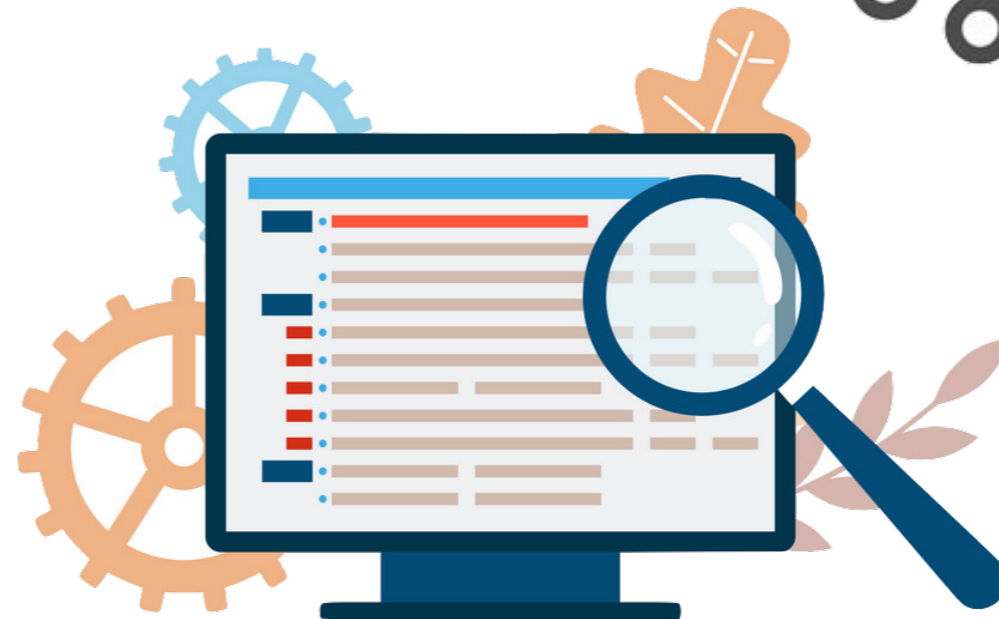
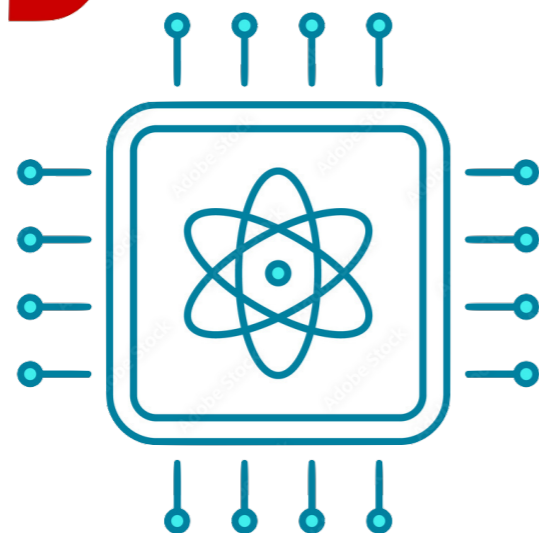
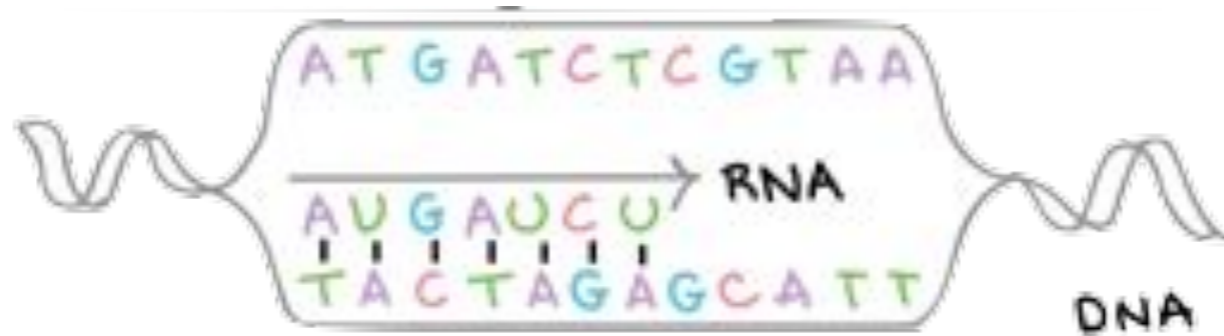


