SAND2014-20209C

Quantum Information Processing
An Overview

Uzoma Onunkwo

Advanced Information and Network Systems Engineering Department
Sandia National Laboratories
Albuquerque, NM

December 4th, 2014

Sandia National Laboratories

1. Demands of Wireless Communication
2. Information Processing
    - Digital Information
    - Quantum Information
3. Quantum Algorithms
4. Cryptography
    - Confidentiality
    - Authentication
    - Signature
5. Quantum Cryptography
    - *Quantumness*: Relevant Laws
    - Achieving Perfect Secrecy
    - Quantum Key Distribution (QKD) Purpose
    - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Outline

1. Demands of Wireless Communication
2. Information Processing
   - Digital Information
   - Quantum Information
3. Quantum Algorithms
4. Cryptography
   - Confidentiality
   - Authentication
   - Signature
5. Quantum Cryptography
   - *Quantumness*: Relevant Laws
   - Achieving Perfect Secrecy
   - Quantum Key Distribution (QKD) Purpose
   - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Demands of Wireless Communications

Demands of Wireless Communications

1. Higher effective data rates: 1G (*circa 1981*) $\rightarrow$ 2G (*circa 1991*)$\rightarrow$ 3G (*circa 2001*)$\rightarrow$ 4G (*circa 2012*)$\rightarrow$ 5G (*maybe 2020*).

Sandia National Laboratories

Demands of Wireless Communications

1. Higher effective data rates: 1G (*circa 1981*) $\rightarrow$ 2G (*circa 1991*)$\rightarrow$ 3G (*circa 2001*)$\rightarrow$ 4G (*circa 2012*)$\rightarrow$ 5G (*maybe 2020*).
2. Higher capacity in terms of number of simultaneous users.

Sandia National Laboratories

Demands of Wireless Communications

1. Higher effective data rates: 1G (*circa 1981*) → 2G (*circa 1991*)→ 3G (*circa 2001*)→ 4G (*circa 2012*)→ 5G (*maybe 2020*).
2. Higher capacity in terms of number of simultaneous users.
3. Secure communications for privacy.

Sandia National Laboratories

Outline

1. Demands of Wireless Communication
2. Information Processing
   - Digital Information
   - Quantum Information
3. Quantum Algorithms
4. Cryptography
   - Confidentiality
   - Authentication
   - Signature
5. Quantum Cryptography
   - *Quantumness*: Relevant Laws
   - Achieving Perfect Secrecy
   - Quantum Key Distribution (QKD) Purpose
   - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Computation 101

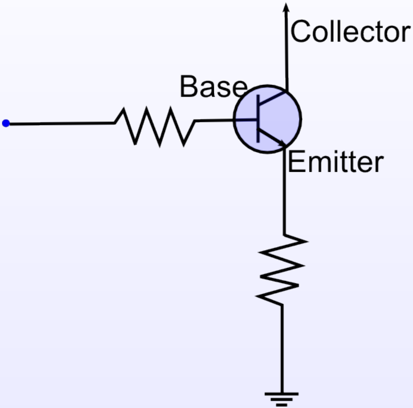
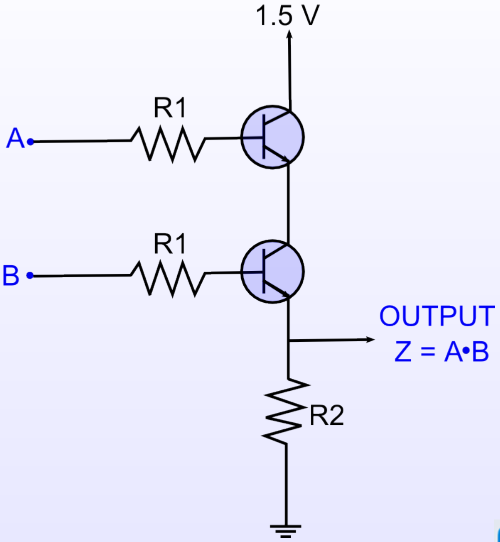


Figure 1: Transistor circuit: *increasing voltage at base, exponentially increases current flow from collector to emitter; the converse is also true...we have a switch!*

Sandia National Laboratories

Computation 101



Sandia National Laboratories

Computation 101

BASIC UNIVERSAL GATES (generally, irreversible)

