Week 13

Quantum Cryptography & Exam Review

THE UNIVERSITY OF SYDNEY

Quantum Cryptography

THE UNIVERSITY OF SYDNEY

Quantum Cryptography

- What is quantum cryptography?
  - Using quantum computers to do cryptography
- What are quantum computers?
  - Quantum physics applied to computational tasks
- What does quantum cryptanalysis mean for classical cryptography?
- Is it feasible?
- Can we exploit quantum effects to solve our security woes?

Quantum Physics

- Matter is "quantised"
  - Atoms emit energy in discrete quanta, called "photons"

- Atoms sometimes interact in unexpected ways. Atomic properties are often undefined, expressed as a **"superposition"** of states
  - Atomic spin might be up, down, or *both*
  - Only defined when observed ("decoherence")

- Classical Bits: 0 1

- Qubits: 0 ? 1

How We've Been Doing Crypto

- Based on complex mathematics:
  - near one-way functions
  - easy to compute one-way (encrypt), hard to reverse (decrypt) without knowing the key

- Security reliant on:
  - computational intractability – how difficult to compute
  - processing times of best-known methods of decryption scale rapidly with the size of key
  - difficulty of factoring is at the core of modern methods of encryption

Perfect Secrecy

- One-Time Pad
  - based on random codes that are only used once
  - perfect secrecy proved by Shannon (1949)

- Problem:
  - code book (one-time pad) needs to be transported from sender to receiver
  - needs to be done securely

Quantum Cryptography

- Quantum cryptography first conceived by Brassard and Bennett (1984)
  - provides a method to transmit a one-time pad (key) using single photons
  - any eavesdropping (attempt to copy the key) results in detectable variations in quantum states of the photons
  - key can be based on true randomness drawn from nature

- Circa 2000 - proposal to use highly-tuned laser beams instead of single photons
  - Australian National University (ANU) Quantum Optics Group amongst one of the first teams in the world to demonstrate a prototype
  - QuintessenceLabs developing this technology for commercial deployment

Classical Crypto Algorithms

- Based on
  - Complex transposition and substitution
  - Hard mathematical algorithms
- Rely on
  - No algorithmic weaknesses
  - Infeasibility of brute force attack
  - Mathematical complexity
- OTP offers provably secure encryption
  - Perfect security

Alice, Bob & Eve

- Eve is omnipresent
  - She is always around
- Eve is omniscient
  - She knows all the tricks, including those we do not know
  - She knows our cryptography algorithm
- Eve is omnipotent
  - She has perfect interception setups
  - She has infinite amount of money
  - She has infinite time
- Eventually RSA will be insecure!!!

Crypto Requirement #1: Randomness

- What is true randomness, what tests are there?
- Why is it difficult to get random number from computers
  - Because it always relies on fixed algorithm.
- In Quantum Physics, it can be achieved:
  - Quantum Decoherence https://en.wikipedia.org/wiki/Quantum_decoherence
  - Reflection of a photon off a half-silvered mirror. https://en.wikipedia.org/wiki/Wheeler%27s_delayed-choice_experiment
  - Quantum Fluctuations ANU QRNG – Quantum random numbers

Crypto Requirement #2: Irreversibility

- There is no known irreversible 1-to-1 mathematical function!
  - Many-to-one functions and one-to-many relations cannot work.

