Trends in

Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 6 (6): 554-562, 2011
ISSN 1819-3579 / DOI: 10.3923/tasr.2011.554.562

Unconditional Security of Cryptosystem: A Review and Outlook

Yong Wang
School of Computer Science and Engineering, Guilin University of Electronic Technology, Guilin 541004, China

ABSTRACT

With the development of computing power and cryptanalysis technology, unconditional security of cryptosystem is more and more important. This study presents a review of the literature on the unconditional security of cryptosystem. One-time pad and most quantum key distribution protocols were proved to be unconditionally secure. The development and extension of unconditional security is represented. As unconditional security is strict and hard to reach, some moderate security ideas are proposed and an outlook is given.

Key words: Unconditional security, cryptography, perfect secrecy, spurious key, redundancy

INTRODUCTION

Cryptosystems are mostly used to protect the security of information and play an important role in the information security. Both symmetric cryptosystems and asymmetric cryptosystems currently used are based on the model of computational security. In principle, all of them can be broken by trying all of the possible keys using brute force approach if ciphertext is long enough (Shannon, 1949). With the development of science and technology, computational power has greatly increased. What's more, quantum computers and DNA computers with infinite computing power for their character of parallel computing may be able to break some cryptosystems. With quantum computer, some quantum algorithms can break cryptosystems such as RSA and DES (Shor, 1994; Grover, 1996, 1997). Quantum computer will come to our daily life in the near future. The development of methods and algorithms of attack are another treat to cryptosystem. We can draw a conclusion from the cryptography history (both classical and modern cryptography): in most cases, the cryptosystems would be broken before the time it was initially expected to be broken and the method of attack was usually unhoped-for. The theory of provable security has been established and developed, but it is mostly based on hypothesis and limited computing power. Cryptosystems of computational security or even provable security at the very start may be unsecure, for example, when RSA was invented, it was predicted that the original RSA challenge large number (129-digit) would not be factored in the not far distant future. However, the new RSA large number, RSA-640 (193-digit), was successfully factored. AES is the current encryption standard (Daemen and Rijmen, 2002), but it is also reported to be vulnerable to algebraic attacks (Courtois and Pieprzyk, 2002). Therefore the unconditional security (theoretical security, perfect secrecy and perfect security), of cryptosystem will become more and more important. But most research nowadays focuses on the computational security of cryptosystem. The study of unconditional security is limited in several areas. This study gives a review and outlook about unconditional security of cryptosystem.

PERFECT SECRECY AND ITS EXTENSION

Shannon defined perfect secrecy by requiring that, given a ciphertext, every message in the message space and its probability are identically the same as the underlying plaintext, in another word, the plaintext is independent of the ciphertext. Thus the perfect secrecy requirement implies that the eavesdropper truly learns nothing at all about the underlying plaintext. Shannon proved that one-time pad was perfect secrecy (perfect security) (Shannon, 1949).

But perfect secrecy requires that number of the keys is not less than the number of the messages possible keys, hence the key is not shorter than the message. For this reason, one-time pad is very expensive for practical use. It needs information-theoretic (unconditionally secure) secret-key agreement to distribute the long key.