AND gate			OR gate			NOT gate	
A	B	Q	A	B	Q	A	Q
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

Computation 101

BASIC UNIVERSAL GATES (generally, irreversible)

AND gate			OR gate			NOT gate	
A	B	Q	A	B	Q	A	Q
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

1-BIT ADDER

input (two 1-bits)		output (2-bit)		
x	y	b_1	b_2	decimal value
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	2

Sandia National Laboratories

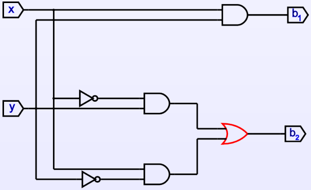
Computation 101

BASIC UNIVERSAL GATES (generally, irreversible)

AND gate			OR gate			NOT gate	
A	B	Q	A	B	Q	A	Q
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

1-BIT ADDER

input (two 1-bits)		output (2-bit)		
x	y	b_1	b_2	decimal value
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	2



Sandia National Laboratories

Quantum computing 101: *A compare and contrast approach*

	Classical	Quantum
Basis of information	Bits: 0 or 1 2-level system	Qubits: $\|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ infinitely possible vectors or states, e.g., $\|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\|\phi\rangle = \begin{pmatrix} 0.8 \\ 0.6 \end{pmatrix}$
Gates	AND, OR, NOT generally irreversible	Bit-flip $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Idle rotation $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ reversible operations
Can transport (qu)bits	Yes	*Yes*
Can clone (copy) (qu)bits	Yes	No
Effect of measurement	Nothing	Destroys original qubit

Potential Realizations of Qubits

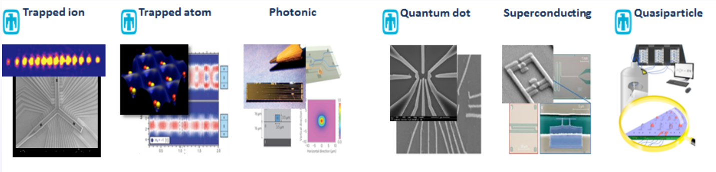


Figure 2: Source: Technical Overview presentation on AQUARIUS Grand Challenge

- Physical realization of qubits; *think of vacuum tubes and transistors for bits*
  - Quantum dots (*non-mobile*)
  - Ion traps (*mobile*)
  - Neutral atom laser (*non-mobile?*)
  - Photons (*mobile*)
  - Superconducting flux (*non-mobile*)

Models of Quantum Computing

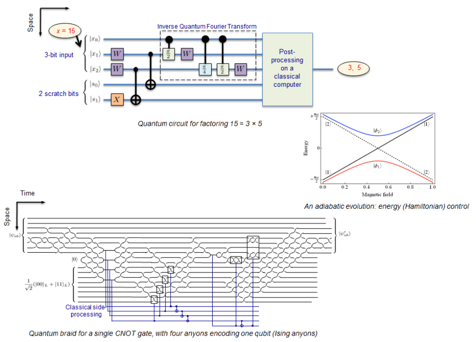


Figure 3: Source: Technical Overview presentation on AQUARIUS Grand Challenge

- Models of quantum computing
  - Circuit or network model
  - Adiabatic quantum computing model
  - One-way (Cluster state) computing model

Sandia National Laboratories

Outline

1. Demands of Wireless Communication
2. Information Processing
   - Digital Information
   - Quantum Information
3. Quantum Algorithms
4. Cryptography
   - Confidentiality
   - Authentication
   - Signature
5. Quantum Cryptography
   - *Quantumness*: Relevant Laws
   - Achieving Perfect Secrecy
   - Quantum Key Distribution (QKD) Purpose
   - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Quantum Algorithms

- *Grover's Algorithm*: Existence in an Unsorted Database.
- *Shor's Algorithm*: Factorization of Composite Numbers.
  - Extremely hard **classically**. Best classical solution takes exponential time in the number of bits to run.
  - Relatively easy to solve **quantum-wise** using *Shor's method*.

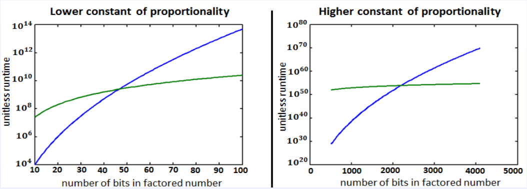


Figure 4:

- *Hallgren's Algorithm*: Solution to *Pell's* equation ($x^2 - dy^2 = 1$, $\{x, y, d\} \in \mathbb{Z}^+$ and d is a non-square positive integer).

