The Use of Quantum Mechanical Effects in Cryptographic Techniques

Thomas Taylor
tt36@uni.brighton.ac.uk

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

Abstract. The biggest weakness of current cryptographic techniques is that they rely upon the inability for current generation hardware to factor large numbers in a useable time-frame. With recent advances in making physical quantum computers a reality, it's becoming increasingly likely that we will soon have hardware capable of applying quantum mechanical algorithms to break classical cryptographic techniques.

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 adversaries that may be listening know nothing about what has been communicated[6]. Given the increasing amount of sensitive data accessible over the internet such as medical records, personal banking and employee payrolls, not to mention the number of social networks and other online services which store individuals' personal data, cryptography and data security has never been more important.

It is somewhat surprising then that the classical cryptographic techniques that we use today are still largely reliant on the performance limitations of current generation hardware; such techniques can be easily broken given enough time and computing power. Whilst this does not prove problematic with current hardware, the recent developments in computer systems capable of quantum computation, 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.

2 Quantum Mechanical Concepts

2.1 Quantum bits and Quantum States

In classical computing, binary digits (or bits) form the basic building block 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), in quantum computing, the qubit can exist in a 0 or 1 state, or as a superposition of both these two states (essentially an infinite number of in-between states).

2.2 Quantum entanglement

Quantum entanglement is a unique behaviour observed when two qubits come into contact. When coming into contact, the pair of qubits are said to have become 'entangled'. Just as individual qubits have a 'superposition' state so too do entangled qubits, which is essentially a superposition of the superposition state of the two qubits.

[MORE INFORMATION NEEDED]

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

3 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 whose running time, while sub-exponential, is still super-polynomial in the size of the input. In December 2009, researchers concluded an experiment into the breaking of an RSA-768 number of 232 digits, using the number field sieve 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 this method has so far proven secure for obvious reasons and using larger numbers would provide greater security, this is not a preferable solution.

When Peter Shor discovered a quantum algorithm in 1994 which was capable of factoring integers in polynomial time[7], suddenly the public-key cryptographic techniques which had become a standard looked vulnerable to attack. Theoretically, the discovery of Shor's algorithm meant that

This was further proven in 2001 when IBM demonstrated the algorithm on a practical quantum computer by factoring 15 using 7 qubits[Citation?]. Although this demonstration was disregarded by some as no quantum entanglement had been observed, subsequent experiments have since been carried out which support IBM's findings[4].

4 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. Public keys also remove the need for a secure exchange of keys between participants, as with some other cryptographic methods.

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 is also the biggest drawback of using public key, as any public key algorithm can be broken fairly trivially given enough computing power and time.

5 Quantum key distribution

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

The sender 'Alice' first encrypts each bit of the message using a key generated from a random quantum state (as chosen by Alice), and sends the message. When the second party 'Bob' receives the transmission, he measures the data using a similarly random key. The two parties then publicly state the method chosen to prepare or measure the message. From this, they can ascertain which bits 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 of the message would cause qubits to become corrupted, as their mere measurement causes them to change state as mentioned earlier. Therefore, Alice and Bob can discover if the data has been compromised.

The biggest advantage to using QKD over existing public key systems is the fact that the data transmission is protected by the laws of physics, rather than computational complexity, and the performance of current systems.

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[10]. 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 is that Zhao et al's proposed attacker is much weaker than the one proposed in the original security proofs; the attacker proposed in the paper is 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 can have 'arbitrarily advanced technology'.

The real point of weakness in a QKD system is the public communications that are required for Bob and Alice to tell each other how they made their measurements. In principle, you can learn nothing beyond the number of bits sent, and which bit positions can be used to generate a secret key unless, two conditions are met: Eve must control the arrival time of the bits at Bob's detectors, and Bob's detectors must not be identical. The first condition is easily met if you insert switches and rolls of fiber optic cable and a few other optic devices to keep the optical pulse length rightactually, making it shorter is even better, and this is possible also. The second condition is always met. No two detectors are ever exactly identical. From Bob and Alice's communication, Eve might get the whole key, or at least enough of it so that a brute force attack can succeed.

6 Conclusion

- Summarise the paper
- Discuss Future Technology/Application of Quantum Cryptography
- Discuss that although methods have been proven insecure, new methods will no doubt be developed (also note that only current commercial techniques have been broken, doesn't change the validity of the theoretical concept)

– NASA Earth to space/satellite communication[2]:

> There will often be the need for onboard capability to process information, make decisions, and sometimes, replan elements of the mission in real time. Unfortunately, planning is an NP-Hard problem, so fine-grained replanning quickly consumes available computational resources.
>
> Currently, no known algorithm (classical or quantum) can solve NP-Hard problems in better than exponential time in the worst case. But it appears that quantum algorithms can be faster than classical ones by a significant factor.

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. 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.