Indeed, Shannon's model is under noise-free channel, but most channels are noisy. Therefore Shannon's model is extended and modified to make practical provably secure cryptosystems possible. The first modification is to reduce the requirement that perfect secrecy means complete independence between the plaintext and the adversary's knowledge and to allow an arbitrary small correlation, which is more suitable for reality. The second crucial modification removes the assumption that the adversary receives exactly the same information as the legitimate users; this modification is also in the face of channel with noise, for the adversary listens in a noisy channel and can not get all of the right information. Wyner introduced noisy channel into cryptography (Wyner, 1975). In his model the eavesdropper is listening in a wiretap channel and he proved it was possible to send message in an unconditionally secure way without shared key. Csiszar and Korner (1978) generalized the model of Wyner on the wiretap channel to a model on the broadcast channel. Based on the model of Csiszar and Korner, Maurer proposed a new model which added a feedback channel between Alice and Bob. Maurer later generalized the model to a more effective model (Maurer, 1992, 1993). His model can be applied in satellite broadcasting channels, two communicants. Alice, Bob and an eavesdropper, Eve, receive three variables X, Y, Z which are distributed according to some probability distribution P_{xyz} from satellite signal with noise, as the channel is noisy, X, Y and Z are usually different from each other. Then Alice and Bob begin secret-key agreement over a public channel. Its aim is to remove the difference of X and Y and get synchronization information between Alice and Bob as shared key and reduce the information of Eve to a desired smallness. Such a secret key agreement over a public channel usually consists of three phases: (1) advantage distillation (Maurer, 1992, 1993; Gander and Maurer, 1994) which makes that the mutual information of communication partners is distilled firstly, or advantage degeneration which makes the information of enemy (Eve) is degenerated firstly (Yupu *et al.*, 2002); (2) information reconciliation whose goal is to remove these errors by exchanging messages on an authenticated public channel (Bennett *et al.*, 1992); (3) privacy amplification whose goal is to eliminate Eve's partial information and to create a shorter, truly secret key (Bennett *et al.*, 1988, 1995; Maurer and Wolf, 1996). Ueli Maurer and Stefan Wolf proved that the foregoing key agreement can be improved to a stronger one (Maurer and Wolf, 2000). The effect of side information was introduced under the communication over the public channel on Eve's Renyi entropy and the relationship between information reconciliation and privacy amplification was demonstrated (Shengli, 1999) and an improvement was made to the strong protocol which was proposed by Maurer and Wolf (2000).

In a traditional way, keys are mostly shared in secret channel or by public key cryptosystem. Secret channel is expensive and hard to defend. Public key cryptosystems are of just computational security. The above secret key agreement schemes provide methods to share secret key in insecure channels which can be used in OPT.

UNCONDITIONAL SECURITY OF QUANTUM CRYPTOGRAPHY LIMITATIONS OF PERFECT SECRECY

Quantum states have special characteristics which are stated as no-cloning theorem and uncertainty principle (Wootters and Zurek, 1982). Using quantum states to encode information is first proposed by Stephen Wiesner. He invented conjugate coding and applied it to design "money physically impossible to counterfeit", but it is hard to store quantum states, so its publication had been rejected for a long time (Wiesner, 1983). Based on Stephen Wiesner's idea, Charles Bennett and Gilles Brassard designed the first practical quantum cryptography protocol, BB84 (Bennett and Brassard, 1984) and then designed BB92 (Bennett, 1992), these two schemes are both based on no-cloning theorem and uncertainty principle. Quantum cryptography schemes based on Bell's theorem were designed (Einstein *et al.*, 1935; Ekert, 1991; Bennett *et al.*, 1993). To conquer the errors made by noise and wiretapping in the quantum channel, unconditionally secure secret-key agreement over a public channel was designed, information reconciliation and privacy amplification can be used to quantum key distribution (Bennett *et al.*, 1988, 1992, 1995; Maurer and Wolf, 1996), or otherwise, quantum entanglement purification should be used. Generally, quantum key distribution allows two parties to establish a secure random cryptographic key if they have access to a quantum communication channel and they can exchange classical public messages which can be monitored but not altered by an eavesdropper. Most of the quantum key distribution schemes were proved to be unconditionally secure. The use of quantum cryptography in the unconditional security of encryption was firstly stated by Charles H. Bennett, Gilles Brassard and etc.: when unconditionally secure key agreement is possible, we can transform unconditionally secure key-agreement protocol into an unconditionally secure encryption scheme by using the generated key as the key stream in the well-known one-time pad. There were some proofs of security of quantum key distribution containing various technical subtleties. But they are not systematic and general. For many years, it was not rigorously proved that security against an adversary is able to perform any physical operation permitted by quantum mechanics.

The first general although rather complex proof of unconditional security was given by Mayers (2001), which was followed by a number of other proofs (Biham *et al.*, 1998; Biham and Mor, 1997). In Mayers' proof, the BB84 scheme proposed by Bennett and Brassard was proved to be unconditionally secure. The proof considers a practical variation on the protocol in which the channel is noisy and photons may be lost during the transmission. Each individual signal sent into the channel must contain a single photon or any two-dimensional system in the exact state described in the protocol. No restriction is imposed on the detector used at the receiving side of the channel, except that whether or not the received system is detected must be independent of the basis used to measure this system. Building on the quantum privacy amplification idea, Lo and Chau (1999), proposed a conceptually simpler proof of security. Their result shows that assuming that the sender and receiver have fault-tolerant quantum computers, quantum key distribution can be made unconditionally secure over arbitrarily long distances even against the most general type of eavesdropping attacks and in the presence of all types of noises. The proof is reduced from a noisy quantum scheme to a noiseless quantum scheme and then from a noiseless quantum scheme to a noiseless classical scheme.

