The Use of Quantum Mechanical Effects to Provide Greater Security in Data Communication

Thomas Taylor
tt36@uni.brighton.ac.uk

School of Computing, Engineering and Mathematics,
University of Brighton.

Abstract. A considerable weakness of current cryptographic techniques lies in the fact that they rely upon the inability for current generation hardware to factor large numbers in polynomial time. With the discovery of a quantum algorithm capable of solving such a problem, we discuss how quantum effects can be utilised to provide an alternative and more secure method of cryptography.

1 Introduction

The primary concern when it comes to accessing sensitive data is *privacy.* More specifically, how to enable secure, private communication between two parties such that any intermediaries listening in to the transmission are unable to obtain any useable information from it[6]. Given the increasing amount of sensitive data accessible over the internet such as medical records, personal banking and employee payrolls, in addition to the number of social networks and other online services which store individuals' personal data, cryptography and data security has never been more important.

The fact that the classical[1] cryptographic systems that we rely on so heavily to secure our sensitive data are still completely reliant on the performance limitations of current generation hardware is not an ideal situation. Such techniques can easily be broken given enough time and computing power. Whilst this does not prove problematic with today's hardware, the recent developments in computer systems capable of quantum computation[4], and the existence of quantum algorithms capable of providing polynomial speed up of integer factorisation[7], modern cryptographic techniques are looking ever more vulnerable to attack, and the need for more secure forms of cryptography are becoming increasingly apparent.

[1] The term 'classical' is used in this paper to refer to computer and cryptographic systems which do not utilise quantum mechanical effects (i.e. all modern systems used today).

2 Quantum Mechanical Concepts

There are a number of key quantum mechanical principles which are utilised in quantum cryptography and specifically in quantum key distribution (QKD). Brief explanations of concepts relevant to the later sections are given here.

2.1 Quantum bits and Quantum States

In classical computing, binary digits (or bits) form the basic building blocks of data. The quantum bit (or qubit) is the quantum computing equivalent, and acts both as a processor as well as memory.

While in classical computing, a bit is capable of existing in one of only two states (0 and 1), in quantum computing, the qubit can exist in a 0 or 1 state, or as a superposition of both these two states ****(the superposition state is essentially an infinite number of in-between states)****. Unlike a classical bit, which is capable of existing in only one state at any one time, before a qubit is measured, it is said to exist in all of its states at once. However, as soon as the qubit is measured, it transitions to a single state. The fact that a qubit changes its state when measured is a very useful behaviour, and is utilised very effectively in QKD, which is described later in section 5.

2.2 Quantum entanglement

Quantum entanglement is another unique quantum mechanical behaviour observed when multiple qubits interact with one another. When coming into contact, the qubits are said to have become 'entangled'. Just as individual qubits have a 'superposition' state, so too do the entangled qubits, which can be described as a superposition of the superposition state of the qubits****citation****.

This interaction causes the two qubits to become associated with each other in such a way that if a measurement of either of the pair is made (with its state being altered as a result), the state of the other qubit is also changed to the complementary state of its partner. This behaviour occurs irrespective of the distance between the qubits.

3 Asymmetric Key Cryptography (Public Key)

The asymmetric (or public key) method is the most popular cryptographic technique used today, and underpins many integral internet standards such as Transport Layer Security (TLS), GNU Privacy Guard (GPG), and Pretty Good Privacy (PGP).

One of the main benefits to using the public key system is that the generation of the keys and the encryption/decryption processes are trivial for the sender and receiver, whereas it is incredibly expensive computationally for an attacker to decypher the message. The use of public keys also removes the need for a secure private exchange of keys between participants, which is a requirement for some other cryptographic methods (such as the symmetric key method).

The security of public key cryptography lies in the fact that it is currently incredibly computationally expensive (and therefore infeasible) to factor very large numbers, or at least to do so in a useable timeframe. However, this could also be viewed as a disadvantage, given the fact that any public key algorithm can be broken fairly trivially provided that the time and computational power available are not a limiting factor.

4 Integer Factorisation

In classical computing, the most efficient algorithm currently available for factoring numbers with more than 100 digits is the general number field sieve (GNFS). The GNFS algorithm has running time which while sub-exponential, is still super-polynomial in the size of the input. To give an idea of what this means in real terms, researchers concluded an experiment in December 2009 into the breaking of an RSA-768 number (consisting of 232 digits) using the GNFS algorithm. It took the team a total of 2 years to factor the number, with their estimation being that to break an RSA-1024 number would be a thousand times harder[3].

****Given these figures, it appears that the public key methods still seem fairly secure,**** especially given that there is always the option to use larger numbers. Although this is true to a certain extent, simply using larger numbers does not provide a solution to the problem.

