Principles of Quantum Cryptography

Dr Basel Halak

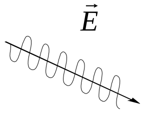
Learning Outcomes

At the end of this lecture you should be able to:

- Describe the Principles of Cryptographic Systems

Quantum Cryptography: The final battle?

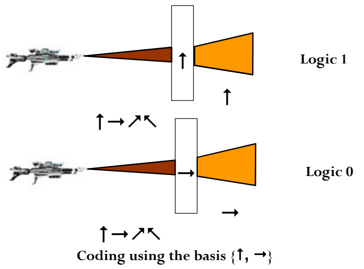
- **Polarization of photons can be though of as the** direction of oscillation of the electric field associated to a light wave



- **Representation of polarized photons:**
  - horizontally: →
  - vertically: ↑
  - diagonally: ↗ and ↖

Quantum Cryptography: The final battle?

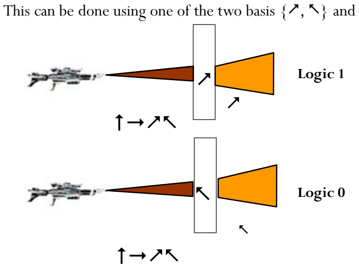
- Information can be encoded on each photon by giving it a particular polarization by passing it through a filter.
- This can be done using one of the two basis {↗, ↖} and {↑, →}.



Coding using the basis {↑, →}

Quantum Cryptography: The final battle?

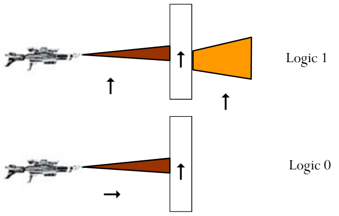
- Information can be encoded on each photon by giving it a particular polarization by passing it through a filter.
- This can be done using one of the two basis {↗, ↖} and {↑, →}



Coding using the basis {↗, ↖}

Quantum Cryptography: The final battle?

- Information can be decoded by measuring the polarization of each photon with respect to basis {↗, ↖} or {↑, →}.



Key distribution - BB84

- **BB84** is the first quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It works as follows:

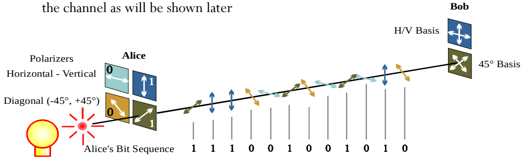
1. Alice and Bob first agree on two representations for ones and zeroes for each basis used, {↑,→} and {↗, ↖}. This agreement can be done in public: for example:

   1 = ↑ 0 = →

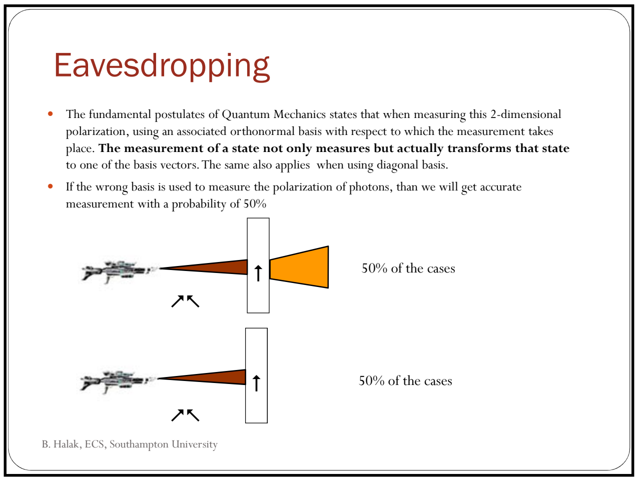
   1 = ↗ 0 = ↖
2. Alice sends a sequence of photons to Bob.
   Each photon in a state with polarization corresponding to 1 or 0, but with randomly chosen basis.

Key distribution - BB84

3. Bob measures the state of the photons he receives, with each state measured with respect to randomly chosen basis.
4. Alice and Bob communicates via an open channel. For each photon, they reveal which basis was used for encoding and decoding respectively. All photons which have been encoded and decoded with the same basis are kept, while all those where the basis don't agree are discarded.
5. Before Alice and Bob can use the key , they need to test the channel for eavesdropping, this can be done transmitting a random subset of the key and measuring e error rate of the channel as will be shown later



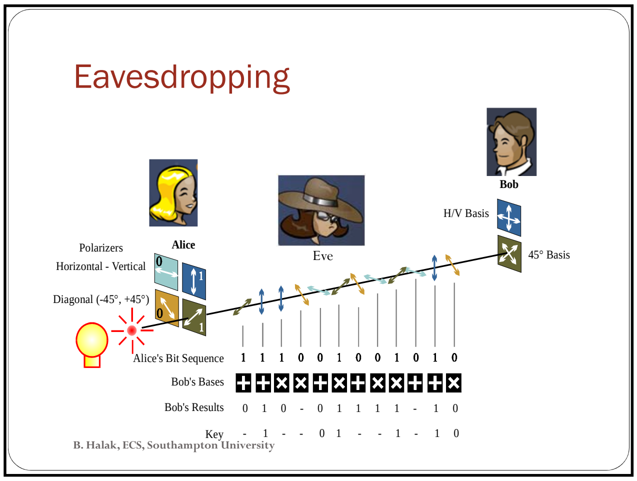
Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0



Eavesdropping

- The fundamental postulates of Quantum Mechanics states that when measuring this 2-dimensional polarization, using an associated orthonormal basis with respect to which the measurement takes place. **The measurement of a state not only measures but actually transforms that state** to one of the basis vectors. The same also applies when using diagonal basis.
- If the wrong basis is used to measure the polarization of photons, than we will get accurate measurement with a probability of 50%

