Integrating Quantum Concepts into Cyber Security

Session 1: Introduction

Dr William Joseph Spring

ACSAC 35, Condado Plaza Hilton, San Juan, Puerto Rico, USA

9th – 13th December 2019

Introduction

This set of presentations will include

- Introduction and Overview
- Classical and Quantum Networks
- Algorithms
- A selection of Attack vectors and their Defence

Introduction

- The potential for realizing quantum-based networks and distributed systems has now been realized through reports of networks in excess of 2000km and commercial quantum based private communication networks reported as complete.
- Quantum based cloud services are now under development on a commercial basis and a quantum-based internet is proposed for the future.
- Associated with these and other developments in for example:
  - types of computer
  - programming paradigms
  - operating systems
  - event ordering

  issues emerge as new quantum concepts are integrated into the cybersecurity landscape.

Introduction

- In this workshop, aimed primarily at researchers new to quantum concepts, we consider a range of underlying concepts employed in the development of ‘secure’ systems for both classical and quantum-based networks and distributed systems.
- From a quantum perspective we will discuss
  - different types of qubit, qudits, superposition
  - discrete and continuous states
  - mixed states
  - multipartite states
  - entanglement,
  - gates
  - measurement

  and their incorporation into the cybersecurity environment.

Introduction

- Research in quantum distributed systems and networks is now said to be in its second wave developing the potential for applications in, for example
  - satellite communication
  - quantum-based resources
  - secure communication
  - …
- We compare and contrast classical and quantum communication systems with a view to:
  - identifying similarities and differences that exist between the two
  - to present a selection of advantages and disadvantages in employing such paradigms
  - to consider a selection of vulnerabilities from each, within for example an attacker defender perspective.
- From a hands on perspective, we seek to present a selection of activities that participants can engage in, in order to develop and extend their understanding in working with quantum systems.

Cyber Security

- Assets
- Motivation
- Attackers and Vulnerabilities

Cyber security

"the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide"

M. Gasser, 1988, Building a secure computer system, van Nostrand Reinhold.

Information security – "the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information"

Assets

- Hardware
  - Servers
  - Switches
  - Sensors
- Software
  - Mission critical applications
  - Support systems
- Confidential data
  - Genome data
  - Medical records
- Assets need to be protected if replacement is expensive or if the asset is important to the owner. Sensors, for example, may be inexpensive but in mission critical systems damage due to not protecting them may be very costly

Motivation

- Motivating factors for using such assets include
  - Sharing of resources
  - Reduction in cost
  - Increase in computational processing
  - Reliability
- With threat modelling for such systems we seek to establish:
  - What data do we need/want to protect
  - Where are the information flows
  - What functions are engaged in the processing of data through the employment of services
    - Cloud services
    - conveyance of packets
  - What systems do I have to rely upon
- ‘Assets should be protected from unwanted access, use, disclosure, alteration, destruction and/or theft resulting in loss to the organisation be it actual or in terms of reputation’ Wiki

Attackers and Vulnerabilities

- Attacks can take various forms:
  - Denial of Service
  - Malware
  - Phishing
  - Session hijack
  - Man in the middle
  - Insider attacks
- Are these applicable to quantum networks?

Cyber security

Naturally following from the previous statements we meet the following concepts:

- Authentication
  - Establishing for example that I am who I say that I am and that I am entitled to gain access to some entity such as my computer
- Confidentiality
  - Any data sent between two parties is not seen by unauthorised observers
- Integrity
  - Establishing that the message sent is the same as the message received
- Non repudiation
  - Ensuring that the sender of some information cannot deny that they sent the information
- Accessibility
  - If I am entitled for example to use a service then I want to be able to do so
- Anonymity
  - In for example voting schemes where one might also like confidentiality

One tool that is often quite useful is cryptography

Protection

Central to the protection of for example networks we have a need for:

- Physical Security
  - For example if I have a communication system reliant upon satellites being in certain positions and or uncompromised I have to ensure that these requirements are met or quickly reinstated
- Trust
  - I have to trust those that can access my systems generally in a covert way, for example who is updating my computer system
- Cryptography
  - A long standing tool in maintaining a degree of control and defence of information systems
- Protocols
  - The way in which we process data matters

Quantum Processing and Tools

Quantum Processing

- Quantum processing promises the possibility for obtaining solutions to a range of ‘difficult’ problems.
- From a security perspective this involves the possibility for
  - Breaking Asymmetric Key Algorithms via Shor’s Algorithm
    - The RSA algorithm based on the IFP (Integer Factorisation Problem)
    - The El Gamal algorithms based on the DLP (Discrete Logarithm Problem)
  - Obtaining secure communication channels for ‘free’
  - Authentication, confidentiality, integrity, …
  - Employing quantum based encryption schemes
  - Detecting eavesdroppers on a channel
  - Detecting intruders in a system
  - Developing new applications in a range of different fields

