Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STUDY ON QUANTUM ZERO KNOWLEDGE PROOF SYSTEM

[1] XIAOQIANG GUO, [2] YAN YAN, [3] LICHAO FENG [4] SHIQIU ZHENG
[1]College of Science, Hebei United University, No.46 Xinhua West Street, Tangshan 063009, Hebei Province, China
E-mail: [1]guoxiaoqiang@heuu.edu.cn, [2]guoxq2004@163.com

ABSTRACT

Zero-knowledge proof is a very interesting problem in modern cryptography, which attracts the attention of many cryptographers, and there are plenty of researches. It is one of the hot research field in cryptography. First, we made a simple introduction of zero-knowledge proof. Then we had given a perfect quantum zero knowledge proof system on a specific NP – complete problem "graph 3-coloring"(G3C). And we use reduction structure to promote any NP – complete problem. At last, we introduced the applications of zero knowledge proof in cryptography.

Keywords: *Quantum Zero-Knowledge Proof, Cryptography, Graph 3-Coloring, Information Security*

1. INTRODUCTION

Suppose we know some secret channel, if we want others to believe that we know this secret information, but do not want people to know this secret information, then we can take advantage of zero knowledge proof to others that we know this secret information. Assume P is the owner of some secret information, P wants to prove himself mastering those secret information to Q. Q is verifier, and to verify whether P really master those secret information. The so-called zero knowledge proof is P managed to make Q believe in himself that he is the master of these secret information, but at the same time not leak these secret information to Q.

The earliest Goldwasser proposed the concept of zero knowledge proof [1]. After verifier participated in the process of zero knowledge proof, any information that can be calculated in polynomial time also can be calculated independently by verifier in polynomial time, as long as he believes the authenticity of the proposition. The definition of zero knowledge proof systems mainly considers two different probability distributions:

- Finished with proof of interaction, the probability distribution generated by the polynomial time verifier.
- A probabilistic polynomial time automata generated the probability distribution based on the premise to be proven proposition correctness.

The resulting three different levels of zero knowledge proof systems:

(i) perfect zero knowledge: in this system in the above two distribution completely identical.

(ii) calculation zero knowledge: in this system the two distributions in polynomial time indistinguishability, that is the two distributions cannot be separated from the test of any probabilistic polynomial time.

(iii) statistical zero knowledge: in this system the two distribution close to the statistical characteristics, namely the statistical difference between the two can be neglected.

NP complete problem is non-deterministic polynomial complexity problem. In [2,3,4], O. Goldreleh, S. M icali, and A. Wigderson use any one-way permutation to construct a zero knowledge proof for any language in NP. In [5], M. Blum, P. Feldman, and S. Micali got the conclusion that any mathematical theorem has a zero knowledge proof. In [8], Y. Deng, and D. D. Lin proposed the new concept of instance-dependent verifiable random functions. It is also a powerful tool to construct a higher security zero knowledge protocol. In [9], S.

Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

F. Huo and F. L. Yan designed a scheme for quantum zero knowledge protocol in a group using a mode of quantum secure communication. In [10], M. R. Shi, and Z. H. Jiang got two efficient implementations of instance-dependent verifiable pseudo random function and the proof of security. In [11], Z. J. Wang, L. L. Sun, and H. Y. Ma presented a new zero-knowledge protocol for SDH pair(A， a)， which is based on Chik How Tan encryption. In [12], C. M. Yuan had given zero knowledge proofs protocol based on Paillier cryptosystem, which runs in one-round while ensure the completeness property and the soundness property, and decreases the communication traffic in the maximum extent.

In section 2 we mainly study on quantum zero knowledge proof system. First we propose a particular NP-complete problems –graph 3-coloring. Next we construct quantum zero knowledge proof system on graph 3- coloring using quantum bit commitment protocol. At last we give a specific reduction process from any NP problem to G3C zero knowledge proof system. In section 3 we introduce the applications of zero knowledge proof in cryptography. We separately discuss in password communication protocol, identification, symmetric use of public key cryptography, against chosen ciphertext attacks, network protection.

2. QUANTUM ZERO KNOWLEDGE PROOF SYSTEM

2.1 A Particular Np Complete Problems -- Graph 3-Coloring

Graph 3-coloring language classes denoted G3C, including all of limited graphs satisfied the following conditions: these graphs may be used in three different colors on the vertex shader, so that any two adjacent vertices have different colors. Formal, if there is a mapping

$$\varphi: \quad V \to \{1,2,3\}$$

make for each $(u,v) \in E$ have $\varphi(u) \neq \varphi(v)$, then the graph $G = (V,E)$ is called three-coloring.

