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[9]. 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[10], 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 Computational Complexity

'The computational complexity of the problem is determined by the number of steps a Turing machine must make in order to complete any algorithmic method to solve the problem.'

Number of steps 's'

If an algorithm exists with 's' given by any polynomial function of L (eg s ? L3 + L) then the problem is deemed tractable and is placed in the complexity class p. If 's' rises exponentially with l (eg s ? 2L = x) then the problem is hard and is in another complexity class. The class np is the set of problems for which solutions can be verified in poly- nomial time. Obviously p ? np, and one would guess that there are problems in np which are not in p, (i.e. np =? p) though surprisingly the latter has never been proved, since it is very hard to rule out the possible existence of as yet undiscovered algorithms. An important example of an intractable problem is that of factorisation: given a composite (i.e. non-prime) number x, the task is to find one of its fac- tors. If x is even, or a multiple of any small number, then it is easy to find a factor. The interesting case is when the prime factors of x are all themselves large. In this case there is no known simple method. The best known method, the number field sieve (Menezes et. al. 1997) requires a number of computational steps of order s ? exp(2L1/3(log L)2/3) where L = ln x. By devoting a substantial machine network to this task, one can today factor a number of 130 decimal digits (Crandall 1997), i.e. L ? 300, giving s ? 1018. This is time-consuming but possible (for example 42 days at 1012 operations per second). However, if we double L, s increases to ? 1025, so now the problem is intractable: it would take a million years with current technology, or would require computers running a million times faster than current ones. The lesson is an important one: a computationally hard problem is one which in practice is not merely difficult but impossible to solve.

The factorisation problem has acquired great practical importance because it is at the heart of widely used cyptographic systems such as that of Rivest, Shamir and Adleman (1979) (see Hellman 1979). For, given a message M (in the form of a long binary number), it is easy to calculate an encrypted version E = Ms mod c where s and c are well-chosen large integers which can be made public. To decrypt the message, the receiver calculates Et mod c which is equal to M for a value of t which can be quickly deduced from s and the factors of c (Schroeder 1984). In practice c = pq is chosen to be the product of two large primes p, q known only to the user who published c, so only that user can read the messagesunless someone manages to factorise c. It is a very useful feature that no secret keys need be distributed in such a system: the key c, s allowing encryption is public knowledge.

3 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 also super-polynomial in the size of the input.

When Peter Shor discovered a quantum algorithm in 1994 which was capable of factoring integers in polynomial time[10], suddenly the public-key cryptographic techniques which had become such a standard looked vulnerable to attack.

Then in 2001, IBM demonstrated the algorithm on a quantum computer by factoring 15 using 7 qubits. Although this demonstration was disregarded by some as no quantum entanglement had been observed, subsequent experiments have been carried out which support IBM's findings[5].

Shor's Algorithm Explanation????

4 Quantum Mechanical Concepts

4.1 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. While in classical computing, a bit is capable of existing in one of two states (0 and 1), in quantum computing, the qubit is capable of existing in

Quantum Computing - Steane: The fundamental resources required for computing are a means to store and to manipulate symbols. The general insight is that computation is deemed hard or inefficient if the amount of resources required rises exponentially with a measure of the size of the problem to be addressed. we find that a computer must be able to manipulate bi- nary symbols, not just unary symbols, otherwise the number of memory locations needed would grow exponentially with the amount of information to be manipulated.

To manipulate n binary symbols, it is not necessary to manipulate them all at once, since it can be shown that any transformation can be brought about by manipulating the binary symbols one at a time or in pairs. A binary logic gate takes two bits x, y as inputs, and calculates a function f(x,y). Since f can be 0 or 1, and there are four possible inputs, there are 16 possible functions f. This set of 16 different logic gates is called a universal set, since by combining such gates in series, any transformation of n bits can be carried out. Futhermore, the action of some of the 16 gates can be reproduced by combining others, so we do not need all 16, and in fact only one, the nand gate, is necessary (nand is not and, for which the output is 0 if and only if both inputs are 1).

