Quantum Cryptography

Guest Lecture for CS134

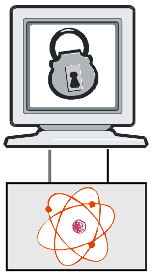
Nick Papanikolaou
http://www.warwick.ac.uk/go/nikos

Quantum Computing & Quantum Information

- Use of the phenomena of quantum physics for:
  - Representation,
  - Manipulation,
  - Transmission
- …of information
- Useful aspects of Quantum Theory for comp. purposes:
  - Randomness of quantum measurements
  - States which are linear combinations of classical states
  - Entanglement
  - …

Introduction

- Quantum cryptography is the single **most successful application** of Quantum Computing/Information Theory.
- **For the first time in history,** we can use the forces of nature to implement **perfectly secure** cryptosystems.
- Quantum cryptography has been tried experimentally: **it works!**



State of the Art

- The commonly used RSA cryptosystem relies heavily on the **complexity of factoring integers.**
- Quantum Computers can use **Shor's Algorithm** to efficiently break today's cryptosystems.
- We need a **new kind** of cryptography which is secure even against quantum computers!

Outline

- Basic Ideas in **Cryptography**
- Ideas from the **Quantum world**
- Quantum Key Distribution **(QKD)**
- **BB84** without eavesdropping
- **BB84** with eavesdropping
- Working **Prototypes**
- Related research here at **Warwick**
- **Conclusion**

Reminder of Basic Cryptography

- **Cryptography:** "the coding and decoding of secret messages." [Merriam-Webster]
- Cryptography < κρυπτός + γραφή.
- The basic idea is **to modify a message so as to make it unintelligible to anyone but the intended recipient.**
- For message (plaintext) *M*,

e(*M, K***)** **encryption:** ciphertext

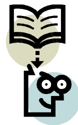
d[e(*M, K***),** ***K*]** = *M* **decryption**

Keys and Key Distribution

- *K* is called the **key.**
- The key is known only to sender and receiver: it is **secret.**
- **Anyone** who knows the key can decrypt the message.
- **Key distribution** is the problem of exchanging the key between sender and receiver.

Perfect Secrecy and the OTP

- There exist **perfect cryptosystems.**
  - **= cryptosystems which maintain secrecy of the message even if the key is found out**
- Example: **One-Time Pad (OTP)**
- The problem of **distributing the keys** in the first place **remains.**



Enter QKD …

- QKD: **Quantum Key Distribution**
- Using **quantum effects,** we can distribute keys in perfect secrecy!
- The Result: The Perfect Cryptosystem,

QC = QKD + OTP

Ideas from the Quantum World

- **Measurement**
  - Observing, or **measuring,** a quantum system will alter its state.
  - Example: the **Qubit**

$$|\psi\rangle = a \cdot |0\rangle + b \cdot |1\rangle$$

  - When observed, the state of a qubit will **collapse** to either *a=0* or *b=0*.

Photons

- **Physical qubits**
  - Any **subatomic particle** can be used to represent a qubit, e.g. an electron.
  - A **photon** is a convenient choice.
  - A photon is an **electromagnetic wave.**

Polarization

- A photon has a property called **polarization,** which is the plane in which the electric field oscillates.
- We can use photons of different polarizations to represent quantum states:

$$\theta = 0^\circ \Rightarrow \text{state } |0\rangle$$
$$\theta' = 90^\circ \Rightarrow \text{state } |1\rangle$$

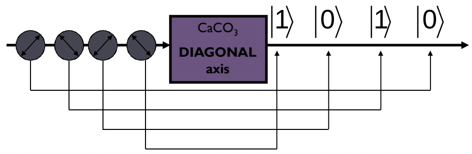
Polarizers and Bases

- A device called a **polarizer** allows us to place a photon in a particular polarization. A **Pockels Cell** can be used too.
- The polarization **basis** is the mapping we decide to use for a particular state.

Rectilinear:	**Diagonal:**
$\theta = 0^\circ \Rightarrow$ state $\lvert 0\rangle$	$\theta = 45^\circ \Rightarrow$ state $\lvert 0\rangle$
$\theta' = 90^\circ \Rightarrow$ state $\lvert 1\rangle$	$\theta' = 135^\circ \Rightarrow$ state $\lvert 1\rangle$

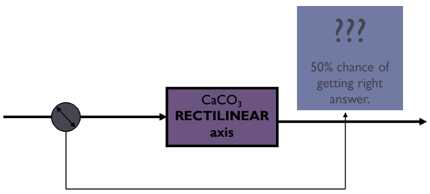
Measuring Photons

- A **calcite crystal** can be used to recover the bits encoded into a stream of photons.