Shor and Preskill (2000) unified the techniques proposed by Mayers (2001) and Lo and Chau (1999) and provided a simple proof of unconditional security of standard BB84 (Gottesman and Preskill, 2001). Shor-Preskill's proof is not a direct proof of BB84 scheme, they first gave a key distribution protocol based on entanglement purification, which can be proven unconditionally secure using methods from Lo and Chau's proof of security for a similar protocol. Then they proved that the security of that protocol implied the security of BB84 (Calderbank and Shor, 1996). The entanglement purification based protocol used Calderbank-Shor-Steane (CSS) quantum error correcting codes to show that the information leaked on the final key is negligible and properties of these codes were used to remove the use of quantum computation from the Lo-Chau protocol.

But in applying Shor and Preskill's method to other protocols, such as the B92 protocol, the first problem we encounter is how to find an equivalent Entanglement Distillation Protocol (EDP). Therefore Shor and Preskill's method could not directly be applied to prove the unconditional security of B92 scheme. In order to take advantage of Shor-Preskill's techniques in their proof of the unconditional security of BB84, a transformation was introduced to exchange between BB84 and B92. By proving that the transformed B92 protocol leaked no more information to eavesdropper, the unconditional security of B92 was proved (Quan *et al.*, 2002). B92 was proved to be unconditionally secure of the protocol by using a reduction to an entanglement distillation protocol initiated by a local filtering process (Tamaki *et al.*, 2003). The proof can be used to quantum key distribution based on two nonorthogonal states.

The first proof of the unconditional security by Mayers is very complex, but it has less limitations. The proof was remedied to a simple proof by Koashi and Preskill by reducing the protocol to a two-party protocol by omitting one of the legitimate users by a symmetry argument. In their approach, the error correction and the privacy amplification is decoupled and the error correction is realized by encrypting the communication by previously secure-shared key. This proof implies that we do not need to find a Calderbank-Shor-Steane (CSS) Quantum Error Correcting Codes (QECC) that is needed in the proof by Koashi and Preskill and we can just use conventional schemes for the error correction to achieve unconditional security. The proof also shows a peculiar property, which allows the use of basis-independent uncharacterized sources or detectors (Koashi, 2005, 2009). The approach based on above proof allows us to solve security problems with imperfect devices that were beyond either of the previous arguments. The above proof also provides an insight into the recently predicted phenomenon of secure key from bound entanglement (Horodecki *et al.*, 2005). The proof proposed by Shor and Preskill has been further extended by Gottesman and Hoi-Kwong (2003) to cover the case of two-way public communication in BB84, which is done by the construction of a new protocol for (the error correction/detection and privacy amplification of) Bennett and Brassard that can tolerate a bit error rate which is higher than what any Bennett and Brassard scheme with only one-way classical communications can possibly tolerate. The six-state QKD scheme over Bennett and Brassard is also proved to be unconditionally secure (Lo, 2001).

The above QKD protocols can be classified in discrete-variable protocols, which are based on photon counting; another class of protocols based on homodyne detection is called continuous-variable protocol (Cerf and Grangier, 2007). The unconditional security of continuous-variable quantum key distribution was proved for all schemes based on the estimation of the channel loss and excess noise (Leverrier *et al.*, 2008). A continuous-variable quantum key distribution protocol combining a discrete modulation and reverse reconciliation was proposed and proved to be unconditional security and it allows the distribution of secret keys over long distances (Leverrier and Grangier, 2009).

LIMITATIONS OF PERFECT SECRECY

In most unconditional secrecy cryptosystems, including QKD, One-Time Pad (OTP) plays an important role, but the perfect secrecy of OTP requires that all the possible plaintexts are in the same length. We can find if any possible message whose probability is not zero is longer or shorter than the ciphertext, when the ciphertext is intercepted, the posteriori probability of this message is changed to zero, which does not meet the requirement of perfect secrecy. Therefore, only when all the messages are of the uniform length, one-time pad may be perfect secrecy. In reality, this condition is seldom satisfied.