Quantum Tools

The tools employed include and are not limited to

- Superposition
- Entanglement
- Error Correction
- Entanglement Swapping
- Teleportation
- Flying and Stationary Qubits
- Parallelism
- Interference

A Comparison of Classical and Quantum States

Classical & Quantum Representations

Classical

- Bits, nibbles, bytes, ….
  - 0’s and 1’s aka cbits
  - 4 bits and 8 bits, …
- Communication of information is achieved via binary bits (cbits) which are grouped into manageable chunks
- Information is processed using gates and communication channels

Quantum

- Quantum bits are used, referred to as qubits, which may be organised into manageable chunks via tensor products
- Information may be encoded using a superposition of quantum bits, (qubits) and organised via the use of tensor products
- Information is processed using gates and communication channels

Classical & Quantum Representations

Classical

- Bits, nibbles, bytes, ….
  - Classical bits (cbits) are scalars
- Examples of gates: logic gates
  - NOT
  - AND
  - OR
  - NOR
  - NAND
  - XOR

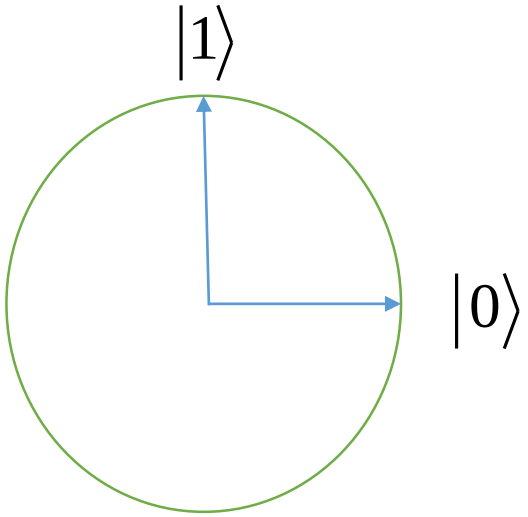
Quantum

- Quantum bits (qubits) are vectors they have magnitude and direction, magnitude = 1
- qubits have 2 degrees of freedom (think of as movement in the x direction and movement in the y direction
- Examples of gates: Matrices
- Pauli gates, Hadamard gate, CNOT gate, Phase gate, …

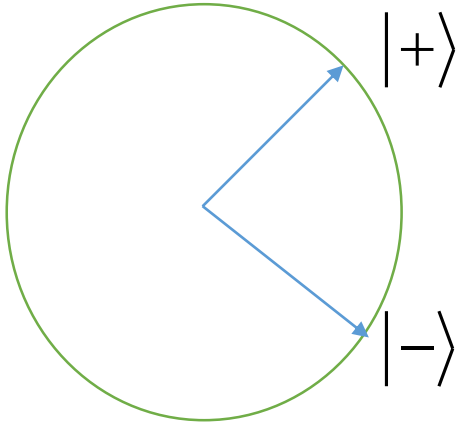
Quantum States

Standard cbits are represented as vectors in a Hilbert Space:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ referred to as the } Z \text{ basis}$$



$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ and } |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \text{ referred to as the } X \text{ basis}$$



Quantum States

Superposition

From the Z basis $\{|0\rangle, |1\rangle\}$ (or the X basis $\{|+\rangle, |-\rangle\}$) qubits are formed as a superposition of their basis vectors

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ with } |\alpha|^2 + |\beta|^2 = 1 \text{ and } \alpha, \beta \in \mathbb{C}$$

or similarly we can express qubits in the X basis

$$|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} \alpha' + \beta' \\ \alpha' - \beta' \end{bmatrix} \text{ (in terms of the Z basis) with } |\alpha'|^2 + |\beta'|^2 = 1$$

and $\alpha', \beta' \in \mathbb{C}$

Postulate 1

State Space

- Associated to any isolated physical system is a complex Hilbert Space (a complex vector space with inner product) known as the state space of the system. The system is completely described by its *state vector*, which is a unit vector in the systems state space

Nielsen and Chuang, Quantum Computation and Quantum Information, CUP, 2000/2010

Quantum States

Superposition

Qubits also have operator representations called density operators

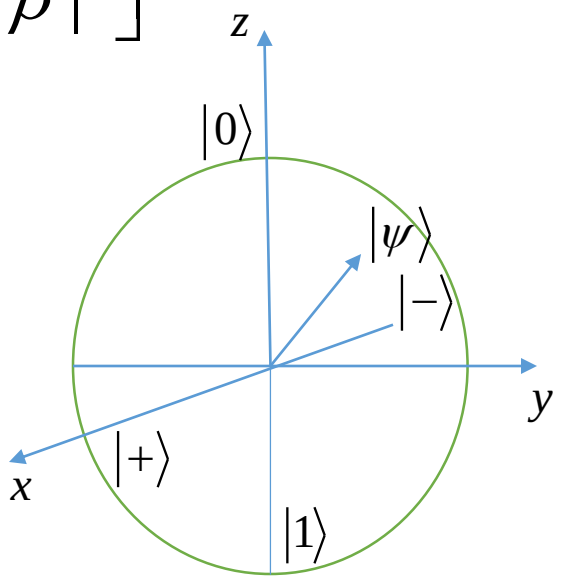
$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\overline{\beta} \\ \overline{\alpha\overline{\beta}} & |\beta|^2 \end{bmatrix}$$