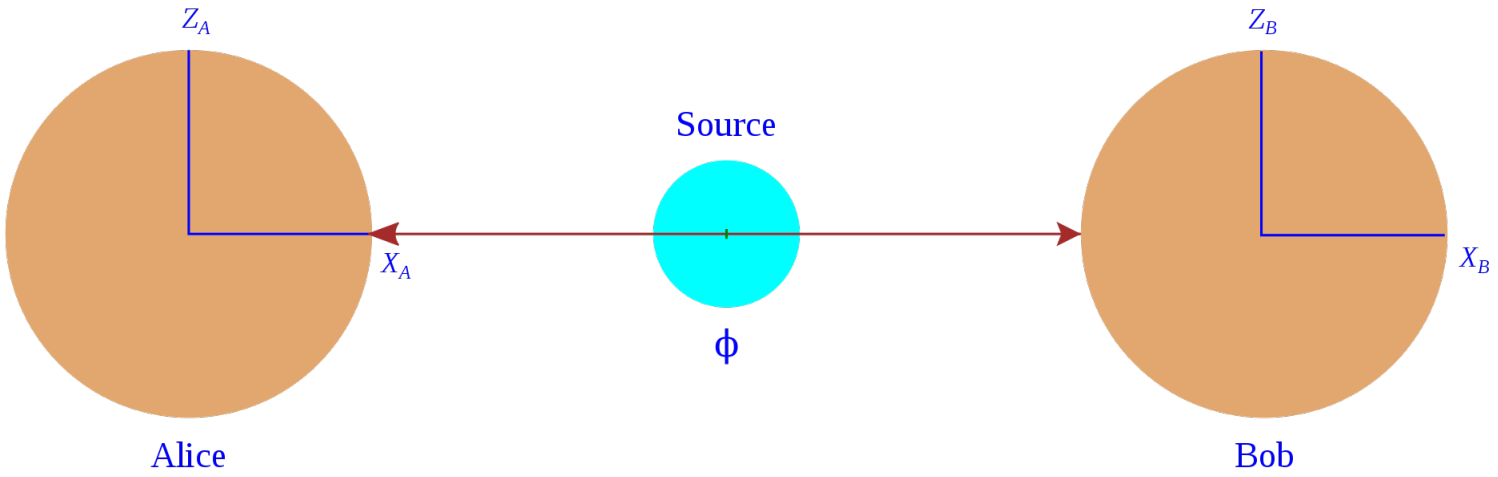
- Best approximation to irreversible function is factorisation.
  - It is easier to multiply large numbers, harder to factorise.
  - It is easier to differentiate complex functions, harder to integrate.

- In Quantum Physics, we can rely on concepts such as observer effect.
  - reduction of a superposition of eigenstates to a single eigenstate after interaction with an observer

EPR Entanglement and Wavefunction Collapse

- Entanglement means that the left hand knows what the right hand is doing, even when the hands are very far apart

- Wavefunction collapse is our 2nd ingredient
  - "a one-time lock/key".