Outline

1. Demands of Wireless Communication
2. Information Processing
   - Digital Information
   - Quantum Information
3. Quantum Algorithms
4. Cryptography
   - Confidentiality
   - Authentication
   - Signature
5. Quantum Cryptography
   - *Quantumness*: Relevant Laws
   - Achieving Perfect Secrecy
   - Quantum Key Distribution (QKD) Purpose
   - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Information Confidentiality

Purpose is to obfuscate information.

- Universally used:
  1. bank transactions,
  2. investment account management,
  3. sensitive e-mails, ...
- Desired property:
  1. *impossible* to decipher (decrypt) by an unwanted entity,
  2. should stand the test of time, and
  3. be easy enough to be *implementable* today.
- Decent solutions: block cipher vs. stream cipher, secret-key vs. public-key, ...

Information Confidentiality

Purpose is to obfuscate information.

- Universally used:
  1. bank transactions,
  2. investment account management,
  3. sensitive e-mails, ...
- Desired property:
  1. *impossible* to decipher (decrypt) by an unwanted entity,
  2. should stand the test of time, and
  3. be easy enough to be *implementable* today.
- Decent solutions: block cipher vs. stream cipher, secret-key vs. public-key, ...

`blahblah` is my password.
Can encrypt as
`cmbicmbi` jt nz qbttxpse.

Is this good?

Sandia National Laboratories

Information Confidentiality

Purpose is to obfuscate information.

- Universally used:
  1. bank transactions,
  2. investment account management,
  3. sensitive e-mails, ...
- Desired property:
  1. *impossible* to decipher (decrypt) by an unwanted entity,
  2. should stand the test of time, and
  3. be easy enough to be *implementable* today.
- Decent solutions: block cipher vs. stream cipher, secret-key vs. public-key, ...

`blahblah` is my password.

Can encrypt as

`cmbicmbi` jt nz qbttxpse.

Is this good? No, it is **horrible!** Susceptible to *Chosen-Plaintext Attack*

Sandia National Laboratories

Authentication: *They are who we thought they were!*

Authentication: *They are who we thought they were!*

- Validates the source of transmitted data.
- This is implemented over a classical channel, even in *quantum crptography*.
- Three main techniques exist:
  1. Use of *message authentication code* (MAC) - amenable to secret-key ciphers;
  2. Use of public key infrastructure (PKI) - amenable to public-key ciphers;
  3. Use of *universal families of hash functions* - amenable to quantum cryptography.

Signature: This is James Bond and I approve this message

- It is okay to eavesdrop, but it is not okay to forge my signature.
- Achievable with a form of encryption, *private-key encryption*.
- **Alice** signs a message. **Bob** receives the message and decrypts with *Alice's public-key*; this confirms Alice's signature.
- **Eve** can listen in the middle and even extract the message, but she cannot forge the signature

Sandia National Laboratories

Perfect Secrecy in Communications

- Can only be achieved if key size is greater than or equal to message size.
- Call $P = \{p : p$ is in the set of all plaintext$\}$ and $C = \{c : c$ is in the set of corresponding ciphertext$\}$, then if

$$Pr[P = p|C = c] = Pr[P = p]$$

  we say that we have perfect secrecy.
- Alice and Bob are legit users, while Eve is the eavesdropper. Eve should be able to listen/view cipher message all she wants, but not decipher it.

Sandia National Laboratories

Perfect Secrecy in Communications

- Can only be achieved if key size is greater than or equal to message size.
- Call $P = \{p : p$ is in the set of all plaintext$\}$ and $C = \{c : c$ is in the set of corresponding ciphertext$\}$, then if

$$Pr[P = p|C = c] = Pr[P = p]$$

  we say that we have perfect secrecy.
- Alice and Bob are legit users, while Eve is the eavesdropper. Eve should be able to listen/view cipher message all she wants, but not decipher it.
- Perfect secrecy of information **cannot** be achieved with key lengths less than message length.
  - Today's ciphers use key lengths much smaller than message lengths!
  - AES-256 uses a key length of 256 bits, message block size of 128 bits, but the same key for a long message.
  - RSA (cipher for SSH) uses keys of size 1024, 2048, and 4096 bits, but much longer messages.

