Quantum Cryptography

by Ralfe Poisson

ralfepoisson@gmail.com Oct 2008

What the ...?

Quantum

an indivisible elementary particle, usually a photon

Cryptography

the practice and study of hiding information

Quantum Cryptography

the use of quantum mechanics to guarantee secure communication.

But Why?

- Key distribution in standard systems can be comprimised by eavesdropping.
- QC overcomes this by the magic of

• HEISENBERG'S UNCERTAINTY PRINCIPLE

- "locating a particle in a small region of space makes the momentum of the particle uncertain; and conversely, measuring the momentum of a particle precisely makes the position uncertain."
- This means that it is possible to detect eavesdropping and compensate for it.

So what is Quantum Mechanics?

Quantum Mechanics is the study of mechanical systems whose dimensions are close to the atomic scale. - http://en.wikipedia.org/wiki/Quantum_mechanics

Quantum effects, such as stable electron orbits, entaglement etc.. are not observable on a macroscopic scale, and exist only at the microscopic level.

Applications of Quantum Mechanics range from explaining features of the subatomic world to computational chemistry.

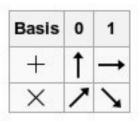
Current research is being done in the fields of Quantum **Cryptography**, Quantum **Computing**, and Quantum **Teleportation**.

Quantum Key Distribution

BB84 protocol

Charles H. Bennett and Gilles Brassard (1984)

Step 1: Alice sends Bob a string of encoded photons.



Step 2 : Bob measures the string of encoded photons using random bases (rectilinear or diagonal).

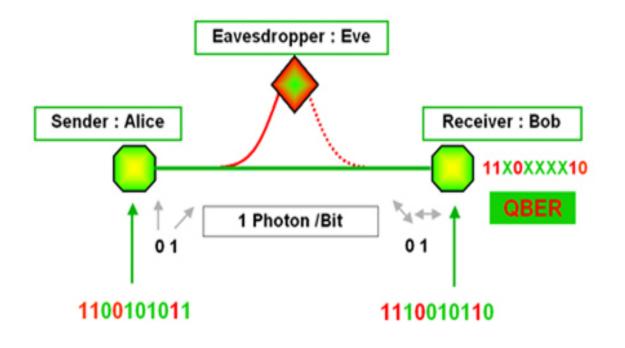
Step 3 : Alice and Bob publically compare the bases they encoded and measured in, and discard all results where they do not match.

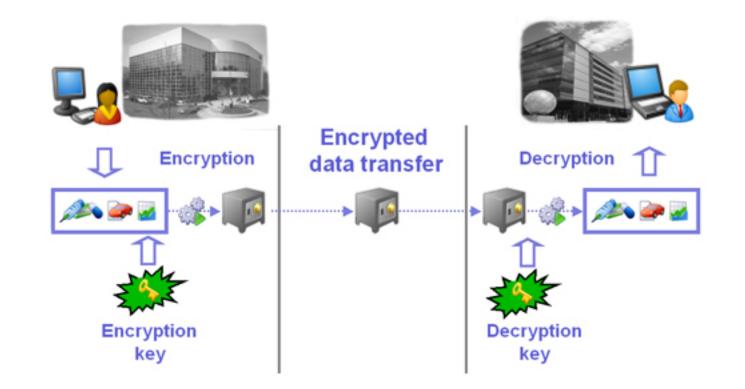
The result is the Shared Secret Key.



Here is the process Alice and Bob went through to generate their Shared secret key:

Alice's random bit	0	1	1	0	1	0	0	1	
Alice's random sending basis	+	+	×	+	×	×	×	+	
Photon polarization Alice sends	1	→	7	1	7	7	7	→	
Bob's random measuring basis	+	×	×	×	+	×	+	+	
Photon polarization Bob measures	1	7	7	7	\rightarrow	7	→	\rightarrow	
PUBLIC DISCUSSION OF BASIS									
Shared secret key	0		1			0		1	





Finding Eve

Problem

If an eavesdropper were to gain information about the photons' polarization, the laws of quantum physics dictates that the quantum state of the photons would be altered, thus causing errors in Bob's measurements.

Solution

Alice and Bob compare a subset of remaining bit strings. If more than p bits differ, the key distribution process is aborted and repeated.

Quantum Key Distribution (2)

E91 Artur Ekert (1991)

- Uses Entagled Pairs.
- Both Alice and Bob have one of the pairs.
- Any attempt at eavesdropping will destroy the entanglement such that Alice and Bob will detect the interference.

Privacy Amplification

As it is impossible to distinguish between eavesdropping and transmission imperfections, a threshhold p (currently 20%) is set for error margins.

If differences occur above the threshhold, privacy amplification can occur.

A new key is created by using Alice and Bob's key to produce a new, shorter key, in such a way that the eavesdropper's knowledge about the new key is negligible.

Information Reconcilliation

An alternative to Privacy Amplification whereby the parity of the measurements, subdivided into chunks, are compared.

If an error is found, a binary search is conducted to find and correct the error.