From another angle, quantum cryptography is based on quantum no-cloning (non-cloning) theorem for it forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key, but quantum no-cloning theorem is not very strictly proved. The proof of quantum no-cloning theorem is very simple and it can not exclude all kinds of possible cloning. The history of science development tells us that the cloning and measure of something that was impossible to be cloned or measured in the past may often become possible with the microscopic understanding of the thing. With the development of quantum technology, it is possible to clone quantum states by more microscopic methods, just like if we clone a man by anatomizing him and trying to measure him on the whole, but the state of him may change, so people had thought it impossible to clone a man before gene technique was developed, but now we can find the gene of him and just using a small gene to clone a man, the drawing of gene has so little influence on him that it is a negligible quantity. That is very similar to the proof of quantum no-cloning theorem. Uncertainty principle declares that an unknown quantum state can not be measured. Bohr's interpretation on uncertainty principle is that the essential difference between classical and quantum physics is that in quantum physics the interaction between the object and the apparatus can not be made arbitrarily small and the interaction must at least comprise one quantum, which is called Bohr's quantum postulate, that is to say, the measure of quantum state must change quantum state (Bohr, 1928). If the particle composes of more microscopic particles (even we may be able to find gene of quantum), we may be able to measure the quantum state by a more microscopic particle, which may lead to enough small interaction that doesn't change the quantum state. The proof of quantum non-cloning theorem is based on quantum theory which is not necessarily the Final Theory and the cloning method in the proof can not cover all the kinds of cloning (Wootters and Zurek, 1982). The ecbolic background of quantum no-cloning theorem is to prevent quantum theory from violating the special theory of relativity, but that seems to be not necessary because the complexity of the problem. According to QKD protocol, unless quantum can be cloned at the time the sender and receiver are processing the protocol, so quantum cryptography will be unconditionally secure before the cloning technology is developed, the past quantum communication is not threatened by later cloning technology.

OUTLOOK OF UNCONDITIONAL PERFECT SECRECY

As OTP restricts and leaks the length of plaintext, in reality, it is seldom unconditionally secure (Wang, 2004). At the same time, unconditional security which demands the probability distribution is completely maintained quite unaltered after the ciphertext is intercepted is a rigorous requirement and it is not an essential condition for the security under unlimited computing power. Shannon defined ideal secrecy that requires the unicity distance is unlimited, that is to say, no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives. It is possible in any language to approximate such behavior. However, such systems have a number of drawbacks, such as complexity and sensitivity to errors in transmission of the ciphertext.

We think it is acceptable to relax the requirement of unconditional secure. Firstly, we can require that for most of the plaintexts, if the prior probability of the plaintext is not zero, then its posterior probability when ciphertext is intercepted is not zero too, that is to say, when all the keys are tried to decrypt the intercepted ciphertext, the prior plaintexts are mostly traversed. We can improve OPT to meet the requirement by padding the ciphertext of OPT to a suitable length longer than the length of most of the possible plaintexts and fusing the cryptographic information of the padding length.

The second approach is to ensure to traverse plaintexts that are close, opposite and similar to the real plaintext. For example, the communication language environment is to tell the receiver the weather is sunny, then the plaintexts decrypted by the intercepted ciphertext should include that the weather is rainy, cloudy, etc. Wang (2004) proposed a scheme like multiple choice questions to achieve this requirement. A cryptosystem which can mislead the cryptanalysts is designed by Wang (2005). The cryptosystem includes inner encryption which is the core and outer encryption which provides an additional and traditional protection using modern cryptography. The encryption procedure is as following: (1) Open the plaintext file; (2) Read text of the file; (3) Do inner encryption; (4) Save the file and (5) Do outer encryption. The inner encryption is an extension like multiple-choice questions with keywords similar and contrary to the keywords in the plaintext according to a database of keywords. The corresponding decryption is like doing multiple-choice questions and the answers are decided by key. It is easy to find spurious keys (pseudokeys) of the cryptosystem that can confuse and mislead cryptanalysts. The real plaintext may be Today is Sunday and the spurious key may get a misleading plaintext Tomorrow is Monday. Though the cryptosystem has some irreplaceable advantages and is secure even under rubber-hose attack, it is complex, redundancy and inefficient. The above cryptosystem was improved to mislead the enemy as one wishes by Wang (2010).