and Bloch Sphere representations in 3d space

- Pure states $|\psi\rangle$ map to the surface
- Mixed states

  $\rho = \sum \rho_i$ with pure states $\rho_i = |\psi_i\rangle\langle\psi_i|$

  map to the interior of the Bloch Sphere
- Mixed states are Hyperbolic space objects



Ungar, A. (2002) The Hyperbolic Geometric Structure of the Density Matrix for Mixed State Qubits. Found. of Phys. **32, 11**

Pure States and Mixed States

Given an ensemble of quantum states we may obtain an overall quantum state

$$\varphi = \sum_{i=1}^{n} p_i \varphi_i \text{ in which each } \varphi_i \text{ is a pure state}$$

A state is said to be pure if and only if the trace of φ^2 is 1 and mixed if the trace of φ^2 lies strictly between 0 and 1

$$tr(\varphi^2) = 1 \text{ for a pure state}$$

$$0 < tr(\varphi^2) < 1 \text{ for a mixed state}$$

Note that the trace of a quantum state is 1: $tr(\varphi) = 1$

Postulate 4 – Composite Systems

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is

$$\bigotimes_{i=1}^{n} |\psi_i\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \ldots \ldots \otimes |\psi_n\rangle$$

Nielsen and Chuang, Quantum Computation and Quantum Information, CUP, 2000/2010

Quantum States

For multipartite states we use tensor products to obtain vectors of the form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \ldots \otimes |\psi_n\rangle = |\psi_1\rangle|\psi_2\rangle|\psi_3\rangle \ldots |\psi_n\rangle = |\psi_1 \ \psi_2 \ \psi_3 \ \ldots \ \psi_n\rangle$$

With corresponding density operators

$$\rho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \ldots \otimes \rho_n = \rho_1 \ \rho_2 \ \rho_3 \ \ldots \rho_n$$

In which

$$|\psi_i\rangle \text{ denotes a qubit and } \rho_i = |\psi_i\rangle\langle\psi_i|$$

This leads us to the concept of entanglement, a major resource in QIP (Quantum Information Processing)

Entanglement

Two fundamental views

- Algebraically no common vector factors, irreducible, prime states
- Correlation View – Entangled photons are seen to be correlated or anti-correlated (both spin up or both spin down as opposed to one spin up and the other spin down)
- Examples:
  - Bell states, GHZ states, W states

$$\left|\beta_{00}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$$

- Partial entanglement for subsystems of a general system also used

Entanglement

From an algebraic perspective entangled states and primes share a common property in that their status is dependent upon the space in which they are perceived to belong.

For example

$$17 = (4+i)(4-i) \text{ is prime over } \mathbb{Z} \text{ but not over } \mathbb{Z}(i)$$

$$x^2 + 1 \text{ is irreducible over } \mathbb{R}[\mathrm{x}] \text{ but not over } \mathbb{C}[\mathrm{x}]$$

Entanglement

Local and Global Operators

Likewise Bell states $\left(\text{for example}\right)$, are said to be entangled provided that they are restricted to the local action of operators from $B(H) \otimes B(H), H$ a qubit space, however if we extend the operator space to $\mathrm{B}(H \otimes H)$ then the Bell states are said to be separable.

It is the potential for access to global operators that characterises a state as either entangled or separable

Gates

The Action of a Matrix on a vector

Matrices: A 2x2 matrix, (2 rows and 2 columns

Example: Let $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $|\psi\rangle=\begin{bmatrix} x \\ y \end{bmatrix}$, then the action of A on $|\psi\rangle$ is defined to be:

$$A|\psi\rangle=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} ax+by \\ cx+dy \end{bmatrix} \quad \text{(definition)}$$

Quantum Gates

In order to describe the development and change of a state we employ gates/operators. Central to our discussions will be the Pauli Gates

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_1 = \sigma_X = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