Specific shown in Figure 1 and Figure 2.

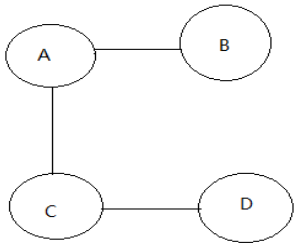

Figure 1 Graph 3- Colorable

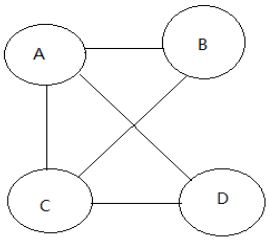

Figure 2 Graph 3- Non-Colorable

2.2 Quantum Zero Knowledge Proof System On G3c

Next, we use the unconditional security of quantum bit commitment scheme to construct quantum zero knowledge proof system on graph 3-coloring.

Protocol 2.1 G3C ( )

i) P and Q common input a graph 3 – colorable $G = (V,E)$.

ii) Repeat the following step 3 to step 6 $|E|^2$ times.

iii) Let φ is a 3-coloring of graph G. P randomly selects a permutation π of $\{1,2,3\}$ with equal probability distribution. And makes $\varphi(u) = \pi(\varphi(u)), u \in V$. That φ is a random 3- coloring of graph G (Color maker 1,2,3 is random). For each one permuted vertex coloring scheme P commit to Q using unconditionally secure QBC( ) in commitment stage of protocol.

iv) Q random uniformly select an edge $(u,v) \in E$, and send to P, and call for checking the coloring of u and v P revealed.

v) P received Q hair (u,v), using the protocol in reveal stage of QBC( ) revealed the coloring of $\varphi(u)$ and $\varphi(v)$.

vi) Q first verified coloring commitment whether it is valid. If passed, then he compare whether the same, if they are different, Q output 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to accept, the other flatly output 0 refused.

If there exists unconditional security bit commitment protocol, then there exist the perfect interactive zero-knowledge proof systems on G3C problem. It shows that unconditional security bit commitment contained zero-knowledge proof of unconditional security G3C problem. In fact, it uses bit commitment reduction to zero knowledge proof in Protocol 2.1.

2.3 All Np Complete Problems Quantum Zero Knowledge Proof

As Goldreich stressed in [2], "a particular NP complete language zero knowledge proof system can be used for each language of the NP and given zero knowledge proof system".

For each $L \in NP$, we only selected and considered a characteristic relation, notes for R_L. From L to G3C reduction abbreviated f_L , then there is a polynomial time computable function g_L, make each $(x, w) \in R_L$, $g_L(x, w)$ is 3-coloring of $f_L(x)$.

The following is a specific reduction process:

Protocol 2.2 NP – to – G3C( )

i) P and Q public input: string x (assume x in L). P auxiliary input: for $x \in L$ membership evidence w.

ii) P and Q all compute $G = f_L(x)$.

iii) P compute $\psi = g_L(x, w)$.

iv) Call the Protocal 2.1 G3C( ) zero knowledge proof: all parties call the zero-knowledge proofs of public input G , when P called this proof it also has an auxiliary input φ.

Obviously, when given a NP evidence (namely a third coloring scheme) as auxiliary input, if the prover P of G3C proof system can realize in the probability polynomial time, then the prover in Protocol 2.1 can also realize in probability polynomial time, thus complete the reduction from any NP problem to G3C zero knowledge proof system.

3. THE APPLICATIONS OF ZERO KNOWLEDGE PROOF IN CRYPTOGRAPHY

In password call, zero knowledge can provide us a method to ensure any identity, so we believe a person's identity. Next, we introduce the applications of zero knowledge proof in cryptography.

i) Password communication protocol: One can construct a communication protocol based on zero knowledge to achieve the effect of zero knowledge in communication. Zero knowledge still plays an important role in proofing the honest majority agreement incompleteness.

ii) Identification: In modern society, many places need the personal identity, such as using check, access to vital sectors, registration accommodation etc. In this case, any misidentification may leak and cause incalculable damage. Zero knowledge proof can provide us a method to ensure the safety of the identity, and this method dose not divulge any information except the identity to the other party or a third party. For example Fiat-Shamir certification system, Beth authentication scheme etc.

iii) Symmetric use of public key cryptography: In public key cryptography network communication, for new users, the public key of this is not his public key number. Thus, the other users in the network cannot communicate him due to the lack of his public key number. If we ture to zero knowledge, then it is very easy to accomplish. Let a new user and B the old user. First, B encrypted the message $m_1, m_2, \cdots, m_n$ into $x_1, x_2, \cdots, x_n$ made $E(m_i) = x_i \ (i = 1, 2, \cdots, n)$. Then B sent $x_1, x_2, \cdots, x_n$ to A. A used zero knowledge to test the public key and obtained the message and complete communication.

