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.

1 Introduction

The primary concern when it comes to accessing sensitive data is *privacy*; how to enable secure, private communication between two parties such that any adversaries that may be listening know nothing about what has been communicated[10]. Given the increasing amount of sensitive data accessible over the internet such as medical records, personal banking and 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.

Given the importance of ensuring data security over the internet, it is somewhat surprising that the modern (classical) cryptographic techniques that we use today are still largely reliant on the current inability to factor very large numbers within a usable time-frame; such techniques can be easily broken given enough computing power. While this does not prove problematic with current generation hardware, with the recent developments in computer systems capable of quantum computation[citation needed], and the existence of quantum algorithms capable of providing polynomial speed up of integer factorisation[11], modern cryptographic techniques are looking ever more vulnerable to attack, and the need for more secure forms of cryptography are becoming increasingly apparent.

1.1 Asymmetric Key Cryptography (Public Key)

One of the most widely used methods of cryptology is asymmetric, or public key cryptography. First proposed by Whitfield Diffie and Martin Hellman in their now seminal 1976 paper *Multi-user cryptographic techniques*[2], public key cryptography introduced the notion of using two different (but mathematically related) keys to secure data communication. One of these keys is used in the encryption process, and the other for decryption. One of the keys is made public, and is used to generate a public-private key pair by the participants. First, the sender encrypts the message using the public key of the recipient. The recipient then uses their own private key to decrypt the message.

One of the main benefits to using this system is that the generation of the keys and the encryption/decryption processes are trivial for the sender/reciever, 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 exchange of keys between participants, as with some other cryptographic methods.

The public key technique proved so effective, that it now underpins many integral internet standards such as Transport Layer Security (TLS), GNU Privacy Guard (GPG), and Pretty Good Privacy (PGP).

Public Key Algorithms: ??????

- Diffie-Hellman
- RSA
- Cramer-Shoup
- ElGamal
- Elliptic Curve

2 Integer Factorisation

In classical computing, the factoring of large numbers is very computationally expensive; 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[4]. Although this method has proven secure, simple using bigger numbers to increase security is not a preferable solution.

When Peter Shor discovered a quantum algorithm in 1994 which was capable of factoring integers in polynomial time[11], suddenly the public-key cryptographic techniques which had become a standard looked vulnerable to attack.

Then in 2001, 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 been since carried out which support IBM's findings[6].

Shor's Algorithm Explanation????

3 Quantum Mechanical Concepts

3.1 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.

3.2 Quantum entanglement

When two qubits come into contact with each other and interact, the pair of qubits are said to have become 'entangled'. Just as individual qubits have a 'superposition' state, which is essentially a superposition of the superposition state of the two qubits.

This interaction causes the qubits to become related in such a way that if a measurement of either of the pair is made, its state is changed. This measurement also causes the other qubit of the pair to change to the complementary state of its partner, irrespective of distance.

It is this behaviour which underpins the concept of quantum bit commitment, which is discussed later.

4 Quantum Cryptography

As practical quantum computers are developed, existing classical cryptographic techniques will no longer provide secure communication. Quantum cryptography however, aims to guarantee 100% security. It is able to do this due to the fact that unlike classical cryptographic methods, it relies on the laws of quantum physics to provide secure transmissions, rather than mathematical functions and computation complexity.

Quantum cryptography is usually divided into two sub-areas: quantum bit commitment, and quantum key distribution.

4.1 Quantum bit commitment

The concept of quantum bit commitment refers to the ability for a person Alice to 'commit' a value and transmit this to another party Bob, without Bob being able to discover the value of the data until Alice decides to reveal it.

This technique relies on quantum entanglement to function; the fact that merely listening in on a quantum message alters the nature of the quantum system, thus is easily detected by the parties sending and receiving the message. The most obvious application for this method of cryptography is in election scenarios, where voters can place their vote in such a way that no-one is able to discover the contents of the vote until the voter specifies, while still providing proof that that voter has indeed place their vote in a specific timeframe.

However, this technique, though long thought to be secure, has since been proven to be insecure[5][8][9].

4.2 Quantum key distribution

Look at different techniques/algorithms, research. Whether it's viable. Discuss current commercial solutions.

1 We can encrypt message (plaintext) (P) according to some algorithm (E) before transmission to produce a ciphertext, C = EK(P), where K is a secret parameter known as a cryptographic key (a random binary number sequence, typically a few hundred bits in length)

2 On receiving the ciphertext, the intended recipient can invert the encryption process using the decryption algorithm (D) to recover the original message P = DK(C), provided the secret key K is known.

3 Although the encryption and decryption algorithms E and D might be publicly known, an eavesdropper passively monitoring the transmission C could not discern the underlying message P because of the randomization the encryption process introduced, provided the key K remains secret.[3]

Although rigorous mathematical proofs have been established which confirm the security of quantum bit commitment[1][12], 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 (known as the time-shift) against a *commercial* quantum key distribution system.[15].

The concept of the time-shift attack:

> Eve can shift the arrival time of each signal to either A or B randomly with probabilities pA and pB = 1 ? pA respectively. Eve can carefully choose pA to keep the number of Bobs detection events of 0s and 1s equal. Since Bobs measurement result will be biased towards 0 or 1 depending on the time shift (A or B), Eve can steal information without alerting Alice or Bob.
>
> Most surprising about this discovery is that Zhao et al's proposed attacker is much weaker than the one proposed in the security proofs; the attacker 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'.
>
> Similarly, fjdskfljdsfkldsjfsdkl[14] and fdjsfjdsklfkjldsfjdslk[7]
>
> This method was successfully trialled using a computer system developed by Id Quantique during the Swiss canton of Geneva parliamentary elections in 2007[citation].

5 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

– Secure voting (bit commitment)
– NASA Earth to space/satellite communication[3]:

> 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. W. Diffie and M. E. Hellman. Multi-user cryptographic techniques. In *Proceedings of the June 7-10, 1976, national computer conference and exposition*, AFIPS '76, New York, New York, 1976. ACM.
3. R. Hughes, C. Williams, and R. Doyle. Quantum computing: The final frontier? *IEEE Intelligent Systems*, September/October, 2000.
4. 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.
5. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17), 1997.
6. 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.
7. 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.
8. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17), 1997.
9. D. Mayers. The trouble with quantum bit commitment. Technical report, Computing Research Repository (CoRR), 1999.
10. R. L. Rivest. *Handbook of Theoretical Computer Science*, chapter 13. The MIT Press, 1990.
11. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring, 1994.
12. 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.

13. A. Steane. Quantum computing. Technical report, University of Oxford, 1997.
14. 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.
15. 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.