Welcome to the Real World

- 2004 World's first bank transfer using quantum cryptography in Vienna, Austria.
- 2004 DARPA Quantum Cryptographic Network in Massachusetts, USA.
- Mar 2007 BB84 implementation along 148.7 km fibre optic cable in Canary Islands.
- Oct 2007 Quantum Cryptography used in Geneva for Swiss elections.
- Oct 2008 World's first computer network protected by quantum cryptography implemented in Vienna.

Sieze and Destroy

Possible Attack Methods:

Intercept and Resend

eve intercepts alice and sends replacement to bob.

Security Proofs

loophole exists if true randomness is not used.

Man in the middle attack

if no authentication in place, this vulnerability still applies.

Photon number splitting attack

eve stores extra photons and uses these to form the key.

Hacking Attacks

direct tampering with protocol software or hardware devices.

Denail of Service

blocking the line or adding interference light to the cable.

Intercept and Resend

- Eve receives Alice's ecoded photon. If she guesses the base correctly, then she just has to encode a new photon and send it on to Bob.
- If Eve guesses incorrectly, she will just generate a new randomly encoded photon to send to Bob.
- Therefore, the probability an intercepted photon generates an error in the key string is 50% x 50% = 25%
- If n bits are compared, the number of bits required to detect an eavesdropper will be 72 key bits.

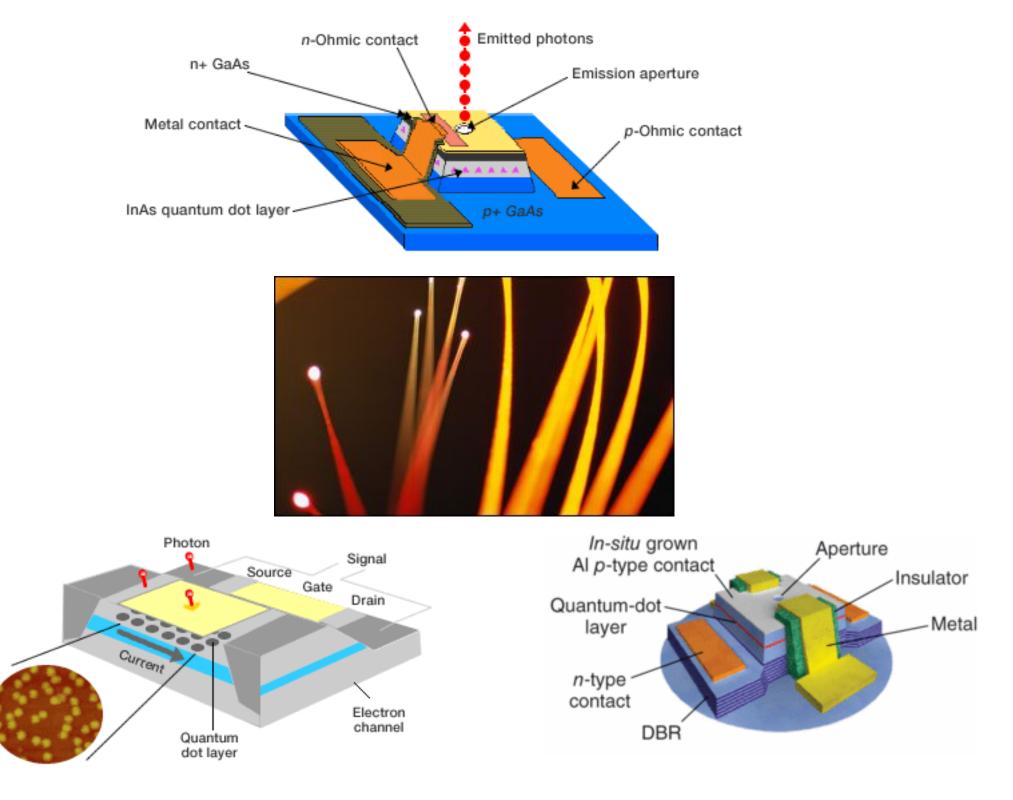
$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

Intercept and Resend

continued...

Example of Intercept and Resend Attack :

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	\times	+	×	×	×	+
Photon polarization Alice sends	1	→	7	1	7	7	7	\rightarrow
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	1	7	\rightarrow	1	\mathbf{Y}	\rightarrow	7	\rightarrow
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	1	7	7	7	\rightarrow	7	1	\rightarrow
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	1					1		1



Suppliers

id Quantique http://idquantique.com

MagiQ http://magiqtech.com

Quintessence Labs http://www.quintessencelabs.com

SmartQuantum http://www.smartquantum.com No balloon animals were harmed in the making of this presentation

References

Sharon Goldwater : Quantum Cryptography and Privacy Amplification <u>http://www.ai.sri.com/~goldwate/quantum.html</u> Wikipedia : Quantum Cryptography <u>http://en.wikipedia.org/wiki/Quantum_cryptography</u>

Gilles Brassard : A Bibliography of Quantum Cryptography http://www.cs.mcgill.ca/~crepeau/CRYPTO?Biblio-QC.html