Quantum Key Distribution

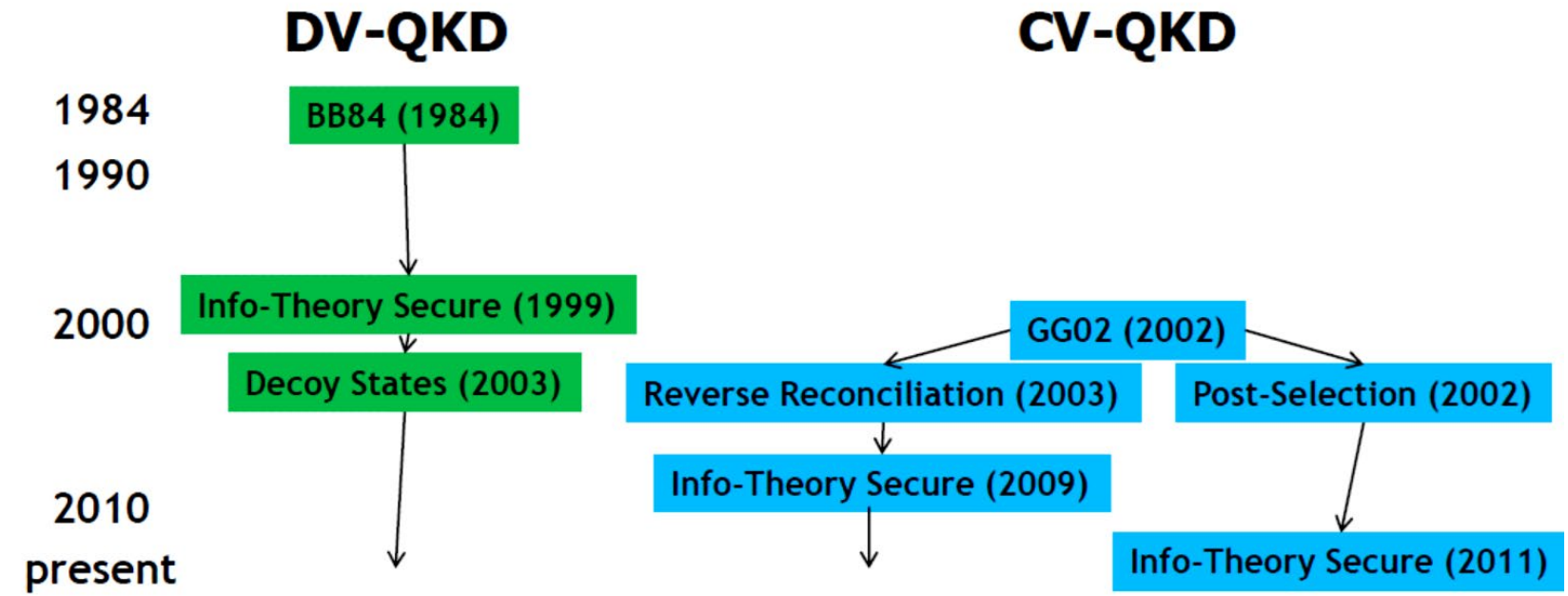
- Secure information

$$\Delta_I = I_{AB} - I_E$$

where I_{AB} is the amount of shared information Alice and Bob can agree on and I_E is the maximum amount of information accessible to a third party with total control over the transmission channel

- A QKD device must:
  - Estimate the channel parameters to bound I_E
  - Reconcile efficiently the information shared between Alice and Bob
  - Extract the secure information

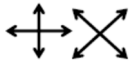
Two Types of QKD



	DV-QKD	CV-QKD
Sources	Single photons/ Attenuated coherent lasers	Weakly modulated bright coherent laser
Detectors	Single-photon detectors	Homodyne detectors

Discrete Variable QKD (DV-QKD)

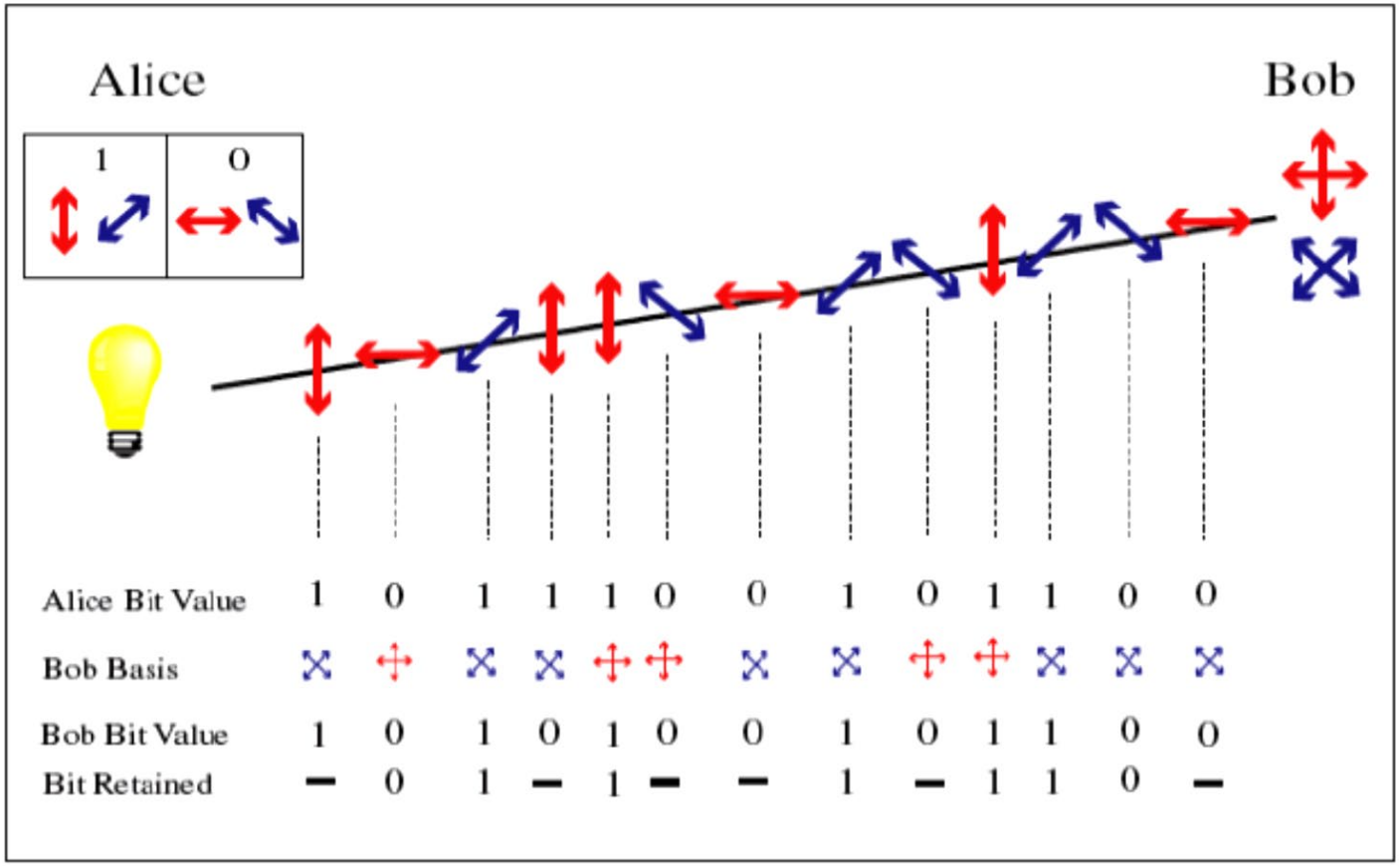
- Quantum key exchange with polarised photons.