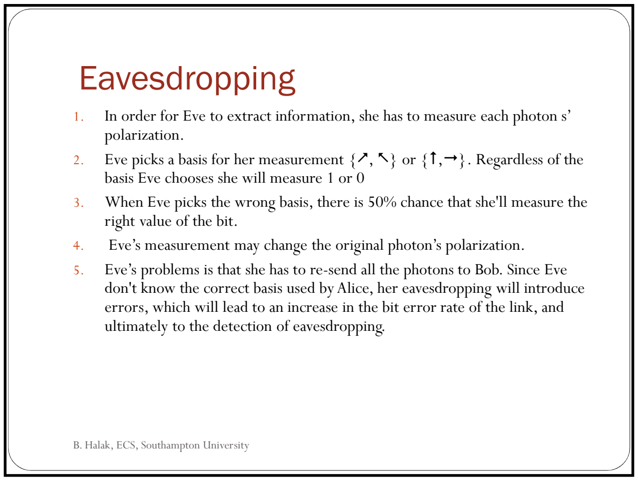
B. Halak, ECS, Southampton University



Eavesdropping

Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

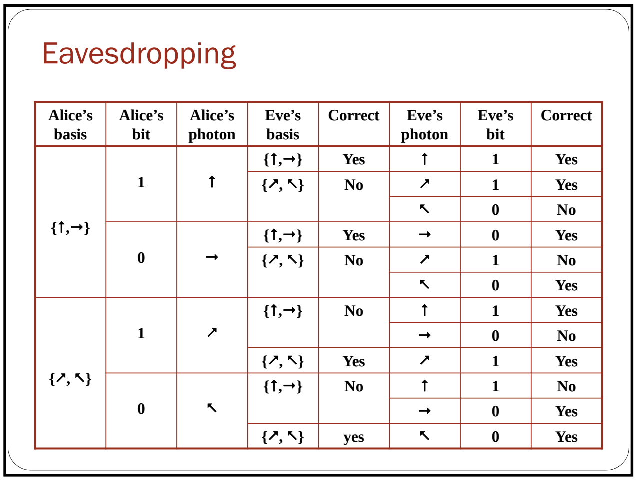
B. Halak, ECS, Southampton University



Eavesdropping

1. In order for Eve to extract information, she has to measure each photon s' polarization.
2. Eve picks a basis for her measurement {↗, ↖} or {↑,→}. Regardless of the basis Eve chooses she will measure 1 or 0
3. When Eve picks the wrong basis, there is 50% chance that she'll measure the right value of the bit.
4. Eve's measurement may change the original photon's polarization.
5. Eve's problems is that she has to re-send all the photons to Bob. Since Eve don't know the correct basis used by Alice, her eavesdropping will introduce errors, which will lead to an increase in the bit error rate of the link, and ultimately to the detection of eavesdropping.

B. Halak, ECS, Southampton University



Eavesdropping

Alice's basis	Alice's bit	Alice's photon	Eve's basis	Correct	Eve's photon	Eve's bit	Correct
{↑,→}	1	↑	{↑,→}	Yes	↑	1	Yes
			{↗, ↖}	No	↗	1	Yes
					↖	0	No
	0	→	{↑,→}	Yes	→	0	Yes
			{↗, ↖}	No	↗	1	No
					↖	0	Yes
{↗, ↖}	1	↗	{↑,→}	No	↑	1	Yes
					→	0	No
			{↗, ↖}	Yes	↗	1	Yes
	0	↖	{↑,→}	No	↑	1	No
					→	0	Yes
			{↗, ↖}	yes	↖	0	Yes

Detecting Eavesdropping

- After Alice and Bob agree on a key, they need to test for eavesdropping
- Alice and Bob randomly select a number of bits from the key and compute its error rate:

1. If error rate < E_{max} ⇒ assume no eavesdropping
2. If error rate > E_{max} ⇒ assume eavesdropping ⇒ discard the whole key and start over.

Where E_{max} is the maximum error rate on a particular channel.

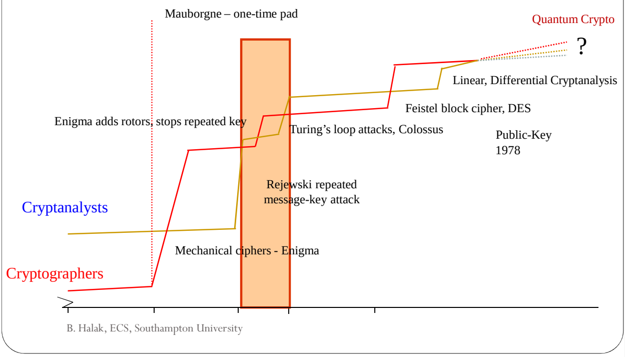
- Still possible for Eve to eavesdrop just a few photons, and hope that this will not increase the error to an alarming rate. If so, Eve would have at least partial knowledge of the key.

Commercial Implementation ..

- There are a number companies offering commercial quantum cryptography systems; id Quantique (Geneva), MagiQ Technologies (New York), SmartQuantum (France) and Quintessence Labs (Australia) and **QinetiQ** Farnborough, England.
- Quantum cryptography is coming to mobile phones

http://physicsworld.com/cws/article/news/2013/sep/02/quantum-cryptography-is-coming-to-mobile-phones

Cryptography : A Brief History (last 120 years)


Mauborgne – one-time pad
Quantum Crypto
?
Linear, Differential Cryptanalysis
Feistel block cipher, DES
Enigma adds rotors, stops repeated key
Turing's loop attacks, Colossus
Public-Key
Rejewski repeated
message-key attack
Cryptanalysts
Mechanical ciphers - Enigma
Cryptographers