Sandia National Laboratories

So, aren't current cryptographic techniques sufficient?

So, aren't current cryptographic techniques sufficient?

- Current classical cryptographic systems are mostly *cat-and-mouse* solutions...propose solutions based on current attacks.
- Strong presumptions made on solvability of currently hard problems, like *modulo-factoring* for the famous RSA-cipher system.

Sandia National Laboratories

Outline

1. Demands of Wireless Communication
2. Information Processing
   - Digital Information
   - Quantum Information
3. Quantum Algorithms
4. Cryptography
   - Confidentiality
   - Authentication
   - Signature
5. Quantum Cryptography
   - *Quantumness*: Relevant Laws
   - Achieving Perfect Secrecy
   - Quantum Key Distribution (QKD) Purpose
   - BB84 - A Quantum Cryptography Protocol
6. Final Remarks
7. References

Sandia National Laboratories

Relevant Laws of Quantum Physics

1. It is impossible to clone a qubit, the equivalent of classical bits. This limitation is mathematically proven and does NOT rely on technological limitation.

Relevant Laws of Quantum Physics

1. It is impossible to clone a qubit, the equivalent of classical bits. This limitation is mathematically proven and does NOT rely on technological limitation.
2. Observing the state of a qubit destroys its previous state; hence, **we cannot distinguish between non-orthogonal states**:
   - Classically, we only have 1 and 0's...we can distinguish these.
   - Quantum-wise, we have $|1\rangle, |0\rangle, |+\rangle, |-\rangle$, ... in fact infinite representative qubits!

Sandia National Laboratories

Cloning qubits is impossible: *A No-go Theorem*

- One can make multiple copies of an *a priori* known qubit, but...
- One cannot make a gadget that makes copy of any arbitrary input qubit

Proof.

If such a gadget existed, then it should do the following: $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \equiv |\psi\psi\rangle$. Let such a gadget be represented by the linear operator, $\mathcal{C}$. The requirement for linearity of the operator comes from Schrödinger's equation. Then,

$$\mathcal{C}\,|\psi\rangle = |\psi\psi\rangle$$

By the same token, we expect

$$\mathcal{C}\,|0\rangle = |00\rangle \tag{1}$$
$$\mathcal{C}\,|1\rangle = |11\rangle \tag{2}$$
$$\mathcal{C}\,(|0\rangle + |1\rangle) = (|00\rangle + |11\rangle) \tag{3}$$

The last line comes from the linearity property of the operator $\mathcal{C}$, which contradicts the expected result of

$$\begin{aligned}\mathcal{C}\,(|0\rangle + |1\rangle) &= (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\\ &\neq (|00\rangle + |11\rangle)\end{aligned}$$

Thus, no such gadget can exist; we call this the *No-cloning Theorem*. $\square$

Sandia National Laboratories

More details on Qubit Observation

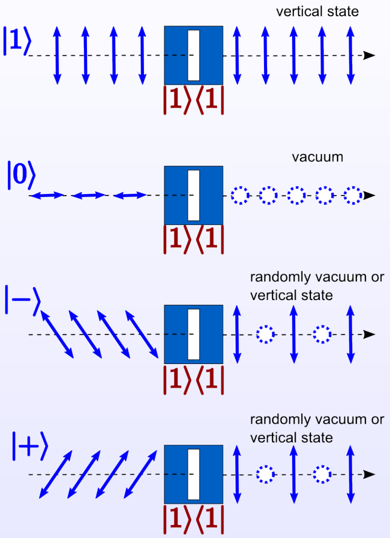


Figure 5: photon qubits being measured by polarizer

Perfect Secrecy Revisited

- One-time pad with key length at least as long as message: assume plaintext is 0110 and random key is 1010, then ciphertext can be 1100. Can't decipher plaintext from this!

Sandia National Laboratories

Perfect Secrecy Revisited

- One-time pad with key length at least as long as message: assume plaintext is 0110 and random key is 1010, then ciphertext can be 1100. Can't decipher plaintext from this!
- Cannot reuse cipher key or Eve can decipher message by performing XOR on consecutive message.

