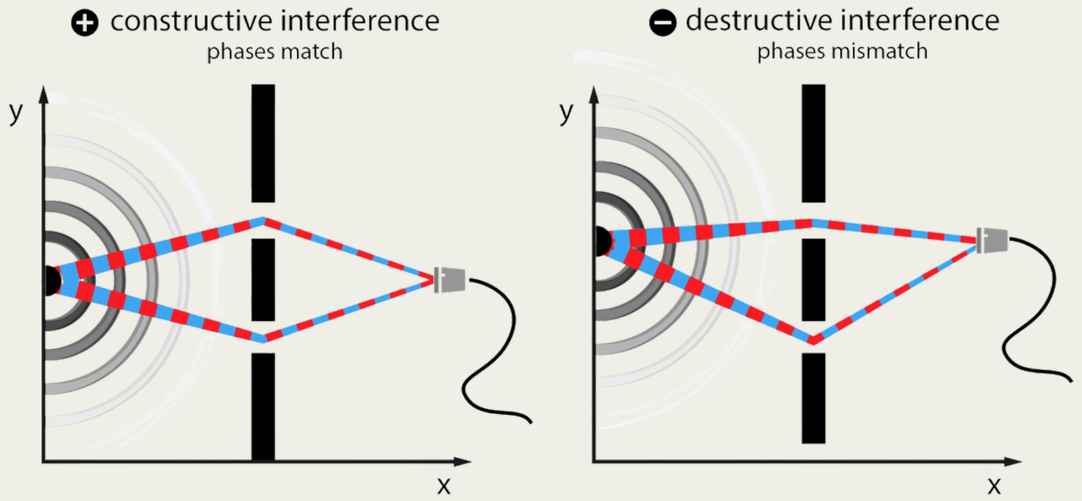


SUPERPOSITION

- Superposition is how you would describe the qubit being 1 and 0 at the same time.
- This allows quantum computers to process multiple possibilities simultaneously.

INTERFERENCE

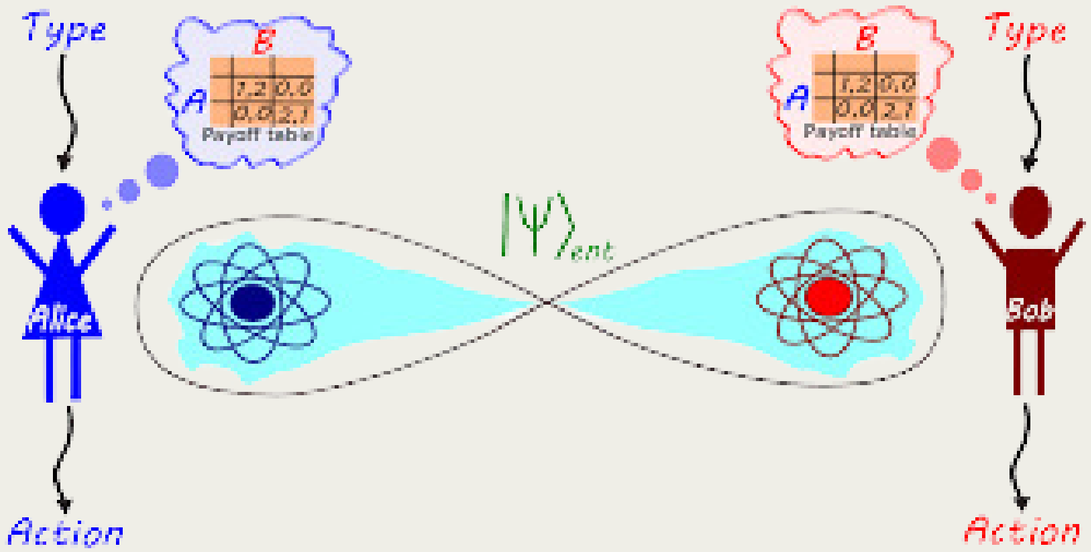
- The probabilities of different outcomes can interfere with each other, either adding up or canceling out
- quantum algorithms can use this interference to amplify the correct solutions and cancel out the wrong ones



ENTANGLEMENT

- When qubits are entangled, the state of one qubit is directly related to the state of another, no matter how far apart they are.

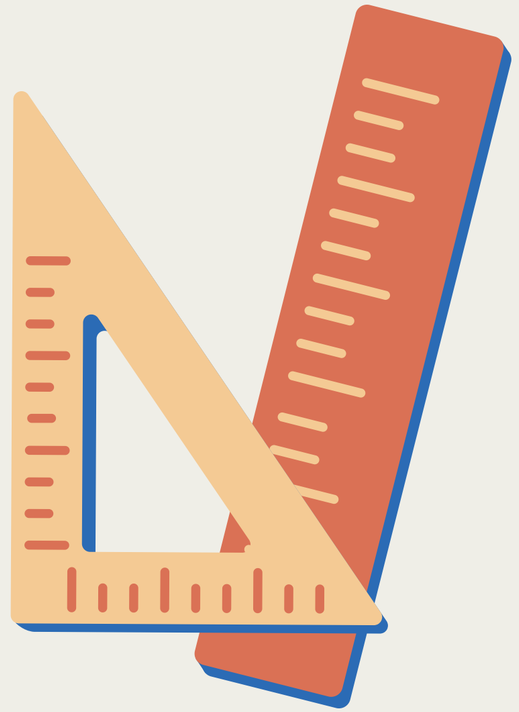
- This lets quantum computers solve complex problems more efficiently by processing multiple calculations in parallel.



MEASUREMENT

- Measurement in quantum computing forces the qubit out of its superposition (where it could be both 0 and 1) into one definite state, either 0 or 1.

- extracts classical information from quantum information



THE ISSUE

Lack of Quantum Algorithm Benchmarking

Quantum technology is advancing rapidly, but there is currently no reliable way to benchmark or test quantum algorithms for performance and efficiency.

Classical Algorithm Vulnerabilities

Classical encryption methods like RSA are increasingly vulnerable to quantum attacks, but we lack tools to measure how susceptible they are.

Need for Future-Proof Testing

As quantum technology progresses, it’s crucial to develop tools that allow us to continuously test and evaluate both classical and quantum algorithms to understand their strength over time

MY SOLUTION

Quantum Toolkit 

Key Features:

Benchmarking Quantum Algorithms: Evaluate performance and efficiency of quantum-resistant algorithms.

Quantum Attack Simulations: Simulate potential quantum attacks on classical systems to assess vulnerabilities.

WHY IT'S IMPORTANT

Evaluate Algorithm Effectiveness

By benchmarking, researchers and organizations can determine which algorithms perform better in terms of security, speed, and resource efficiency, allowing for the optimal choice in future cryptographic systems

Prepare for Quantum Threats

Benchmarking quantum algorithms now ensures we're prepared to replace vulnerable systems with quantum-resistant alternatives before major security breaches occur

Guide Technological Development

Benchmarking helps researchers identify gaps and weaknesses in current quantum algorithms, directing future innovation toward strengthening cryptographic systems and developing more effective solutions to stay ahead of evolving threats

CONCLUSION: SHAPING QUANTUM BENCHMARKING

- A Vision for Benchmarking:
  - This project demonstrates what benchmarking quantum algorithms could look like.

- The Quantum Toolkit:
  - With this tool, researchers, cryptographers, and security professionals will have the ability to test, compare, and better understand the performance and of quantum and classical algorithms, helping them prepare for the quantum era

Thank you!