- Two basis pairs of two states (rectilinear and diagonal) 
  - Alice generates random bit string, and random basis sequence
    e.g. 0110101 and 
  - Alice sends a photon per bit, polarised with the chosen basis
  - Bob randomly picks a basis for each bit
  - Alice and Bob compare notes later, only about chosen basis

- Any interception by Eve destroys initial photon state. Immune to MITM if Alice and Bob can verify each other's identity

Discrete Variable QKD (DV-QKD)

– Bennett and Brassard proposed in 1984 that if single photons are sent from Alice to Bob, communication between them can be absolutely secure.



Practicality of DV-QKD

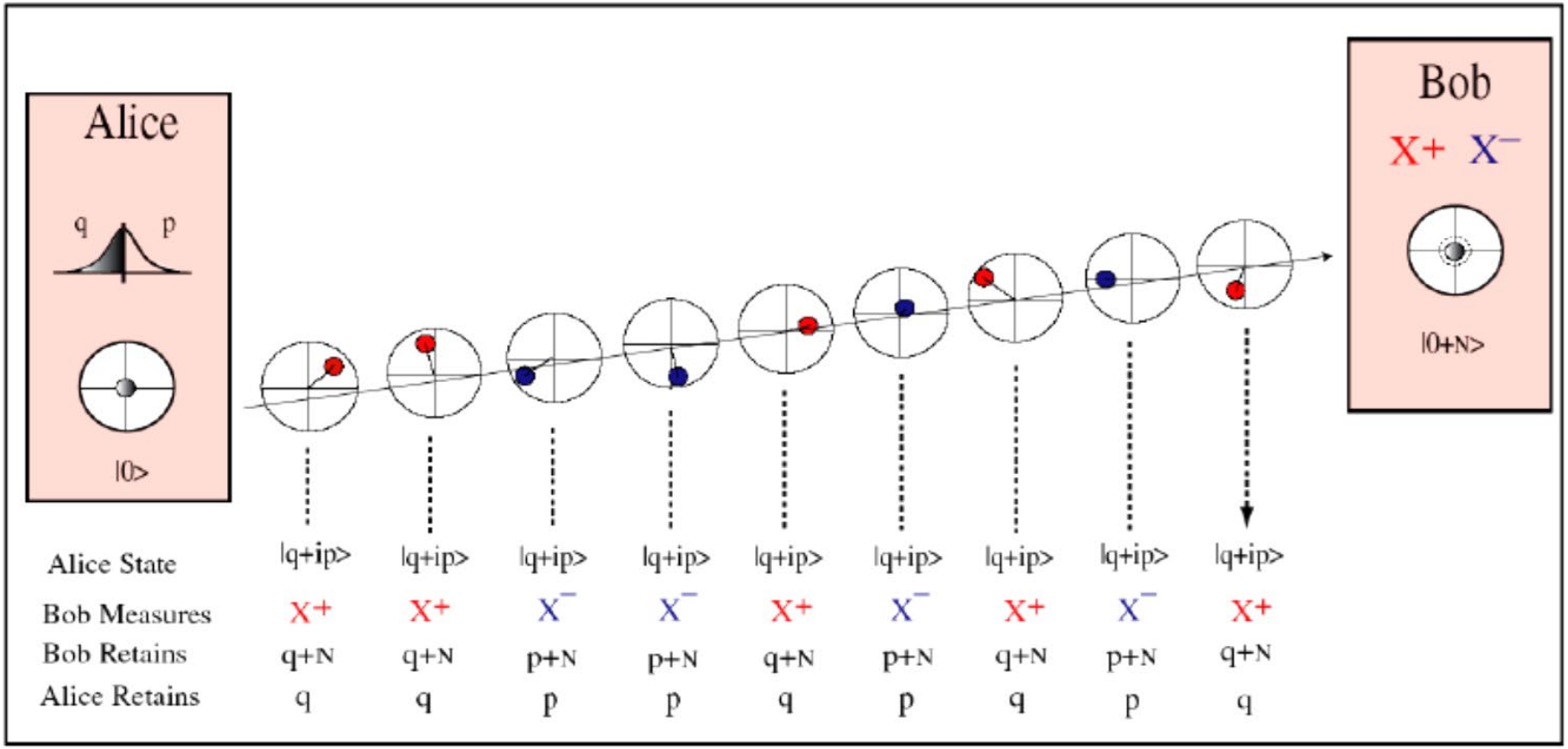
- Implementations are getting better
  - 1989: 32 cm
  - Now ~200km
  - 144km Free Space

