Applied Mechanics and Materials Vols. 275-277 (2013) pp 2511-2514 *Online: 2013-01-11*
© (2013) Trans Tech Publications, Switzerland
doi:10.4028/www.scientific.net/AMM.275-277.2511

Introduction of Quantum Cryptography

Xiaoqiang Guo, Yan Yan, Lichao Feng and Shiqiu Zheng

College of Science, Hebei United University,
No.46 Xinhua West Street, Tangshan 063009, Hebei Province, China

guoxiaoqiang@heuu.edu.cn, guoxq2004@163.com

Keywords: Quantum key distribution, Quantum commitment, Bounded quantum storage model, Position-based quantum cryptography, Post-quantum cryptography.

Abstract. Quantum cryptography is the use of quantum existence state as the key of information encrption and decryption, the principle is the Einstein called "mysterious long distance activities" quantum entangled state. It is a quantum mechanical phenomenon, regardless of the distance between the two particles far, a particle changes will affect another particle, compared with the traditional password technology has a higher level of security. Quantum cryptography is a research hotspot of international academia in recent years. We introduce quantum key distribution, quantum commitment, bounded quantum storage model, position based quantum cryptography and post-quantum cryptography.

Introduction

Quantum cryptography describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems. The use of classical cryptography to protect against quantum attackers is also often considered as quantum cryptography .

Well-known examples of quantum cryptography are the use of quantum communication to securely exchange a key (quantum key distribution) and the (hypothetical) use of quantum computers that would allow the breaking of various popular public-key encryption and signature schemes (e.g., RSA and ElGamal).

The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical communication. In particular, quantum mechanics guarantees that measuring quantum data disturbs that data, this can be used to detect an adversary's interference with a message. However, researchers at the University of Toronto and NTNU have shown that undetected quantum hacking might be possible in a variety of implementations of quantum key distribution systems[1, 2].

Quantum key distribution

Arguably the best-known application of quantum cryptography is quantum key distribution (QKD). QKD describes the process of using quantum communication to establish a shared key between two parties (usually called Alice and Bob) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. This is achieved (roughly speaking) by letting Alice encode the bits of the key as quantum data before sending them to Bob; if Eve tries to learn these bits, the messages will be disturbed and Alice and Bob will notice.

QKD is possible without imposing any computational assumptions (that is, assumptions stating that certain mathematical problems such as factoring large numbers take very long time to solve on a computer). One also speaks of "unconditional security". The only assumptions are that the laws of quantum mechanics hold, which is to a certain extent disputable due to the difficulties of unifying relativity theory and quantum mechanics, and that Alice and Bob have an authenticated channel, i.e., Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible.QKD is the only example of commercially available quantum cryptography.

Quantum commitment

Following the discovery of quantum key distribution and its unconditional security, researchers tried to achieve other cryptographic tasks with unconditional security. One such task was 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. Such commitment schemes are commonly used in cryptographic protocols. In the quantum setting, they would be particularly useful: Crépeau and Kilian showed that from a commitment and a quantum channel, one can construct an unconditionally secure protocol for performing so-called oblivious transfer.[3] Oblivious transfer, on the other hand, had been shown by Kilian to allow to implement almost any distributed computation in a secure way so-called secure multi-party computation.[4] Notice that here we are a bit imprecise: The results by Crépeau and Kilian[3] and Kilian[4] together do not directly imply that given a commitment and a quantum channel one can perform secure multi-party computation. This is because the results do not guarantee "composability", that is, when plugging them together, one might lose security. Later works showed, however, how composability can be ensured in this setting.

Unfortunately, early quantum commitment protocols[5] were shown to be flawed. In fact, Mayers showed that unconditionally secure quantum commitment is impossible. A computationally unlimited attacker can break any quantum commitment protocol.[6]

Yet, the result by Mayers does not preclude the possibility of constructing quantum commitment protocols and thus secure multi-party computation protocols under assumptions that are much weaker than the assumptions needed for commitment protocols that do not use quantum communication. The bounded quantum storage model described below is an example for a setting in which quantum communication can be used to construct commitment protocols.

Bounded quantum storage model

One possibility to construct unconditionally secure quantum commitment and quantum oblivious transfer (OT) protocols is to use the bounded quantum storage model (BQSM). In this model, we assume that the amount of quantum data that an adversary can store is limited by some known constant Q. We do not, however, impose any limit on the amount of classical data the adversary may store.

In the BQSM, one can construct commitment and oblivious transfer protocols.[7] The underlying idea is the following: The protocol parties exchange more than Q quantum bits. Since even a dishonest party cannot store all that information, the quantum memory of the adversary is limited to Q qubits, a large part of the data will have to be either measured or discarded. Forcing dishonest parties to measure a large part of the data allows to circumvent the impossibility result by Mayers[6]; commitment and oblivious transfer protocols can now be implemented.

The protocols in the BQSM presented by Damgård, Fehr, Salvail, and Schaffner do not assume that honest protocol participants store any quantum information; the technical requirements are similar to those in QKD protocols. These protocols can thus, at least in principle, be realized with today's technology. The communication complexity is only a constant factor larger than the bound Q on the adversary's quantum memory.