The vulnerability of public-key based systems was further amplified in 1994, when Peter Shor discovered a quantum algorithm which was capable of factoring integers in polynomial time[7] (which provided an exponential speed-up over the general number field sieve). Suddenly the public-key cryptographic techniques which had become a standard looked susceptible to attack. Although the development of quantum computers capable of such powerful computation is still in its infancy, the fact that such computation is theoretically possible is extremely dangerous to the integrity of our sensitive data.

Shor's discovery was further substantiated in 2001 when researchers at IBM demonstrated the algorithm on a practical quantum computer by factoring 15 using 7 qubits[10]. Although this demonstration was disregarded by some due to the fact that no quantum entanglement had been observed, subsequent experiments have since been carried out which support IBM's findings[4].

5 Quantum key distribution

With the discovery of Shor's quantum algorithm suddenly rendering the public key method insecure (in theory at least), there was a need to develop new cryptographic techniques which could utilise the same quantum mechanical concepts in order to provide more secure data transmission. QKD provides a solution to this problem.

QKD functions in a similar way to public key cryptography, but makes use of quantum effects to ensure much greater privacy:

The first step is for the sender 'Alice' to encrypt the intended message using a secret key generated from a random quantum state. The message is then sent to the intended recipient: 'Bob'. Upon receipt of the transmission, Bob measures the data using his own quantum-state-key. The two parties then publicly communicate to each other the method that they used to prepare (or measure) the transmission. From this, they are able ascertain which bits of the transmission were prepared in the same way, and collate these bits into a new string. Provided there was no interference, these two strings should be identical to one another, although in practise, a transmission is considered secure if it has an error rate of considerably less than 25%[9]. Any eavesdroppers attempting to gain access to the transmission will make their evidence known to Alice and Bob due to the fact that merely measuring the state of the transmission causes it to change its state, thus increasing the error rate.

One of the biggest advantages to using QKD over existing public key systems is the fact that the data transmission is protected by the laws of quantum physics, as opposed to public key methods whereby computational complexity and the performance of current systems is all that ensures the security. In addition, QKD systems are able to utilise quantum entanglement to detect whether the transmitted message has been compromised by a third party, something not possible with the public key method. Importantly, QKD still allows public channels to be used to transmit the data, which is a much less costly solution than having to communicate via private channels. This also opens up the opportunity to use QKD as a method for surface-to-satellite, satellite-to-satellite or potentially even deep-space communication.

Although rigorous mathematical proofs have been established which seemingly confirm the security of QKD[1][8], researchers at the University of Toronto have recently shown that it is not only possible, but technologically feasible using *current* technology to mount an undetected attack against a *commercial* QKD system. Known as a time-shift attack, an eavesdropper 'Eve' can exploit the efficiency of detectors used to receive the transmission to break the security of the system[11]. Although these commercial solutions have been proven insecure, it is important to note that the commercial QKD systems 'deviate from the models in the security proofs'[5]. Most surprising about this discovery though, is that Zhao et al's proposed attacker was much weaker than the one proposed in the original security proofs; the attacker proposed in the paper was unable to 'perform a quantum non-demolition (QND) measurement on the photon number or compensate any loss introduced by the attack', while the attacker in the proofs could have 'arbitrarily advanced technology'. Using this method, Eve might be able to ascertain the whole key, or at least to obtain enough of the key for a brute force attack to prove successful.

6 Conclusion

Theoretically, QKD provides an unconditionally secure method of data transmission, regardless of what technology an attacker might possess; its security is guaranteed by the laws of quantum physics. Whereas classical methods are reliant on computational complexity.

However, while the theory behind QKD has been rigorously tested on paper, there have yet to be any viable implementations of such a system. This, combined with the fact that we have yet to see a quantum computer system developed which is capable of performing functions even remotely close to the complexity of those of current generation hardware, such a cryptographic system still seems likely to be a way off.

References

1. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanperra. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996.
2. R. Hughes, C. Williams, and R. Doyle. Quantum computing: The final frontier? *IEEE Intelligent Systems*, September/October, 2000.
3. T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. Te Riele, A. Timofeev, and P. Zimmermann. Factorization of a 768-bit rsa modulus. In *Proceedings of the 30th annual conference on Advances in cryptology*, CRYPTO'10, pages 333–350, Berlin, Heidelberg, 2010. Springer-Verlag.
4. C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.*, 99(25), December 2007.
5. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10), 2010.
6. R. L. Rivest. *Handbook of Theoretical Computer Science*, chapter 13. The MIT Press, 1990.
7. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring, 1994.
8. P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000.
9. A. Steane. Quantum computing. Technical report, University of Oxford, 1997.
10. L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, 12 2001.
11. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A.*, 78(4), October 2008.