- Still very slow and difficult, and doesn't solve everything
  - authentication
  - non-repudiation (digital signatures)
  - and more …

- Moral: there are no "silver bullets" for security problems

Continuous Variable QKD (CV-QKD)

– Several proposals surfaced after 2000 suggested that whole laser beams can be used for quantum cryptographic communication



CV-QKD Advantages

- Higher detector efficiencies
- Off-the-shelf components
- Telecommunications compatible
- Higher key rates achievable

	Optical Device	Bandwidth
Laser	Shot-noise-limited laser	Essentially unlimited*
Modulators	Amplitude and phase modulators	Available: >40 GHz
Detectors	Shot-noise-limited homodyne detectors	Available: 10 GHz

Shor's Algorithm (1994)

- Algorithms for quantum computation: discrete logarithms and factoring (https://ieeexplore.ieee.org/document/365700)
  - Efficient factoring of n-bit integers with 2n-qubit registers with polynomial time

- Anything relying on integer factorisation or the discrete logarithm problem can't resist quantum cryptanalysis, e.g., RSA, DSA, Diffie-Hellman, El Gamal, ECC. Note: One-Time Pad is still fine – why?

- Quantum cryptography offers the possibility of perfect secrecy that cannot be compromised by advances in computational or mathematical capabilities

- https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Exam Review

THE UNIVERSITY OF SYDNEY

How to make your USS feedback count

– Your Unit of Study Survey (USS) feedback is **confidential.**

– It's a way to share what you enjoyed and found most useful in your learning, and to provide constructive feedback. It's also a way to 'pay it forward' for the students coming behind you, so that their **learning experience** in this class is as good, or even better, than your own.

When you complete your USS survey (https://student-surveys.sydney.edu.au), please:

Be specific.

– Which class tasks, assessments or other activities helped you to learn? *Why* were they helpful? Which one(s) *didn't* help you to learn? *Why* didn't they work for you?

Be constructive.

– What practical changes can you suggest to class tasks, assessments or other activities, to help the next class learn better?

Be relevant.

– Imagine you are the teacher. What sort of feedback would you find most useful to help make your teaching more effective?

