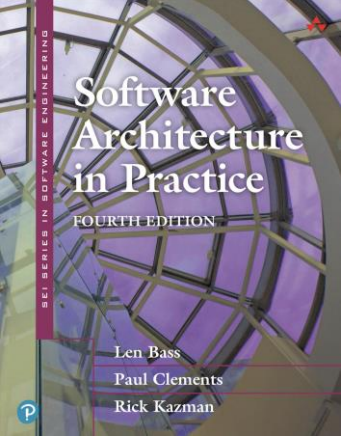
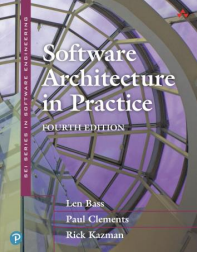


Chapter 26: A Glimpse of the Future: Quantum Computing

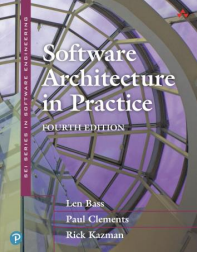
[A quantum computer can be compared] to the airplane the Wright brothers flew at Kitty Hawk in 1903. The Wright Flyer barely got off the ground, but it foretold a revolution.

—wired.com



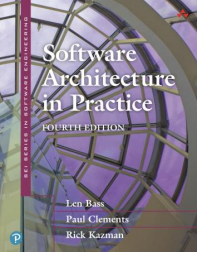
Chapter Outline

- Single Qubit
- Quantum Teleportation
- Quantum Computing and Encryption
- Potential Applications
- Final Thoughts



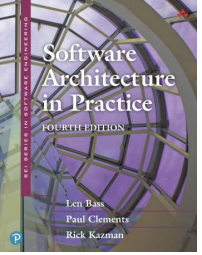
Quantum Computing

- Quantum computers will likely become practical over the next five to ten years.
- Quantum computers are generating interest because of their potential to outperform classical computers.
- They will not replace classical computers; they are good at problems that involve combinatorics and are computationally difficult for classic computers.



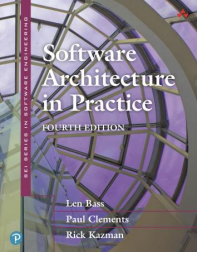
Single Qubit

- The fundamental unit of calculation in a quantum computer is a unit of quantum information called a qubit.
- A quantum computer manipulates qubits.



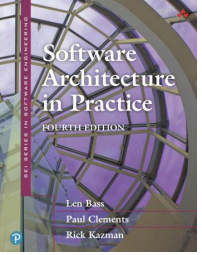
Single Qubit

- A qubit is characterized by three numbers. Two of these are probabilities:
  - the probability that a measurement will deliver 1 and
  - the probability that a measurement will deliver 0.
  - the third number, called the phase, describes a rotation of the qubit.
- A measurement of a qubit will return either a 0 or a 1 (with probabilities as designated) and will destroy the current value of the qubit and replace it with the value that it returned.
- A qubit with non-zero probabilities for both 0 and 1 is said to be in superposition.



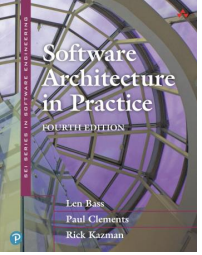
Single Qubit

- Entanglement is a key element of quantum computing. It has no analog in classical computing.
- Two qubits are “entangled” if, when measured, the second qubit measurement matches the measurement of the first.
- Entanglement can occur no matter the amount of time between the two measurements, or the physical distance between the qubits.
- This leads us to quantum teleportation.



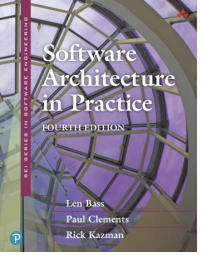
Quantum Teleportation

- If we want to copy one qubit to another we must accept the destruction of the state of the original qubit.
- The recipient qubit will have the same state as the original, destroyed qubit.
- *Quantum teleportation* is the name given to this copying of the state.



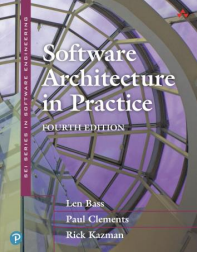
Quantum Teleportation

- There is no requirement that the original qubit and the recipient qubit have any physical relationship.
- In consequence, it is possible to transfer information over great distances between qubits.
- The teleportation of the state of a qubit depends on entanglement.



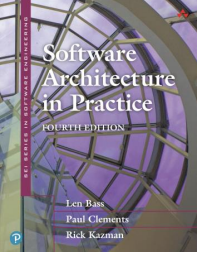
Quantum Teleportation

- This is inherently secure.
- Because two qubits "communicate" through entanglement, they are not physically sent over a communication line.



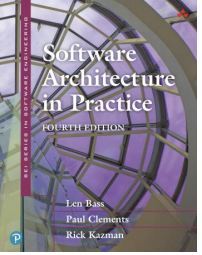
Quantum Computing and Encryption

- Quantum computers are extremely proficient at calculating the inverse of a function—in particular, the inverse of a hash function.
- This kind of calculation is useful in decrypting passwords.
- This makes an enormous amount of password-protected material, previously thought to be secure, quite vulnerable.
- Shor's algorithm is a quantum algorithm that can factor two primes, *p* and *q* with running time on the order of log (number of bits in *p* and *q*).



Potential Applications

- IBM is focusing on cybersecurity, drug development, financial modeling, better batteries, cleaner fertilization, traffic optimization, weather forecasting and climate change, and artificial intelligence and machine learning.
- To date, except for cybersecurity, this list of potential quantum computing applications remains mostly speculation.



Final Thoughts

- Quantum computers are in their infancy.
- Applications for such computers are mostly speculation at this point.
- Nonetheless, progress is happening rapidly. If Moore's law applies to quantum computers, then the number of qubits available will grow exponentially over time.
- So … stay tuned!