iv) Against chosen ciphertext attacks: For general users, public key cryptography equivalent to solve an NP-complete problem. Thus it is able to achieve their purpose. But it is fragile for “chosen ciphertext” recognized the strongest attack. The non-interactive zero knowledge proof provided a way for us solving this problem. Send two strings Y and φ to users, where Y is ciphertext of message M , φ is a non-interactive zero knowledge proof on decryption knowledge of Y . The decryption device inspected whether φ made convincing decryption of Y . If convincing, then output plaintext M . Otherwise, nothing output.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The decryption device can only output the secret that we had known. Therefore cipher clerk can also not solve the ciphertext at liberty.

v) Network protection: In net communication, many users do not want others understand their own secret and even their own intentions. The convertible zero knowledge interactive proof systems are capable of this important task, it can protect the secret of any user in network. This zero knowledge proof can complete the implicit signature and apply to electronic fund transfer system and the secret ballot system.

4. CONCLUSIONS

In this paper, we had given a perfect quantum zero knowledge proof system on a specific NP – complete problem "graph 3-coloring"(G3C). And we use reduction structure to promote any NP – complete problem. At last, we introduce the applications of zero knowledge proof in cryptography. "Software as a service" the concept is a future development trends, both application software and security software are so. Safety kind workers should be fewer but better. We should provide valuable time, information and resources with minimal cost for software developers. For this purpose, cryptography study is not in order to create all sorts of rich inspirational password, but for the average user convenient using, simple, efficient. The unconditional security research of quantum cryptography is in line with the requirements of the times. The purpose of researches of quantum cryptography is the applications. So laboratory research and standardization work are the long-term future and the most important two aspects. Let the quantum cryptography into enterprise, and then step into ordinary people's homes to uncover the cryptography mysterious veil, and serve the public, this is the unchanged responsibilities and obligations of the science and technology workers.

ACKNOWLEDGEMENTS

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

REFRENCES:

[1] S. Goldwasser, S. Micali, and C. Rackoff, “The Knowledge Complexity of Interactive Proofs Systems”, *Proe of STOC*[C], New York：ACM Press, 1985, pp. 291-304.

[2] O. Goldreich, S. Micali, and A. Wigderson, “Proofs that Yield Nothing but their Validity and a Methodology of Cryptographic Protocol Design”, *In 27th Annual Symposium on Foundations of Computer Science, IEEE* , 1986, pp. 174–187.

[3] O. Goldreleh， S. M icali, and A. Wigderson, “How to Prove all NP．Statements in Zero—knowledge and a Methodology of Cryptographic Protoca1”, *Advances in CryptologyEuroerypt* 1986.

[4] O. Goldreleh，S. M icali and A. Wigderson, “Proofs that Yield Nothing but their Validity or all Languages in NP have Zero-knowledge Proof Systems”, *J.ACM*, 38(3), 1991, pp. 691-729.

[5] M. Blum, P. Feldman, and S. Micali, “Non-Interactive Zero-Knowledge and Its Applications” , *STOC*, 1988, pp. 103-112.

[6] China Science and Technology Association, “Cryptography Subject Development Report”, *China Science and Technology Press*, 2007-2010.

[7] G. H. Zeng, “Quantum Cryptography”, *China Science and Technology Press*, 2006.

[8] Y. Deng, and D. D. Lin, “Instance-dependent Verifiable Random Functions and their Application to Simultaneous Resettability”, *Proc of the 26th Annual International Conference on Advances in Cryptology*, Berlin:Springer, 2007, pp. 148-168.

[9] S. F. Huo, and F. L. Yan, “Quantum Zero Knowledge Proof in a Group”, *Journal of Hebei Normal University(Natural Science Edition)*, Vol. 32, No. 1, 2008, pp. 37-38.

[10] M. R. Shi, and Z. H. Jiang, “Construction of High Performance Instance-dependent Verifiable Random Functions” , *Application Research of Computers*, Vol.27, No.7, 2010, pp.2621-2624.

[11] Z. J. Wang, L. L. Sun, and H. Y. Ma, “A New Zero Knowledge Proof Protocol”, *Journal of Nantong University(Natural Science Edition)*, Vo1. 10 , No. 1 , 2011, pp.16-19.

[12] C. M. Yuan, “Zero Knowledge Proofs Protocol Based on Paillier Cryptosystem”**,** *Computer and Modernization*, No.4, 2011, pp.45-49.