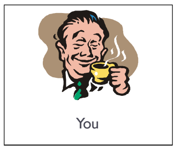


Uncertainty Principle

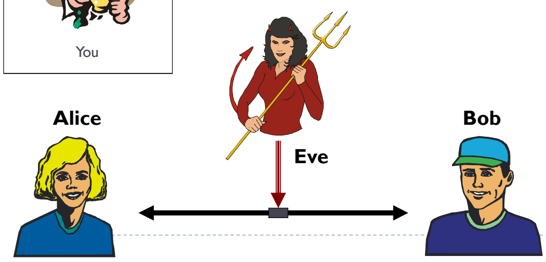
- What if the crystal has the **wrong orientation?**



Meet Alice and Bob



We have to prevent **Eve** from **eavesdropping** on communications between **Alice** and **Bob**.



Quantum Key Distribution

- **Quantum Key Distribution** exploits the effects discussed in order to **thwart eavesdropping.**
- If an eavesdropper uses the wrong polarization basis to measure the channel, **the result of the measurement will be random.**

QKD Protocols

- A **protocol** is a set of rules governing the exchange of messages over a channel.
- A **security protocol** is a special protocol designed to ensure security properties are met during communications.
- There are three main security protocols for QKD: **BB84**, **B92**, and **Entanglement-Based QKD.**
- We will only discuss **BB84** here.

BB84 …

- **BB84** was **the first security protocol** implementing Quantum Key Distribution.
- It uses the idea of **photon polarization.**
- The **key** consists of bits that will be transmitted as photons.
- Each bit is encoded with a **random polarization basis!**

BB84 with no eavesdropping

- **Alice** is going to send **Bob** a key.
- She begins with a **random sequence of bits.**
- Bits are encoded with a **random basis,** and then sent to Bob:

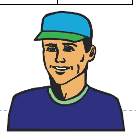
Bit	0	1	0	1	1
Basis	+	×	×	+	×
Photon	↔	⤡	⤢	↕	⤡

BB84 with no eavesdropping (2)

- **Bob receives the photons** and must decode them using a random basis.

Photon	↔	⤡	⤢	↕	⤡
Basis?	+	+	×	+	×
Bit?	0	0	0	1	1

- **Some** of his measurements are correct.



BB84 with no eavesdropping (3)

- Alice and Bob talk **on the telephone:**
  - **Alice** chooses a subset of the bits (the **test bits**) and reveals which basis she used to encode them to Bob.
  - **Bob** tells Alice which basis he used to decode **the same** bits.
  - **Where the same basis was used,** Alice tells Bob what bits he ought to have got.

Comparing measurements

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon	↔	⤡	⤢	↕	⤡
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits

The **test bits** allow Alice and Bob to test **whether the channel is secure.**

The Trick

- As long as no errors and/or eavesdropping have occurred, **the test bits should agree.**
- Alice and Bob have now made sure that **the channel is secure.** The test bits are removed.
- Alice tells Bob **the basis she used for the other bits,** and they both have a common set of bits: the final key!

Getting the Final Key

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits discarded

Final Key = 01

In the presence of eavesdropping

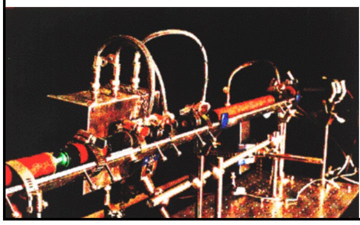
- **If an eavesdropper Eve tries to tap the channel,** this will automatically show up in Bob's measurements.
- **In those cases where Alice and Bob have used the same basis,** Bob is likely to obtain an **incorrect measurement:** Eve's measurements are bound to affect the states of the photons.

In the presence of eavesdropping (2)

- As Eve intercepts Alice's photons, **she has to measure them** with a random basis and send new photons to Bob.
- The photon states cannot be cloned **(non-cloneability).**
- Eve's presence is always detected: **measuring** a quantum system **irreparably alters its state.**

Working Prototypes

- Quantum cryptography has been tried experimentally over **fibre-optic cables** and, more recently, **open air (23km).**



Left: The first prototype implementation of quantum cryptography

(IBM, 1989)

Research on QC at Warwick

- Research group of Dr R. Nagarajan [DCS, 3.26]
  - Nick Papanikolaou [DCS, 3.27]
  - Tim Davidson [DCS, 3.27]
  - Various collaborations and research projects in UK + Europe
- Key Focus:
  - formal methods for modelling and verifying security of quantum cryptographic systems (and, more generally, quantum communication protocols)

Conclusion

- Quantum cryptography is a **major achievement** in security engineering.
- As it gets implemented, it will allow perfectly secure **bank transactions,** secret discussions for **government** officials, and well-guarded **trade secrets** for industry!
- Limitation: what happens at the endpoints…