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 have never been more important.

With data security of such paramount importance, it is surprising to see that the classical[1] cryptographic systems we use today still rely on computational complexity as their best line of defence. Breaking such techniques becomes a fairly trivial matter given enough time and computing power. Whilst this does not prove problematic with today's hardware, with the recent developments in computer systems capable of quantum computation [4], as well as the existence of a quantum algorithm capable of factoring large integers in polynomial time [7], modern cryptographic techniques are looking ever more vulnerable to attack. The need for alternative forms of cryptography which can offer better long-term security is 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 in order to provide a greater level of security than is possible using classical techniques. 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, acting 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), the qubit can also exist in an additional 'superposition' state, which is essentially a combination of the qubit's other states. This is best envisioned using an 'energy wave' analogy: if you add two waves together, the result is a third wave which is a combination of the two original waves. This third wave is essentially a 'superposition' of the two initial waves, as it exists with the energy of the first two waves simultaneously. When a qubit in the superposition state is measured however, it collapses, and the qubit transitions to a single state.

It is this unusual behaviour which is utilised very effectively in quantum key distribution, 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'. 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 is known to occur irrespective of the distance between the qubits [10].

3 Asymmetric Key Cryptography (Public-Key)

The asymmetric key (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 major benefits to using the public-key system is that whilst the generation of the keys and the encryption/decryption processes are trivial for the sender and receiver, it is incredibly expensive computationally for an attacker to decipher the message. Even further security can be provided by using larger keys, and by changing the keys regularly. 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 strength 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 time-frame. However, this could also be viewed as a disadvantage, given the fact that any public-key system can be broken fairly trivially provided that time and computational power are not limiting factors.

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 a 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 breaking an RSA-1024 number would be a thousand times harder [3].

Although these findings could easily lead one to believe that the security of the public-key method is assured for some time to come, the fact that their strength relies on computational complexity means that an unforeseen advancement in computer hardware could severely compromise its security.

This vulnerability was further amplified in 1994, when Peter Shor discovered a quantum algorithm which was capable of factoring integers in polynomial time, providing an exponential speed-up over the general number field sieve algorithm [7]. With this discovery came the realisation that as soon as sufficiently powerful systems capable of quantum computation became available, attackers would be able to efficiently break into public-key systems, effectively rendering them completely insecure. 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 [11]. 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 finally rendering large-number integer factorisation a feasible possibility, 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. Quantum key distribution (QKD) provides a solution to this problem. QKD functions in a similar way to

public-key cryptography, but makes use of quantum states and quantum entanglement to ensure much greater privacy.

As with the public-key method, the first step of QKD is for the sender to encrypt the intended message, which is done using a secret key generated from random quantum states chosen by the sender. The message is then sent to the intended recipient who, upon receipt of the transmission, 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 qubits of the transmission were prepared in the same way, and collate these qubits into a new string. Any intermediaries listening in must first measure the transmission, thus causing the state of any measured qubits to change as a result. This will become immediately obvious to the communicating parties who will detect an unusually high error-rate when comparing the two strings. Provided there was no interference during the transmission, and assuming that the transmission was not intercepted by a third party, one would expect these two strings to be identical to one another. However in practice, a transmission is highly unlikely to be completely error-free, and so is considered to be secure if it has an error-rate of less than 25% [9].

One of the biggest advantages to using QKD over existing public-key systems is that the transmission of data is protected by the laws of quantum physics rather than computational complexity, meaning that its security will be ensured regardless of any unforeseen technological advances in the future. In addition, as previously mentioned, QKD systems are able to effectively utilise quantum entanglement in order to allow the two communicating parties to detect the presence of any third parties; something not possible with existing classical methods. Another key benefit of QKD is that it still allows public channels (for example, Wi-Fi networks) to be used to transmit the data, which is a much less costly solution than having to communicate via private channels. This also means that QKD could have a use in secure satellite communications. The importance of ensuring the security of satellite communications was emphasised in 1986, when a US television satellite was hijacked by a computer hacker known as 'Captain Midnight' [2].

With various rigorous mathematical proofs having been established which confirm the security of QKD[1, 8], it clearly offers a promising new method of cryptography. In fact, there are already several companies which are currently offering commercial QKD systems. However, major flaws have been found in these commercial systems which mean that a third party is able to manipulate quantum mechanical effects to eavesdrop on the transmission undetected [12, 13]. For example, researchers at the University of Toronto led by Yi Zhao 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 is able exploit the efficiency of detectors used to receive the data transmission and gain access to its information content. Most surprising about this discovery is that their proposed attacker was much weaker than the one proposed in the original security proofs,

which could have 'arbitrarily advanced technology'. Using the time-shift attack, the eavesdropper might be able to ascertain the whole key, or at least enough of it for a brute force attack to prove successful.

Although these commercial solutions have been proven to be insecure, it is important to note that the systems in fact 'deviate from the models in the security proofs' [5], and so do not invalidate the underlying concept of QKD.

6 Conclusion

With so much sensitive data accessible over the internet, it is critical that the methods we use to transmit that data are suitably secure. While the public-key systems that we use today are well protected against attacks from current generation hardware, they cannot provide the same kind of guarantee against the quantum-based systems which are currently being developed.

QKD proves to be a promising candidate as a successor to the existing public-key method. In addition to relying on the laws of quantum physics for security rather than computational complexity, QKD also allows the communicating parties to detect the presence of any third parties; a key benefit over any classical cryptographic methods.

However, although QKD has been proven secure in theory, there have yet to be any practical solutions developed which provide a true demonstration of the method, and that provide the kind of unconditional security proposed in the original proofs, although this is something which is likely to change as practical quantum computing systems are developed.

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. *Reports on Progress in Physics*, 61(2):117–173, 1998.
10. M. Tegmark and J. A. Wheeler. 100 years of quantum mysteries. *Sci.Am.*, 284:68–75, 2001. An abbreviated version of this article, with much better graphic, was published in the February 2001 issue of Scientific American, p.68-75.
11. 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.
12. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1), 2011.
13. 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.