The advantage of the BQSM is that the assumption that the adversary's quantum memory is limited is quite realistic. With today's technology, storing even a single qubit reliably over a sufficiently long time is difficult. What "sufficiently long" means depends on the protocol details. By introducing an artificial pause in the protocol, the amount of time over which the adversary needs to store quantum data can be made arbitrarily large.

In the classical setting, similar results can be achieved when assuming a bound on the amount of classical data that the adversary can store. [8] It was proven, however, that in this model also the honest parties have to use a large amount of memory namely the square-root of the adversary's memory

bound. [9] This makes these protocols impractical for realistic memory bounds. Note that with today's technology such as hard disks, an adversary can cheaply store large amounts of classical data.

Position based quantum cryptography

The goal of position based quantum cryptography is to use the geographical location of a player as its only credential. For example, one wants to send a message to a player at a specified position with the guarantee that it can only be read if the receiving party is located at that particular position. In the basic task of position verification, a player Alice wants to convince the honest verifiers that she is located at a particular point. It has been shown by Chandran et al. that position verification using classical protocols is impossible against colluding adversaries who control all positions except the prover's claimed position.[10] Under various restrictions on the adversaries, schemes are possible.

Under the name of 'quantum tagging', the first position-based quantum schemes have been investigated in 2002 by Kent. A US-patent was granted in 2006, but the results have only appeared in the scientific literature in 2010.[11] After several other quantum protocols for position verification have been suggested in 2010, Buhrman et al. were able to show a general impossibility result:[12] using an enormous amount of quantum entanglement, colluding adversaries are always able to make it look to the verifiers as if they were at the claimed position. However, this result does not exclude the possibility of practical schemes in the bounded quantum storage model.

Post-quantum cryptography

In a predictive sense, quantum computers may become a technological reality, it is therefore important to study cryptographic schemes that are not themselves making use of quantum mechanical effects but that are supposedly secure even against adversaries with access to a quantum computer. The study of such schemes is often referred to as post-quantum cryptography. The need for post-quantum cryptography arises from the fact that many popular encryption and signature schemes such as RSA and its variants, and schemes based on elliptic curves can be broken using Shor's algorithm for factoring and computing discrete logarithms on a quantum computer. Examples for schemes that are, as of today's knowledge, secure against quantum adversaries are McEliece and lattice-based schemes. Surveys of post-quantum cryptography are available.[13]

There is also research into how existing cryptographic techniques have to be modified to be able to cope with quantum adversaries. For example, when trying to develop zero-knowledge proof systems that are secure against quantum adversaries, new techniques need to be used. In a classical setting, the analysis of a zero-knowledge proof system usually involves "rewinding", a technique that makes it necessary to copy the internal state of the adversary. In a quantum setting, copying a state is not always possible no-cloning theorem, a variant of the rewinding technique has to be used.[14]

Acknowledgements

This work was supported by the Scientific Technology Research and Development Plan Project of Tangshan (No. 121302001a).

References

[1] Y.Zhao, C.H. Fung, B. Qi, H.K. Lo: *Quantum Hacking: Experimental Demonstration of Time-shift Attack against Practical Quantum-Key-Distribution Systems*, Physical Review A(2008).

[2] F.H.Xu, B.Qi, H.K.Lo: *Experimental Demonstration of Phase-remapping Attack in a Practical Quantum Key Distribution Systems*, New Journal of Physics. (2010).

[3] C.Crépeau,K. Joe: *Achieving Oblivious Transfer Using Weakened Security Assumptions*. FOCS, IEEE. (1988), pp. 42-52.

[4] K.Joe: *Founding cryptography on oblivious transfer*, STOC, ACM. (1988), pp. 20-31.

[5] B.Gilles, C.Crépeau, J.Richard, D.Langlois: *A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties*, FOCS, IEEE. (1993), pp. 362-371.

[6] D.Mayers: *Unconditionally Secure Quantum Bit Commitment is Impossible*, Physical Review Letters (APS), **78** (17) (1997), pp. 3414–3417.

[7] I.Damgård, S.Fehr, L.Salvail, C.Schaffner: *Cryptography In the Bounded Quantum-Storage Model*, FOCS, IEEE. (2005), pp. 449-458.

[8] C.Cachin, C.Crépeau, J.Marcil: *Oblivious Transfer with a Memory-Bounded Receiver*, FOCS, IEEE. (1998), pp. 493-502.

[9] S.Dziembowski,M.Ueli: *On Generating the Initial Key in the Bounded-Storage Model*, LNCS, Eurocrypt, Springer. (2004), pp. 126-137.

[10] N.Chandran, R.Moriarty, V.Goyal, R.Ostrovsky: *Position-Based Cryptography*, (2009) .

[11] A.Kent, B.Munro, T.Spiller: *Quantum Tagging with Cryptographically Secure Tags*, (2010) .

[12] H. Buhrman, N. Chandran, S. Fehr, R.Gelles, V.Goyal, R.Ostrovsky, C. Schaffner: *Position-Based Quantum Cryptography: Impossibility and Constructions*, (2010).

[13] Post-quantum cryptography, http://pqcrypto.org

[14] J.Watrous: *Zero-Knowledge against Quantum Attacks*, SIAM J,Comput, **39** (1), (2009), pp.25–58.

Applied Mechanics and Materials I
10.4028/www.scientific.net/AMM.275-277

Introduction of Quantum Cryptography
10.4028/www.scientific.net/AMM.275-277.2511