CPE5021
Advanced Network Security

Cryptography with Quantum Computing and Quantum Cryptography ---

Lecture 9

Purpose of the Lecture

- The main aims of this lecture are the discussion of the following things:
  - Will there be very fast computers which can be used to break all current crypto algorithms with a feasible amount of time?
  - Is there any technology that will allow us to secure our communications no matter how fast future computers will be and how good crypto cracking techniques will be?

Reasons for this Lecture

- If there will be affordable computers that are 10^10 or more times faster than the present fast computers, what will happen to our computing communications?
  - we will definitely have to shutdown most of our wireless computing communications and certain parts of wired computing networks. More seriously the Internet may have to be shutdown.

(Test Tube computers can complete tasks which require a conventional computer millions of years in a few days. http://www.research.ibm.com/resources/news/20011219_quantum.shtml)

Reasons for this Lecture

- Is there any technology that will allow us to secure our communications no matter how fast future computers will be and how good crypto cracking techniques will be.
  - If there will be such a technology, then
    - depending on the technology, part of our networks may survive. Eg. Wired networks
    - The nature of wireless networks is harder to protect so it is probably we will it hard to protect wireless networks.

Quantum Computers

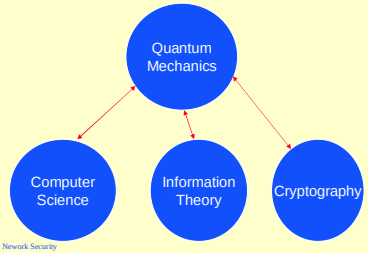
- Ion Trap (NIST Ion Storage Group)
  (http://www.boulder.nist.gov/timefreq/ion/index.htm)
- Quantum ElectroDynamics : Cavity QED
  (http://www.lkb.ens.fr/recherche/qedcav/english/englishframes.html)
- Test Tube Quantum Computer
  (http://www.research.ibm.com/resources/news/20011219_quantum.shtml)
- Molecular Quantum Computer
  (http://www.qcaustralia.org/crp_mm.htm)

Benefits of Quantum Computers

- Solve very complex problems which require thousands or millions of number) years of current conventional computers.
  - Factorisation problem.
  - Problems that employ artificial intelligence.
- Validate many complex algorithms.
  - Machine learning.
  - Computer vision.
- Provide powerful tools for safety and security
  - Face recognition.
  - Used to predict natural disasters.
  - Weather forecast.

QC and Its Applications

- Study of QC will provide significant information about computer Science, Information Theory and Cryptography.



Quantum Cryptography

- Needed for privacy in the possibility of unlimited computing power.
- Current cryptographic schemes, symmetric or private key crypto based on unproven mathematical principles like the existence of a practical trapdoor function.
- Shor's quantum factoring algorithm using nuclear magnetic resonance could break RSA in polynomial time (Letters to Nature 414, pp 883-887, Dec 2001).
- Quantum cryptography is realisable with current technology (Design and Implementation of Small Quantum Circuits and Algorithms – Cambridge University, June 2003) .

Quantum Cryptography

- main point is the Key Distribution
- Protected by the laws of physics
- Key is transmitted over a private channel
- Correct measurements are combined into the Key
- Eavesdroppers are always detected

QCrypt- Basic Protocol

- Alice sends random sequence of 4 types of polarized photons over the *quantum channel*: horizontal, vertical, right-circular, left-circular
- Bob measures each in a random basis
- After full sequence, Bob tells Alice the bases he used over the *public channel*
- Alice informs Bob which bases were correct
- Alice and Bob discard the data from incorrectly measured photons
- The polarization data is converted to a bit string (↔ = ↶ = 0 and ↕ = ↷ = 1)

Basic Protocol Example

QCrypt - Commercial Products

- id Quantique (Swiss company - Genève)
  - QKD prototype
- MagiQ (Company with headquarter in New York/USA)
  - Has unveiled the first commercial QKD-system

Possible Applications

- Provides absolute security where it is needed.

  For example:
  - Financial institutions and trading exchanges
    - QKD can secure most critical communications
  - Storage area networks
    - Transfer of know how
  - Ultra secure point-to-point links
    - Generally where a high secure point-to-point communication is needed

Quantum Cryptography Benefits

- Provides Perfectly Secure Communications
  - absolutely secure transmission of cryptographic keys, even against quantum computers
  - any eavesdropping of key transmission is demonstrably detectable (man in middle attacks, etc.)
  - security based on inviolability of facts of physics and natural law

Technical Challenges

- Distance limitation
  - Qubit are encoded into photons
  - Optical fibres are used to transmit photons
  - Losses along the fibre
  - No amplifiers (destroy the qubit state)
  - Distance is limited to tens of kilometres

Technical Challenges

- Single photon source
  - Problems through insufficiency of photon source
  - Leads into a low data rate
  - Data rate depends on the distance between sender and receiver
  - but feasible with current technology
  - Single photon source will increase the performance of QKD