Quantum Cryptography

David Thorne

November 14, 2002

1 The History of Cryptography

Classical digital cryptography is concerned with the problem of providing *secure* and *secret* communication over a medium which guarantees neither of these functions. This provision is achieved through the encryption of data at the sender, and the decryption of that cyphertext at the receiver (an encrypted message is known in cryptography as the *cyphertext* of the message). There are further considerations concerning cryptography such as fair exchange and non-repudiation, but these notions are separate to the security issue which we will be discussing here.

The majority of cryptographic techniques in common use today rely on the notion of computational complexity to ensure the difficulty (but not impossibility) of decrypting cyphertexts. Such methods make use of cryptographic *keys* to encrypt and decrypt data, and depending on the encryption chosen can be extremely secure[1].

The problem with this system is that the receiver must know which encryption was used by the sender in order to decrypt the cyphertext correctly. Obviously, this means that the decryption instructions (the decryption key) also need to be communicated from one party to another. Herein lies the quandary that quantum cryptography is looking to solve: the *Key Distribution Problem.*

2 The Quantum Perspective

Quantum Cryptography, which was first proposed by Stephen Weisner in the early 1970s, harnesses the Heisenberg Uncertainty Principle. Uncertainty is a major constituent in all quantum mechanics, and basically states the indeterminism of the universe around us. This indeterminism gives rise to certain mechanisms that can be put to great use in cryptography.

The first of those mechanisms specifies sets of conjugate pairs to which Heisenberg's uncertainty is bound, such as position and velocity. In fact, the principle states that if you could know with absolute precision the position of a particle then you could never know with any degree of certainty the velocity of that particle (and vice versa). Depending on how these quantities are measured, different aspects of the system can be quantified - for example, polarisation of photons can be expressed in any of three different bases: rectilinear, circular and diagonal. Measuring polarisation in the rectilinear base destroys the certainty of the other two bases (i.e. randomises the conjugates). It therefore follows, that if the data is encoded using these conjugate values, then the sender and receiver must use the same measurement base otherwise this randomisation will destroy any meaningful information. This is the mechanism that was used in Stephen Weisner's original proposal.

The second mechanism is derived from the absoluteness of indeterminism. This absoluteness states that whichever method you choose to measure the above conjugates and however cleverly you may try to cheat, uncertainty will always be preserved. This notion is so strong that quantum mechanics gives rise to (experimentally demonstrable) behaviour that is so counter-intuitive that it seems, to all but the most learned theorists, to break the laws of physics as we know them.

Fortunately, that same perplexing behaviour can be used to our advantage as will be explained later in this paper.

3 Practical Quantum Cryptography

In 1984, Bennett and Brassard designed a protocol (imaginatively named the BB84 protocol[1]) based on the above behaviour using four polarisation states that worked as follows. The sender encodes the information into quantum states using a random sequence of bases and transmits the information to the receiver. Each bit of this data will be in the form of a short burst of light, polarised using the said bases of measurement. The receiver then reads the incoming information using their own random sequence of bases. Once the data has been transferred, it only remains for the sender and receiver to publicly discuss which bases were used and in which order. Whenever the bases agree, it can be shown that the relevant bit of information is identical at both ends of the transfer, except in the following two situations:

- When random noise disrupts the data channel.
- When an eavesdropper attempts to intercept the data stream (Bucket brigade attack[2]).

This shared data, otherwise known as the *raw key*, could not be compared publicly otherwise the secrecy of that data would be compromised, so instead of comparing data, the normal step to take would be to recursively compare parity at different levels of coarseness (effectively a binary search for errors). Any errors detected are removed from the key. Once the parity is compared, the parity bits are also thrown away, hence making all publicly available data redundant.

What is left after this protocol is carried out is a shared sequence of bits that can only be known by the two parties involved (the *reconciled key*). This secret key can then be used to encrypt and decrypt the data communication, with full certainty that the data transmitted will be secure.

4 A Chink in the Armour

There is one insecurity with the above protocol and this is based on the nature of light, in particular on the nature of the bursts of light used to encode the transmitted data. The fundamental particle of light is the photon, a finite packet of energy that cannot be split, and each of the above bursts of light are made up of an arbitrary number of these photons (depending on the energy of those bursts). In our protocol, a burst of light will almost certainly contain many thousands of photons. It is therefore technically possible to 'shave off' a couple of photons and decode them, without affecting the photons that get through to the legitimate receiver.

This means that eavesdropping is technically possible. Luckily for most usages, the actual act of shaving off those photons would destroy the data for both eavesdropper and receiver. However, with highly precision instruments and sufficient experience, eavesdropping could feasibly take place.

5 Evolved Cryptography

Since the conception of quantum theory, there have been countless breakthroughs and one such leap has been that of 'quantum entanglement' which was first proposed back in 1935 in a paper by Einstein, Podolsky and Rosen[3]. This area of quantum theory states that you can create two 'entangled' particles (an EPR pair) such that the measurement of a chosen observable property of one particle automatically determines the result of the measurement of that property for the other particle. This entanglement holds for *all* situations, even those where the particles are separated by vast distances. This leads to the great "action at a distance" paradox.