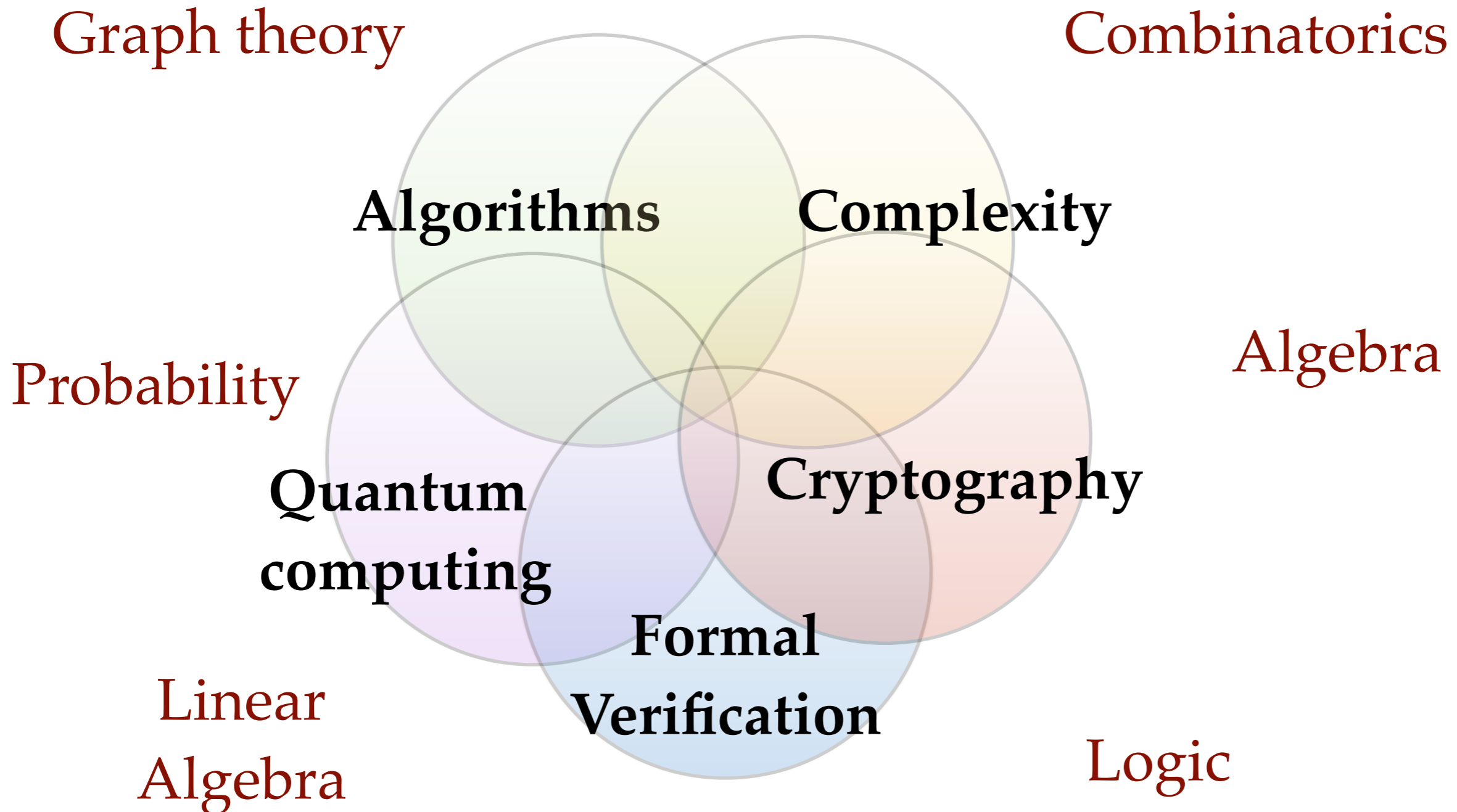
# ACM ROCS 2024

Algorithms:

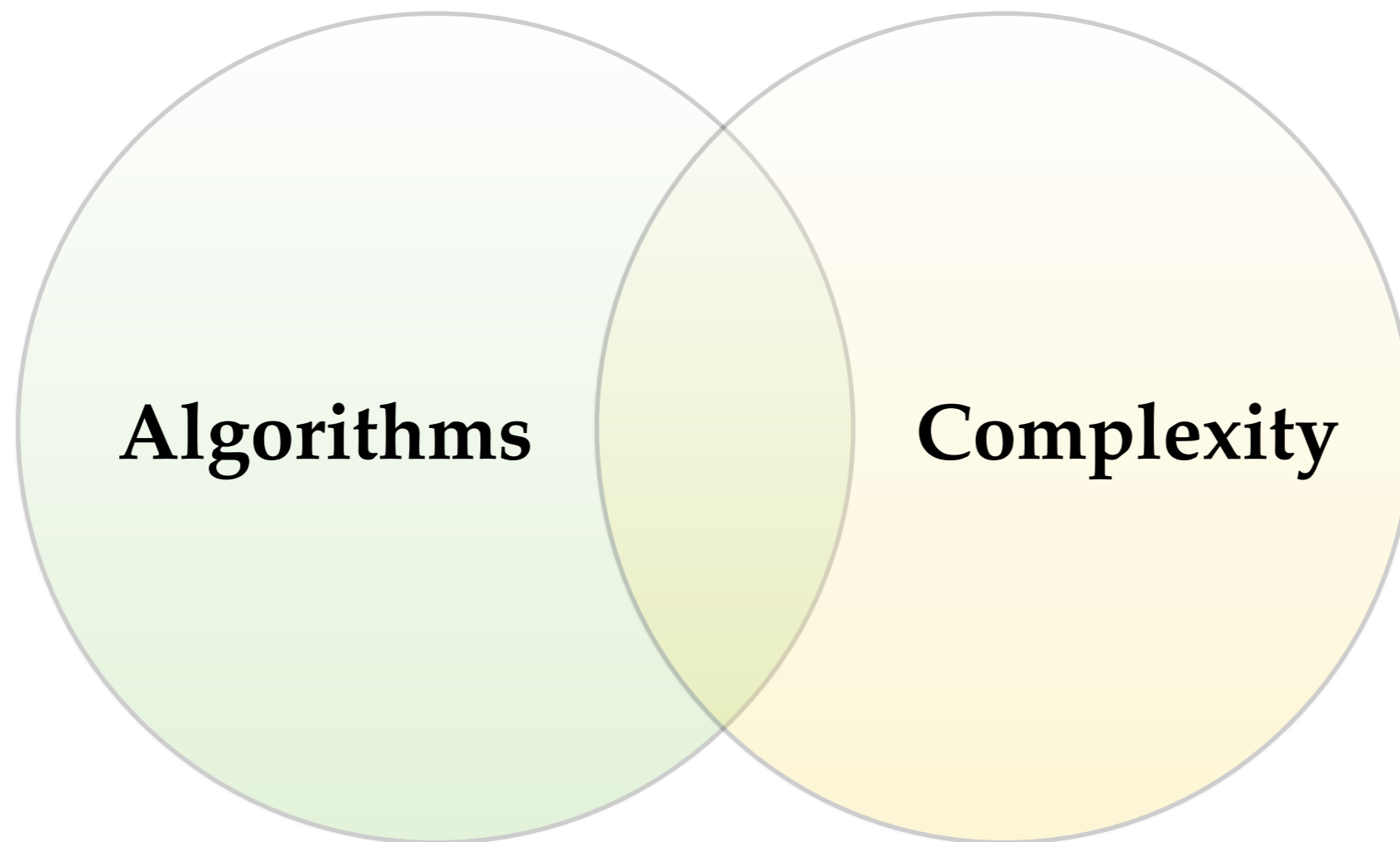
Easy, hard and everything in between



# Theory of Computation



# Theory of Computation



# Integer multiplication and factoring

- How much time does it take to multiply two 100 digit integers?
- Less than a second
- Finding factors of a 200 digit integer?
- Within seconds or many years?
- **Naive method:** try dividing by all smaller numbers
  - $10^{100}$  numbers to try
  - Number of atoms on earth  $\sim 10^{50}$
  - Amount of energy received from sun  $\sim 10^{30}$  Joules

# Integer multiplication and factoring

- Faster methods to factor integers?
- **[2019]** Factored a 240-digit number using 900 core-years of computing
- How about factoring 1000-digit number?
  - A million years
  - It's possible that tomorrow a clever idea comes and makes it possible in a few seconds
- All internet security, e-commerce, secure messaging depends on the assumption that it takes million years
- **Twist:** a quantum computer could possibly do it in seconds

# DNA sequence matching

cow	ATG---	ACTAACATT	CGAAAGT	CCCACCC	ACTAATA	AAAAATT	GTAAC
sheep	ATG---	ATCAACAT	CCGAAAA	ACCACCC	ACTAATA	AAAAATT	GTAAC
goat	ATG---	ACCAACAT	CCGAAAG	ACCACCC	ATTAATA	AAAAATT	GTAAC
horse	ATG---	ACAAACAT	CCGGAAT	CTCACCC	ACTAATT	AAAAAT	CATCAAT

- Identifying regions of similarities in two sequences
- To find evolutionary, functional, or structural relationships
- Can be up to 500 million characters long
- **Key challenge:** linear time algorithms

# QR codes



- Can be read, even when partially erased
- Can correct up to 30% errors
- It is not simply duplication of data.
- **Coding theory:** algebra and geometry


