Cryptographic Techniques and Quantum Computing

Thomas Taylor

School of Computing, Engineering and Mathematics,
University of Brighton,
Brighton, United Kingdom
tt36@uni.brighton.ac.uk

Abstract. Research into quantum cryptographic techniques.

1 Introduction

> If you think you understand quantum theory, you don't understand quantum theory.
>
> You don't understand quantum theory, you just get used to it.

Richard Feynman[uncited]

1.1 Brief Introduction to Quantum Computing

As we're currently moving towards maximum capacity for the old transistor/silicon hardware (predictions of exhausted capacity by 2020)[need citation], there's a call for a higher capacity/smaller form-factor alternative. Quantum computing works at an atomic level, compared with the current transistor technology, allowing for much 'smaller' hardware. Research is already backed by government and military operations.

Although since proven unable to perform NP-complete problems in polynomial time as originally hoped, quantum computers/algorithms have still been proven to perform calculations significantly quicker than classical computers (able to speed up NP-complete problems quadratically, but not exponentially?)[Strengths and Weaknesses of Quantum Computing]. Quantum computers are also able to handle values too large for classical computers.

Introduce some keywords:

Quantum bits and Quantum States 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.

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]

Quantum Error Correction Used to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is essential if one is to achieve fault-tolerant quantum computation that can deal not only with noise on stored quantum information, but also with faulty quantum gates, faulty quantum preparation, and faulty measurements.

The possibility of preserving quantum coherence in the presence of irreversible noise processes.

[Andrew Steane's research]

Quantum Algorithms

Simon's Algorithm (1994) Daniel Simon - algorithm capable of solving problems exponentially faster than classical algorithms. Has little practical value.

Shor's Algorithm (1994) Peter Shor - quantum algorithm for integer factorisation (given 'n', find its prime factors) in polynomial time. Could be used to break RSA public cryptology scheme - based on the assumption that it's computationally infeasible for classical computers to carry out for large numbers. Demonstrated by IBM (2001) - factored 15 into 3 and 5 using 7 qubits. Doubts have been raised as to whether IBM's experiment was a true demonstration of quantum computation, since no entanglement was observed, but other experiments have since proved this. [Demonstration of Shors quantum factoring algorithm using photonic qubits]

Grover's Algorithm (1996) Lov Grover - a probabilistic algorithm for searching an unsorted database with 'n' entries (provides quadratic speed-up over classical alternatives)

1.2 Brief Introduction to Cryptography

Brief description of what cryptography is, applications etc.

2 Cryptographic Techniques

2.1 Classical cryptography

Classical cryptographic techniques are largely reliant on the current inability to factor very large numbers within a useable timeframe. However, this is likely to change with improvements in computational processing power/introduction of quantum computers (Shor's algorithm).

Public Key Cryptography Underpins such Internet standards as Transport Layer Security (TLS) (successor to SSL), PGP, and GPG.

Requires two keys (one for encryption, one for decryption), one of which is made public, participants must create a public/private key pair.

The sender encrypts the message using the recipient's public key. To decrypt the message, the recipient uses the private key which no-one else (including the sender) has.

While It is easy for the sender/recipient to generate the public/private keys and encrypt/decrypt the message, it is extremely difficult for anyone to calculate out the private key based on knowledge of the public key, based on the fact that the factorisation of very large numbers has no efficient solution.

A public key algorithm does not require a secure initial exchange of secret keys between the sender and receiver. It also allows authenticity of a message to be checked by creating a digital signature of a message using the private key, which can be verified using the public key.

2.2 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]

Discuss the use of quantum entanglement.

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

Quantum bit commitment 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[The Trouble with Bit Commitment - Mayers] [Unconditionally secure commitment is impossible - Mayers, 1997] - a computationally unlimited attacker can break any quantum commitment method. (also, [Is Quantum Bit Commitment Really Possible? - Lo and Chau, 1997])

> 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)[2]

Discuss what's still possible. Whether it's still viable.

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.[1]

Mathematical proofs have been established which confirm the security of quantum bit commitment[citation needed].

3 Conclusion
Future Technology/Application of Quantum Cryptography

- Secure voting (bit commitment)
- NASA Earth to space/satellite communication[1]:

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. R. Hughes, C. Williams, and R. Doyle. Quantum computing: The final frontier? *IEEE Intelligent Systems*, September/October, 2000.
2. R. Steine. Quantum computing. Technical report, University of Oxford, 1997.