In classical information theory...

'The elementary unit of quantum information is the qubit (Schumacher 1995). A single qubit can be envisaged as a two-state system such as a spin-half or a two- level atom (see fig. 12), but when we measure quan- tum information in qubits we are really doing something more abstract: a quantum system is said to have n qubits if it has a Hilbert space of 2n dimensions, and so has available 2n mutually orthogonal quantum states (recall that n classical bits can represent up to 2n different things). This definition of the qubit will be elaborated in section 5.6.'

Quantum equivalent of a bit. Quantum bits(qubits) act as a processor as well as memory. An atom's electron cloud has a spin (the angular momentum of its magnetic field) called spin up/spin down - similar to the 0/1 of bit/transistor technology. Whereas a classical bit can only be one of two states: 0 or 1, a qubit can also be up and down, as well as every value in between.

4.2 Quantum entanglement

> Occurs when qubits interact and become separated. Each resulting member of a pair is properly described by the same quantum mechanical description (state), which is indefinite in terms of important factors such as position, momentum, spin, polarization, etc. According to the Copenhagen interpretation of quantum mechanics, their shared state is indefinite until measured. Quantum entanglement is a form of quantum superposition. When a measurement is made and it causes one member of such a pair to take on a definite value (e.g., clockwise spin), the other member of this entangled pair will at any subsequent time be found to have taken the complementary value (e.g., counterclockwise spin). Thus, there is a correlation between the results of measurements performed on entangled pairs, and this occurs even though the entangled pair may have been separated by arbitrarily large distances.[wiki]

5 Quantum Cryptography

As quantum computers are developed, exiting 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 laws of quantum physics to provide security, rather than mathematical functions.

> Touted by scientists as the ultimate unbreakable code[IEEE Quantum cryptography cracked online article]

Discuss the use of quantum entanglement.

Current 150km limitation - limitation of optical fibre length and the loss of photons.

5.1 Quantum bit commitment

- Who developed it?
- What is it used for/where is it used?
- Why is it used?
- (How is it used?)
- Discuss what's still possible. Whether it's still viable

A commitment scheme allows a party Alice to fix a certain value (to "commit") in such a way that Alice cannot change that value any more while still ensuring that the recipient Bob cannot learn anything about that value until Alice decides to reveal it.

The idea that a person can 'commit' a value and transmit this to another party without said party being able to discover the value of the data until the sender decides to reveal it. Based upon the idea that in quantum mechanics, merely listening in on a quantum message alters the nature of the quantum system, thus is easily detected by the parties sending/receiving the message. This has an obvious application in election scenarios. In fact, a computer developed by Id Quantique was used during the Swiss canton of Geneva parliamentary elections (2007)[citation needed].

However, this has been proven to be impossible - a computationally unlimited attacker can break any quantum commitment method[4][7][8]. 'Participants can cheat and make use of quantum entanglement' steane

'Bit commit- ment refers to the scenario in which Alice must make some decision, such as a vote, in such a way that Bob can be sure that Alice fixed her vote before a given time, but where Bob can only learn Alices vote at some later time which she chooses.' Steane

> However, the bit commitment idea, long thought to be secure through quantum methods, was recently proved to be insecure (Mayers 1997, Lo and Chau 1997)[12]

5.2 Quantum key distribution

- Who developed it?
- What is it used for/where is it used?

- Why is it used?
- (How is it used?)

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][11], 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.[14].

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[13] and fdjsfjdsklfkjldsfjdslk[6]

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

– 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. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17), 1997.
5. 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.
6. 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.
7. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17), 1997.
8. D. Mayers. The trouble with quantum bit commitment. Technical report, Computing Research Repository (CoRR), 1999.
9. R. L. Rivest. *Handbook of Theoretical Computer Science*, chapter 13. The MIT Press, 1990.
10. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring, 1994.
11. 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.
12. A. Steane. Quantum computing. Technical report, University of Oxford, 1997.
13. 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.
14. 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.