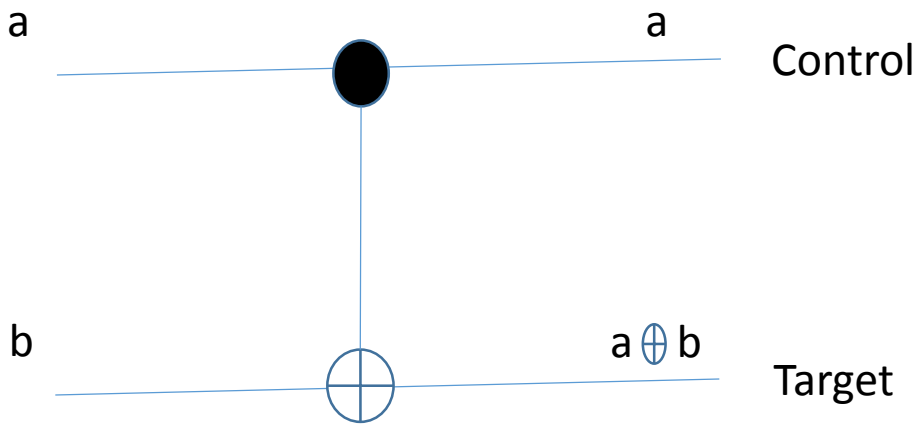
$$\sigma_2 = \sigma_Y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ with } i = \sqrt{-1}$$

$$\sigma_3 = \sigma_Z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Quantum Gates

The CNOT Gate (controlled NOT gate)

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \underbrace{|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 3| + |3\rangle\langle 2|}_{\text{Dirac Notation}}$$



a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Quantum Gates

The Hadamard Gate

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Note: $$|0\rangle \overset{H}{\mapsto} |+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{H}{\mapsto} |0\rangle$$

and $$|1\rangle \overset{H}{\mapsto} |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \overset{H}{\mapsto} |1\rangle$$

Quantum Gates

The Phase Gate

$$P_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$$

In which

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto e^{i\theta}|1\rangle$$

Each of the above gates are examples of unitary gates

They are reversible, unlike many of the classical gates

Quantum Gates

The Projection Gate / Operator

Let P denote a projection operator

Then $P = P^2 = P^\dagger$ in which $P^\dagger = \overline{P^T}$

Examples

$$I,\ P_{|0\rangle} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = |0\rangle\langle 0|,\ P_{|1\rangle} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = |1\rangle\langle 1|,\ P_{|+\rangle},\ P_{|-\rangle}$$

Projection gates are in general not reversible

- They are in general examples of Hermitian / Self Adjoint Operators

Postulate 2 - Nielsen and Chuang

Evolution

- The evolution of a *closed* system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle$$

Nielsen and Chuang, Quantum Computation and Quantum Information, CUP, 2000/2010

- A selection of quantum properties and tools

Quantum Properties

Some Useful Properties that we have to work with:

- No Cloning

  The No Cloning Theorem states that it is impossible to copy general quantum states, with a ‘Unitary’ copier. For non orthogonal pure states, copying is impossible, without a loss in fidelity for any copier

- Measurement (in general) leads to change

  So if you try to measure a quantum state you will in general change the state – see measurement postulate below

  These properties have been employed in, for example, quantum key agreement protocols such as: BB84, B92, E91, …

Quantum Supremacy

- Quantum Supremacy
  - 2018 Google 49 qubits, IBM 51, ? 53 qubit
  - 2019 Google claim quantum supremacy, using 54-qubit Sycamore processor
  - Performs calculation in 200 seconds rather than 10,000 years by the most powerful supercomputer
  - IBM challenge the fidelity of the work, claiming Google “failed to fully account for plentiful disk storage”
  - The calculation involved generating random numbers Quantum Supremacy using a programmable superconducting processor, Nature, vol574,24th October 2019, https://doi.org/10.1038/s41586-019-1666-5

Quantum Tools

The tools employed include and are not limited to

- Superposition
- Entanglement
- Error Correction
- Entanglement Swapping
- Teleportation
- Flying and Stationary Qubits
- Parallelism
- Interference

Quantum Communication

- Not Explicitly Using Entanglement
  - La Palma To Tenerife experiment
  - Line of sight, flying and stationary qubits
  - Dark fibre channels
  - Key Agreement Protocols
    - BB84, B92
- Explicitly Using Entanglement
  - Shanghai to Beijing Quantum Network
  - Key Agreement Protocols
    - E91
  - Security protocols – for example authentication

The Measurement Postulate

Postulate 3 - Measurement

- Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment

$$|\psi'\rangle = U|\psi\rangle$$

Postulate 3 – Measurement continued

- If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle \psi | M_m^* M_m | \psi \rangle$$

and the state of the system after the measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^* M_m | \psi \rangle}}$$

Postulate 3 – Measurement continued

- The measurement operators satisfy the completeness equation

$$\sum_m M_m^* M_m = I$$

- The completeness equation expresses the fact that probabilities sum to one

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^* M_m | \psi \rangle$$

- This equation being satisfied for all $|\psi\rangle$ is equivalent to the completeness equation

Activity 1