The third approach is to ensure there are enough spurious keys. The concept key authentic degree of cryptosystem was proposed by Wang (2005). The key authentic degree of cryptosystem means the difficulty of finding out the spurious keys which we can decrypt to obtain semantic meaning plaintexts without flaws under certain conditions. Essentially it is used to weigh the degree of the trustworthiness of the key provided by a key holder who is intimidated but not willing to leak the plaintext under the condition that the ciphertext and the algorithm are known by cryptanalysts, assuming that the key holder tries his best to provide a spurious key without flaws to misguide the people who intimidate him. The key authentic degree is high if the spurious keys of the cryptographic algorithms are hard to find out. Researches indicated that the key authentic degree of modern cryptosystem is very high (Wang and Huadeng, 2010). Some ways to increase the spurious key and lower key authentic degree are provided such as increasing the length of key, reducing the redundancy, designing cryptosystem with natural language processing and Artificial Intelligence (AI) technology which can encrypt and decrypt intellectually and thus avoid plentiful redundancy and ensure enough spurious keys.

The three approaches may provide new directions for the intending cryptosystem under adversary with unlimited computing power.

CONCLUSIONS

In this study, we summarize the progress in unconditional security of cryptosystem. OPT and most QKD protocols were proved to be unconditionally secure (perfect secrecy). But in reality, there are limitations such as noise, information leakage and plaintexts unequal in length to prevent the achievement of unconditional security. The concept of unconditional security was extended and additional technology is used to adapt the reality situation, such as advantage distillation, information reconciliation, privacy amplification and padding. As unconditional security is strict and hard to reach, some moderate security ideas are proposed. There is a broader space for development of cryptosystem under unlimited computing power, but these cryptosystems may be more complex and dependent on other technology.

ACKNOWLEDGMENT

This research was supported by Science and Research Foundation of Guangxi Ministry of Education (200911MS88).

REFERENCES

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public-key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, December 1984, Bangalore, India, pp: 175-179.

Bennett, C.H., G. Brassard and J.M. Robert, 1988. Privacy amplification by public discussion. SIAM J. Comput., 17: 210-229.

Bennett, C.H., 1992. Quantum cryptography using any two non-orthogonal states. Phys. Rev. Lett., 68: 3121-3124.

Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, 1992. Experimental quantum cryptography. J. Cryptol., 5: 3-28.

Bennett, C.H., G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. Wootters, 1993. Teleporting an unknown quantum state via dual classical and EPR channels. Phys. Rev. Lett., 70: 1895-1899.

Bennett, C.H., G. Brassard, C. Crkpeau and U.M. Maurer, 1995. Generalized privacy amplification. IEEE Trans. Inform. Theory, 41: 1915-1923.

Biham, E. and T. Mor, 1997. On the security of quantum cryptography against collective attacks. Phys. Rev. Lett., 78: 2256-2259.

Biham, E., M. Boyer, G. Brassard, J. van-de-Graaf and T. Mor, 1998. Security of quantum key distribution against all collective attacks. Los Alamos Archives quant-ph/9801022, January 1998. http://www.iacr.org/archive/eurocrypt2000/1807/18070294-new.pdf.

Bohr, N., 1928. The quantum postulate and the recent development of atomic theory 1. Nature, 121: 580-590.

Calderbank, A.R. and P. Shor, 1996. Good quantum error correcting codes exist. Phys. Rev. A, 54: 1098-1105.

Cerf, N.J. and P. Grangier, 2007. From quantum cloning to quantum key distribution with continuous variables: A review. J. Optical Soc. Am. B, 24: 324-334.

Courtois, N. and J. Pieprzyk, 2002. Cryptanalysis of block ciphers with over-defined systems of equations. Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Dec. 1-5, Springer-Verlag, London, UK., pp: 267-287.

Csiszar, I. and J. Korner, 1978. Broadcast channels with confidential messages. IEEE Trans. Inform. Theory, 22: 339-348.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer-Verlag, Berline.

Einstein, A., B. Podolsky and N. Rosen, 1935. Can quantum-mechanical description of physical reality be considered complete. Phys. Rev., 47: 777-780.

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663.

Gander, M.J. and U.M. Maurer, 1994. On the secret key rate of binary random variables. Proceedings of the IEEE International Symposium on Information Theory, June 27-July 1, Trondheim, Norway, pp: 351-351.

Gottesman, D. and J. Preskill, 2001. Secure quantum key distribution using squeezed states. Phys. Rev. A, 63: 22309-22309.

