

# Quantum Computing & Cryptography

## Revision notes

Steve Vickers

### Past papers

- 2010 Quantum computing & cryptography
- to 2009 Introduction to quantum and molecular computation

### Summary of module

<u>Week</u>	<u>Topic</u>	<u>Chapters in Mermin</u>
1	Vectors, matrices for Cbits	1.1-1.4
2	General vectors	} 1.5-1.12
3	Qbits & their states	
4	Cryptographic protocols	6.1-6.3
5	Cryptography issues [Nielsen/Chuang 12.6]	
6	More applications of entanglement	6.4-6.5
7	Quantum algorithms - introduction	2.1-2.5
8	Special gates for quantum algorithms	2.6, 4
9	Quantum Fourier transform, period finding	3.4-3.9
10	Breaking RSA	3.1-3.3, 3.10
11	Quantum error correction	5

### Practical focus

Module most about protocols and algorithms

- What are they trying to achieve?
- How do you run them?
- How do they compare with classical computing?
- How do they work?
  - circuit diagrams
  - vector manipulation
  - some statistics

## Vectors, matrices for Cbits

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

• World's worst notation for numbers

• Operations as matrices • permutation

Reversible

• NOT (X), CNOT, SWAP

• Skill: write operation in matrix form

## General vectors

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

• Complex numbers

• Bras & kets (row & column vectors)  
 $\langle \phi |$   $|\psi\rangle$

• Tensor products  $|\phi\rangle|\psi\rangle$

• Inner product  $\langle \phi | \psi \rangle$

various notations

• Applications, eg.  $\langle n | A | n \rangle$  for matrix entries

• Operators X, Y, Z, H, C<sup>Z</sup>

• Equations, eg.  $XZ = -ZX$

• Skills: normalize vectors, use notation with confidence

## Qbits & their states

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

• state = ray of vector

• Bloch sphere for states of 1 qbit

• Entanglement

• Born rule - for measurements

• Important skill Calculate resulting state after a partial measurement

## Cryptographic protocols

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

Current technology:  
polarized photons

General issues

• What are Alice & Bob trying to achieve?

• What do they actually do? • specification

algorithm

## Cryptographic protocols

### Quantum 1-time pad (BB84)

- What are Alice & Bob trying to achieve? — key distribution
- What do they actually do? — specification — quantum & classical messages exchanged
- algorithm

- What effect does Eve have?
- How do Alice & Bob detect Eve? — Statistical
- Advantage of using quantum?

## Cryptographic protocols

### Quantum bit commitment

Similar story, different ending

- What are Alice & Bob trying to achieve? — bit commitment
- What do they actually do? — specification — quantum & classical messages exchanged
- algorithm

- How does Alice use entanglement to cheat?  
Need to understand vector calculations for entangled states.

## Cryptography issues

- Quantum  $\Rightarrow$  no passive eavesdropping
- Information reconciliation
- Privacy amplification
- Other attacks

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

## More applications of entanglement

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

## Quantum dense coding

## Teleportation

Note: No-Cloning theorem

- Same questions:
- What are Alice & Bob trying to achieve?
  - What do they actually do? — specification — algorithm

# Quantum algorithms

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

Toy problems { Deutsch's problem  
Bernstein-Vazirani - diagrams easier than algebra  
Simon } be sure to understand algorithm & how you execute it

# Special gates

Building the gates is quite intricate - I don't expect you to remember all the details

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

- Grover { ① Geometric using  $V$  and  $W$  - executing algorithm  
② Gates for  $W$  ?
- Toffoli gates - can be built from 2-qbit gates

# Breaking RSA

QFT - building gate

Period finding

- how to execute algorithm?

- Continued fractions

RSA - background

- how to execute RSA

- how to use period finding

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

No need to memorize proofs

# Quantum error correction

- 1 Vectors, matrices for Cbits
- 2 General vectors
- 3 Qbits & their states
- 4 Cryptographic protocols
- 5 Cryptography issues
- 6 More applications of entanglement
- 7 Quantum algorithms - introduction
- 8 Special gates for quantum algorithms
- 9 Quantum Fourier transform, period finding
- 10 Breaking RSA
- 11 Quantum error correction

Basic principles rather than details