Sandia National Laboratories

Perfect Secrecy Revisited

- One-time pad with key length at least as long as message: assume plaintext is 0110 and random key is 1010, then ciphertext can be 1100. Can't decipher plaintext from this!
- Cannot reuse cipher key or Eve can decipher message by performing XOR on consecutive message.
- Requires true random keys. Pseudo-random numbers prevalent on today's computers is not sufficient; they are deterministic unfortunately. TRNG generators exist:
  1. Hotbits - rely on radioactive decay, but slow rates $<$ 1Kbits/sec.
  2. Protego's SG100 EVO-USB - rely on resistive circuit elements and yields about 16 Mbits/sec per module.
  3. Quantum measurement of qubits.

Sandia National Laboratories

Quantum Cryptography is really Quantum Key Distribution

- We are not encrypting *qubits*, we are encrypting *bits* in plaintext.
- One-time pad needs constantly changing keys equal to message length or more.
- QKD achieves safe secret sharing using (a) quantum channel and (b) classically authenticated channel.

A Quantum Cryptography Protocol - BB84

- Alice will send messages to Bob. Eve is the eavesdropper.
- Alice and Bob authenticate to each other, using classical channel but maybe with universal hash function technique.
- Alice chooses four *non-orthogonal* qubit states.
- Bob measures these states, with some errors.
- Alice and Bob negotiate error and decide whether to discard or to correct and use distilled key.

A Quantum Cryptography Protocol - BB84

- Alice will send messages to Bob. Eve is the eavesdropper.
- Alice and Bob authenticate to each other, using classical channel but maybe with universal hash function technique.
- Alice chooses four *non-orthogonal* qubit states.
- Bob measures these states, with some errors.
- Alice and Bob negotiate error and decide whether to discard or to correct and use distilled key.
- If Eve observes the channel, she will likely cause errors that both Alice and Bob will detect.

A Quantum Cryptography Protocol - BB84

- Alice will send messages to Bob. Eve is the eavesdropper.
- Alice and Bob authenticate to each other, using classical channel but maybe with universal hash function technique.
- Alice chooses four *non-orthogonal* qubit states.
- Bob measures these states, with some errors.
- Alice and Bob negotiate error and decide whether to discard or to correct and use distilled key.
- If Eve observes the channel, she will likely cause errors that both Alice and Bob will detect.
- In addition, Eve cannot store the qubits for future use in deciphering messages (*No-cloning principle*).

BB84 - Pictoral Depiction

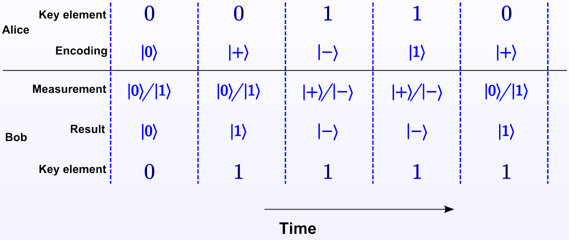
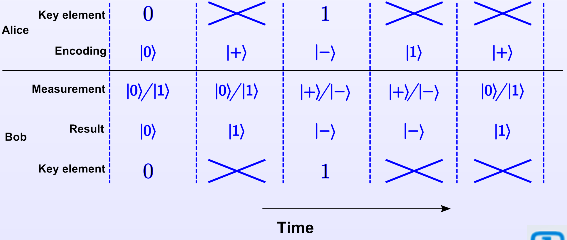


Figure 6:



Sandia National Laboratories

Figure 7: Redrawn from G.V. Assche's textbook [2].

Final Remarks

- Quantum science shows promises for alternative way of information processing.
- QKD aides secret sharing of cryptographic keys based on information-theoretic limits not computational constraint. When combined with a one-time padding cipher, one can attain perfect secrecy.
- Commercial companies providing quantum key distribution (QKD) systems are:
    1. **id Quantique** in Geneva, Switzerland,
    2. **MagiQ Technologies** in New York, USA, and
    3. **QuintessenceLabs** in Australia.

Sandia National Laboratories

Questions

Thank you for being here!

Q & A

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[2] G. V. Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.

[3] U. M. Maurer, "Authentication theory and hypothesis testing," *Information Theory, IEEE Transactions on* vol. 46, no. 4, pp. 1350 - 1356, 2000.

Sandia National Laboratories