Gottesman, D. and L. Hoi-Kwong, 2003. Proof of security of quantum key distribution with two-way classical communication. IEEE Trans. Inform. Theory, 49: 457-475.

Grover, L.K., 1996. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computation, May 22-24, ACM Press, New York, pp: 212-219.

Grover, L.K., 1997. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett., 79: 325-328.

Horodecki, K., M. Horodecki, P. Horodecki and J. Oppenheim, 2005. Secure key from bound entanglement. Phys. Rev. Lett., 94: 160502-160502.

Koashi, M., 2005. Recent progress on the unconditional security proof for quantum key distribution protocols. Proceedings of the International Quantum Electronics Conference, July 11, Tokyo, Japan, pp: 1608-1609.

Koashi, M., 2009. Simple security proof of quantum key distribution based on complementarity. New J. Phys., 11: 045018-045018.

Leverrier, A., E. Karpov, P. Grangier and N.J. Cerf, 2008. Unconditional security of continuous-variable quantum key distribution. http://arxiv.org/abs/0809.2252.

Leverrier, A. and P. Grangier, 2009. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys. Rev. Lett., 102: 180504-180504.

Lo, H.K. and H.F. Chau, 1999. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283: 2050-2057.

Lo, H.K., 2001. Proof of unconditional security of six-state quantum key distribution scheme. Quant. Inform. Comput., 1: 81-94.

Maurer, U.M., 1992. Protocols for secret key agreement based on common information. Lecture Notes Comput. Sci., 740: 461-470.

Maurer, U.M., 1993. Secret key agreement by public discussion from common information. IEEE Trans. Inform. Theory, 39: 733-742.

Maurer, U.M. and S. Wolf, 1996. Privacy amplification secure against active. Adv. Cryptol. CRYPTO'91, 1294: 307-321.

Maurer, U.M. and S. Wolf, 2000. From weak to strong information-theoretic key agreement. Proceedings of the IEEE International Symposium on Information Theory, June 25-30, Sorrento, Italy, pp: 18-18.

Mayers, D., 2001. Unconditional security in quantum cryptography. J. ACM, 48: 351-406.

Quan, Z., T. Chao-Jing and Z. Sen-Qiang, 2002. Modification of B92 protocol and the proof of its unconditional security. Acta Physica Sinica, 51: 51-1447.

Shannon, C.E., 1949. Communication theory of secrete systems. Bell Tech. J., 28: 656-715.

Shengli, L., 1999. Research on information-theoretic security in cryptography. Ph.D. Thesis, Xidian University, China.

Shor, P.W., 1994. Algorithms for quantum computation discretelog and factoring. Proceeding of the 35th IEEE Symposium on the Foundations of Computer Science, Nov. 20-22, Santa Fe, NM, USA., pp: 124-134.

Shor, P.W. and J. Preskill, 2000. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett., 2: 441-444.

Tamaki, K., M. Koashi and N. Imoto, 2003. Unconditionally secure key distribution based on two nonorthogonal states. Phys. Rev. Lett., 90: 167904-167904.

Wang, Y., 2004. Security of one-time system and new secure system [J]. Netinfo Security, pp: 41-43. http://arxiv.org/ftp/arxiv/papers/0709/0709.4303.pdf.

Wang, Y., 2005. Study of some problems of quantum cryptography and theoretical security of cryptosystem [D]. Southwest Jiaotong University, 2005 (In Chinese).

Wang, Y., 2010. An improved cryptosystem of low key authentic degree. Proceedings of the 2nd IEEE International Conference on Information Management and Engineering (ICIME), April 16-18, Chengdu, pp: 78-80.

Wang, Y. and W. Huadeng, 2010. On key authentic degree of cryptosystem. Proceeedings of the 2nd IEEE International Conference on Information Management and Engineering (ICIME), April 16-18, Chengdu, pp: 301-304.

Wiesner, S., 1983. Conjugate coding. ACM SIGACT News, 15: 78-88.

Wootters, W.K. and W.H. Zurek, 1982. A single quantum cannot be cloned. Nature, 299: 802-803.

Wyner, A.D., 1975. The wire-tap channel. Bell Syst. Technical J., 54: 1355-1387.

Yupu, H.U., Y. Bo and Z. Yuqing, 2002. An advantage degeneration protocol in complete security scheme. Acta Electronica Sinica, 30: 533-535.