The Use of Quantum Mechanical Effects in Cryptographic Techniques

Thomas Taylor

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

Abstract. With the recent advances in making physical quantum computers a reality, It's becoming more likely that we will soon have hardware capable of applying quantum mechanical algorithms to break classical cryptographic techniques. In this paper, I discuss some of the classical techniques used today, and their quantum equivalents.

Questions

- Fair to assume knowledge of NP-completeness, polynomial/quadratic time?
- Have split paper into: intro, classical techniques, quantum concepts, quantum techniques, conclusion

1 Introduction

- What is cryptography?
- What is it used for?
- Why is it important?
- Discuss the how security may (will) be compromised given the introduction of quantum computational hardware (with relation to the factoring of large numbers - specifically Shor's algorithm)

2 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).

2.1 Symmetric Key Cryptography

- Who developed it?
- What is it used for/where is it used?
- Why is it used?
- (How is it used?)

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.[18]

One round (out of 8.5) of the patented IDEA cipher, used in some versions of PGP for high-speed encryption of, for instance, e-mail Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).[20] Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken, such as FEAL.

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher; see Category:Stream ciphers. Block ciphers can be used as stream ciphers; see Block cipher modes of operation.

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed length hash which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function which is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The U.S. National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but it isn't yet widely deployed, and the U.S. standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition is underway and meant to select a new U.S. national standard, to be called SHA-3, by 2012.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt.

2.2 Assymmetric Key Cryptography (Public Key)

- Who developed it?
- What is it used for/where is it used?
- Why is it used?
- (How is it used?)

1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used.[1]

Underpins such Internet standards as Transport Layer Security (TLS), Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG).

Public Key Algorithms:

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

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.

3 Quantum Mechanical Concepts

3.1 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.

3.2 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]

3.3 Quantum Algorithms

Shor's Algorithm (1994) Peter Shor - quantum algorithm for integer factorisation (given 'n', find its prime factors) in polynomial time.[8] Could be used to break RSA public key cryptography 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.[4]

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

4 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.

4.1 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[3][6][7].

> 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)[9]

4.2 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.[2]

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

Researchers have recently shown that it is not only possible, but technologically feasible to mount an undetected attack (known as the time-shift) against a commercial quantum key distribution system.[11]

Similarly, fjdskfljdsfkldsjfsdkl[10] and fdjsfjdsklfkjldsfjdslk[5]

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[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. 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.
2. R. Hughes, C. Williams, and R. Doyle. Quantum computing: The final frontier? *IEEE Intelligent Systems*, September/October, 2000.
3. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17), 1997.
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. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17), 1997.
7. D. Mayers. The trouble with quantum bit commitment. Technical report, Computing Research Repository (CoRR), 1999.
8. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring, 1994.
9. A. Steane. Quantum computing. Technical report, University of Oxford, 1997.
10. 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.
11. 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.