ELEC5616 Final Exam

THE UNIVERSITY OF SYDNEY

Room Number	
Seat Number	
Student Number	

ANONYMOUSLY MARKED

(Please do not write your name on this exam paper)

CONFIDENTIAL EXAM PAPER

This paper is not to be removed from the exam venue

Electrical and Information Engineering

EXAMINATION

Semester 1 - Final, 2025

ELEC5616 Computer and Network Security

EXAM WRITING TIME: 2 hours

READING TIME: 10 minutes

EXAM CONDITIONS:
This is a CLOSED book exam - no material permitted

MATERIALS PERMITTED IN THE EXAM VENUE:
(No electronic aids are permitted e.g. laptops, phones)

Calculator - non-programmable

MATERIALS TO BE SUPPLIED TO STUDENTS:
Answer sheet: Gradescope MCQ (single-sided - 100 Qs)

Blank scratch paper (2 sheets)

ELEC5616 Final Exam

INSTRUCTIONS TO STUDENTS:

1. This exam contains two (2) sections and twenty-five (25) questions. All questions must be answered.

    - Section A: This section contains twenty (20) questions. For each question, choose only one option that answers the question best. You must record your answers on the *Answer Sheet: Gradescope MCQ sheet*. Do not write your answers on the exam paper or anywhere else as they will not be counted.
    - Section B: This section contains five (5) questions. You must fill in the student number box in Part B (page 8), before answering the questions. Answer all the questions in the corresponding spaces provided on this exam paper booklet. If you need additional writing space, use the extra pages provided at the end of this exam paper booklet. Only answers written within the designated spaces on this exam paper booklet will be marked. Scratch papers will not be marked.

2. The total mark for this exam is 50. The mark for each question is indicated at the start of the section.

3. Write all your final answers to the questions in this paper in ink, not pencil. Take care to write legibly. Do not remove this paper from the exam venue.

ELEC5616 Final Exam

- Part A – Multiple Choice [Total 20 marks, 1 mark per question]
  - Record your answers on the Gradescope MCQ sheet
  - Total 20 questions, worth 1 mark each
    - 6 questions from Weeks 1-7
    - 14 questions from Weeks 8-13

- Part B – Short answer question [Total 30 marks, 6 marks per question]
  - Fill in the student number box in Part B, before answering the questions
  - Answer all the questions in the spaces provided on this exam paper booklet
  - Total 5 questions worth 6 marks each
    - 2 questions from Weeks 1-7
    - 3 questions from Weeks 8-13

ELEC5616 Review

- Week 1
  - Basic Principles of Security, CIA triad, Kerckhoff's Principle
  - Properties of Secure Hash Functions, Collision Resistance
- Week 2
  - Ciphers and cryptanalysis, COA, KPA, CCA
  - Substitution Ciphers, Caesar Cipher, Vigenere Cipher, OTP, Pseudorandom number generators (PRNGs)
- Week 3
  - Block Ciphers, DES design, modes of operation, ECB, CBC, OFB
- Week 4
  - Number theory, Diffie-Hellman key exchange, RSA public key encryption

ELEC5616 Review

- Week 5
  - Attacks on RSA, Digital Signatures based on RSA
  - Authentication, Passwords, Zero Knowledge Proofs

- Week 6
  - Diffie Hellman MITM Attacks, Public Key Management using Certificate Authorities
  - SSL/TLS protocol, Attacks on SSL/TLS

- Week 7
  - Shamir Secret Sharing, Commitment Protocols, Steganography, Botnet Attacks

ELEC5616 Review

- Week 9
  - Blockchain Network, Proof-of-Work, Blockchain Security & Attacks
- Week 10
  - Software Security, Bell-Lapadula Model, Buffer Overflow Attacks, Preventing Buffer Overflows, Race Conditions, Timing Attacks
  - Network Security, OSI Model, TCP/IP Handshake, Spoofing Attack
- Week 11
  - Network DoS Attacks, SYN Flooding, Smurfing, DDoS, Session Hijacking
  - Port Scanning, Firewalls, ARP attacks, DNS attacks
  - Web security, SQL, XSS, CSRF

ELEC5616 Review

- Week 12
  - Wireless Security, WEP, WPA/WPA2, Hardware Security
- Week 13
  - Quantum Cryptography, Quantum Key Distribution, Shor's Algorithm

Final Exam Tips

- Keep track of time. Exam duration 2 hours plus 10 minutes reading time.

- Write clearly and concisely
  - Write student number clearly on front page and on student number box in Part B.
  - Only answers written within the designated spaces on this exam paper booklet will be marked. Scratch papers will not be marked.
  - You may use relevant diagrams/examples to support or clarify your extended answer questions.
  - Examples cannot substitute definitions (but they can be used to clarify your answer).
  - Read question carefully and make sure to answer directly. Don't include unrelated information.

- Good luck!

THE UNIVERSITY OF SYDNEY