# Theory of Computation



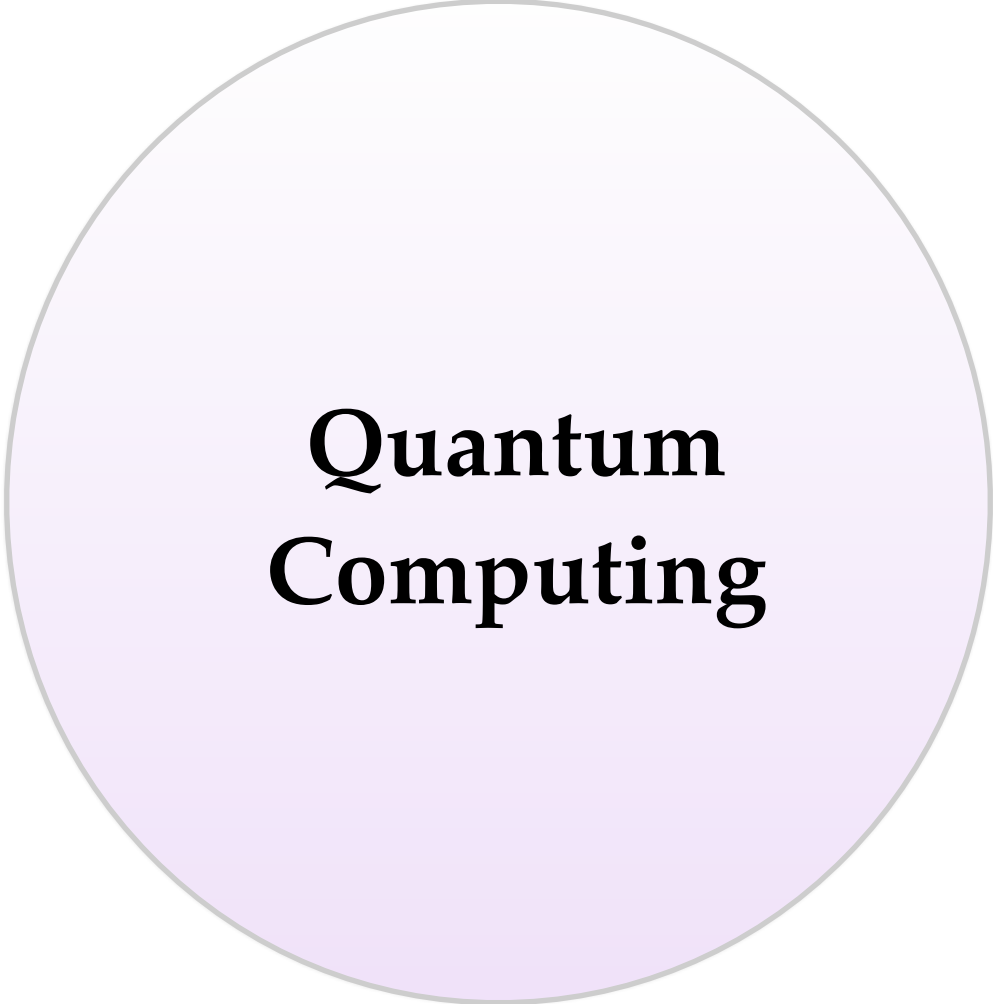
**Cryptography**



# Cryptography

- Secure payments, messaging etc.
-  End-to-end encryption
- No one can decode your messages other than your friend
- Not even the internet provider, or WhatsApp.
- Everyone has a secret key that never travels out of one's phone
- Public key cryptography (uses algebra)

# Theory of Computation



**Quantum  
Computing**

# Quantum Computing

- Classical computers use bit operations at the lowest level: AND, OR etc.
- All programs you can write are converted into a sequence of bit operations
- Can you program to simulate any physical process?
- Approximately yes.
- Even with randomness, yes.
- But, what about quantum processes.

# Quantum Computing

- Can you write a program to simulate quantum processes?
- It seems quantum mechanical phenomena are fundamentally different
- Quantum computers were proposed to simulate quantum processes
- In addition to bits, they have qubits (quantum states)
- **Twist:** Theoretically, there is a fast algorithm for factoring integers on a quantum computer
- More interest generated due to potential of breaking widely used crypto systems

# Quantum Computing

- Theory part: linear algebra and classical algorithm design
- Building quantum computers: quantum physics
- **Fun fact:** you can do quantum computing, without knowing much about quantum physics

# Theory of Computation



**Formal  
Verification**

# Formal verification

- Correctness of a program or system
- Exhaustive and comprehensive guarantees that systems are bug free
- Model checking: whether a system satisfies certain desired properties?
- **Tools:** Automata theory and Logic
- Efficiency of verification algorithms

# Common theme

- Provable guarantees
- Mathematical foundations
- Efficiency
- Resources: time, memory, information, communication, randomness etc.



# Active research groups

- TIFR Mumbai
- Chennai Mathematical Institute (CMI)
- Institute of Math Science, Chennai
- IIT Bombay, IIT Delhi, IIT Kanpur, IIT Kharagpur, IIT Madras, IIT Hyderabad, IIT Gandhinagar
- And many others.
- **Top conferences:** STOC, FOCS, SODA, CCC, ICALP, SOCG, LICS, TCC, EUROCRYPT, ITCS, CAV, ICLA

# Job Opportunities

- Academia
- Intel, TCS, Microsoft, IBM, Google, Mathworks, Starkware, Autocad
- Within theory, some areas are better suited to industry than others.