This theory has allowed for a new form of quantum cryptography based on the absoluteness of the above stated entanglement. Ekert's 1991 proposal for such a protocol[4], works as follows. An EPR pair transmitter is placed between the sender and receiver. One of the pair of particles is detected by each of the parties (sender and receiver) using a random sequence of bases, and so will produce identical data when both bases agree. This relation will hold under *all* circumstances, except for random noise and when an eavesdropper attempts to intercept the data stream, in which case the quantum correlation of the particles is destroyed. One important distinction between this protocol and that of BB84 is the detection of an eavesdropper. Instead of recursively checking the raw key, it is the information discarded due to base discrepancies that is used (the *rejected key*). A mathematical theorem known as Bell's Inequality[5] is used, which is based on the indeterminism of quantum theory, to check to see if an eavesdropper was present. Once both parties are satisfied that no eavesdropper was present, they then continue to check the raw key for random noise using the same process as for BB84.

One important point to note is that as the vessel of communication is effectively one photon per bit of information, the above stated 'chink in the armour' does not apply. This is because it is impossible to split a photon, and so eavesdropping of any kind will *guarantee* that the photon will be affected on a quantum level and so be detected.

6 Summary

Quantum Cryptography, as has already been explained, is based on sound physical phenomena. Although these phenomena can be somewhat counter-intuitive, they have a strong basis and have been shown experimentally to be correct. Just as with classical cryptography, the security of a particular quantum protocol can be mathematically evaluated. Although a full description of such evaluations is beyond this paper, it suffices to mention that all the above mechanisms can be *proved* to be be secure (either absolutely or effectively) using mathematical and physical concepts[6].

Quantum key distribution is currently an active area of research and as such has seen steady progress in the years since it was first formulated. So far there have been a number of proposed protocols, each with its strengths and weaknesses, and each relying on some quantum mechanism to provide its security in detecting an eavesdropper. The following list shows the most common of those protocols.

- **BB84** - Relies on Weisner's "Conjugate coding" proposal and uses four polarisation states[1].
- **B92** - Similar to BB84 but only uses two polarisation states[7].
- **EPR entanglement** - Uses Bell's Inequality and quantum entanglement [4].
- **Interference phase drift** - This protocol uses the mechanism of interference to ensure security[8]. Eavesdropping would cause any interference to be destroyed, and so can be detected.

In addition to this, the above protocols have all been applied experimentally. The first working prototype, constructed in 1989 at IBM in Yorktown Heights, New York and using the BB84 protocol, transmitted quantum signals over 32 cm of open air. However modest, this was the beginning of a decade of experiments into the application of quantum cryptography. In this decade, there have been many fundamental improvements to the equipment required by such a system. Photon sources have become much better at creating clean bursts of light, and photon detectors have become ever more sensitive. These along with better fibre optic cabling technologies have drastically increased the effective range of such protocols.

Using fibre optic cables, the world record for effective quantum cryptography is currently an impressive 67km - and in fact is already commercially available[9]. In open air, the maximum distance for a successful transfer has been increased to approximately 1.6km and employs the B92 protocol.

Although impressive considering the technology involved, these distances are not really sufficient for a commercially viable solution. Until they can match conventional cryptographic techniques in distance (that can be used over any distance of cabling or through any distance of open air) they cannot be a true contender. So despite the impressive improvements that have been made over the last couple of decades, there is still a long way to go before quantum cryptography will become widely used. In summary, the following areas need to be developed further:

- The distance with which quantum cryptography is a practical solution must be increased to at least that of currently used systems.
- Quantum protocols must be incorporated into current network technologies, so that a more transparent use can be made of the technology, and by a wider group of users.
- However well the intrusion techniques used here may seem to work, unfortunately we do not currently have a great enough understanding of intrusion and detection techniques to confidently say the protocols are uncrackable.
- The intrusion detection algorithms used here are not very efficient, and always leave room for possible errors. So far, we have been accepting these as 'small enough risks'. In order to be totally secure though, more extensive algorithms will be needed.

Notes

[1] Though such techniques will never be entirely secure, it can be shown that a sufficiently complex algorithm can make a cyphertext *almost* impossible to break. As an example, an algorithm that uses a 128 bit secret key and ensures that each bit of output relies on *every* bit of input could be used. Such a set up, assuming that both brute force and parallelism are employed, should be safe: a billion computers doing a billion operations a second would require a trillion years to decode the cyphertext.

[2] Otherwise known as opaque eavesdropping, or the 'Man-in-the-middle attack'[2]. In this situation, the eavesdropper transparently relays all incoming data from the sender to the receiver. Luckily with quantum cryptography, this act of relaying data causes the randomisation of the data stream (as the photons received by the receiver are not exactly the same photons that are sent by the sender).

References

[1] Charles H. Bennett, Gilles Brassard: **Quantum cryptography: Public key distribution and coin tossing**, International Conference on Computers, Systems & Signal Processing, Bagalore, India, December 10-12, 1984, pp175-179

[2] A. K. Ekert, B. Huttner, G. M. Palma, A. Peres: **Eavesdropping on quantum cryptographical systems**, Physics Review A, Vol. 50, No. 2, August 1994, pp 1047-1056

[3] A. Einstein, B. Podolsky, N. Rosen: **Can a quantum mechanical description of physical reality be considered complete?**, Physical Review 47, 777 (1935)

[4] A. K. Ekert: **Quantum cryptography based on Bell's Theorem**, Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661-663

[5] J. S. Bell: Physics, 1, (1964), pp 195-200

[6] S. J. Lomonaco Jr: **A quick glance at quantum cryptography**
http://www.cs.umbc.edu/∼lomonaco/Publications.html

[7] Charles H. Bennett: **Quantum cryptography using any two nonorthogonal states**, Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121-3124

[8] Alexey Brylevski: **Quantum key distribution: Real-time compensation of interferometer phase drift**, Masters Thesis, Norwegian University of Science and Technology, February 2002

[9] **id Quantique**, http://www.idquantique.com/