Higher Education Research
2021; 6(5): 142-147
http://www.sciencepublishinggroup.com/j/her
doi: 10.11648/j.her.20210605.18
ISSN: 2578-9341 (Print); ISSN: 2578-935X (Online)

Teaching Suggestions of Quantum Information to Undergraduate Students

Jianhong Shi*, Xiangqun Fu, Hongwei Li

Henan Key Laboratory of Quantum Information and Cryptography, Information Engineering University, Zhengzhou, China

Email address:
shijianhong2011@163.com (Jianhong Shi)

*Corresponding author

To cite this article:
Jianhong Shi, Xiangqun Fu, Hongwei Li. Teaching Suggestions of Quantum Information to Undergraduate Students. *Higher Education Research*. Vol. 6, No. 5, 2021, pp. 142-147. doi: 10.11648/j.her.20210605.18

Received: September 10, 2021; **Accepted**: September 29, 2021; **Published**: October 12, 2021

Abstract: Quantum information is a new subject produced by the cross integration of quantum physics and information technology, mainly including quantum communication, quantum computing and quantum metrology. In recent years, quantum information technologies such as quantum cryptography and quantum computing have developed rapidly. Under this background, some universities have set up a professional elective course of quantum information for undergraduates majoring in cyberspace security. This course mainly introduces students to quantum information related to cyberspace security, such as quantum key distribution, quantum cryptographic algorithm, quantum computing algorithm and quantum computer. This paper combs and summarizes the teaching experience of quantum information course group from the perspectives of teaching and learning. On the one hand, it discusses how teachers organize teaching effectively. According to the characteristics of undergraduates majoring in cyberspace security, teacher need to set clear teaching objectives, carefully choose teaching contents, compile appropriate teaching materials, select appropriate teaching methods and make exquisite teaching slides. At the same time, when implementing classroom teaching, teacher need to pay attention to teach the course from the perspective of cyberspace security and integrate the latest research results of quantum information into classroom teaching in real time. On the other hand, it discusses how teachers help students learn quantum information course well. Teachers should focus on visualizing the abstract theory, helping students build their own quantum information knowledge system and improve their learning enthusiasm. The teaching experience has certain reference significance for the teaching and curriculum construction of quantum information.

Keywords: Quantum Cryptography, Quantum Key Distribution, Quantum Computation, Teaching Content, Teaching Method

1. Introduction

One lesson is an organic component of one course. To instruct every lesson well, the teacher must first consider how to organize each lesson well [1-3]. This paper initially discusses how to teach the course of quantum information. Quantum information is a professional elective course in cyberspace security [4]. Quantum information technology includes quantum communication, quantum computing and quantum metrology. Among them, quantum cryptography and quantum computing are closely related to cyberspace security. The aim of the course is to help students to expand the professional knowledge vision, and understand fundamentals of quantum mechanics, quantum key distribution, quantum cryptographic algorithms, quantum computing algorithms [5-9]. Furthermore, this course can make students comprehend the influence of quantum computer on the security of classical cryptography, and acquaintance the development forefront of quantum information.

Teaching is an educational activity that teachers instruct students to understand the objective world and then promote students' physical and mental development [2, 3]. Teaching consists of teachers' teaching and students' learning, both of which are indispensable [1-3]. Only when "teaching" and "learning" are organically combined and integrated into a whole, teachers can achieve good teaching quality and effect. And then really make teaching play its due role. Therefore, in the following, it will discuss how to teach quantum information well from the two aspects of teachers' teaching

and students' learning.

There are some research results in the teaching of quantum information related courses. Chen Wei [10] introduced the teaching experience of the introduction to quantum information course offered by university of science and technology of China for undergraduates majoring in cyberspace security. This paper expounds in detail from the aspects of teaching objectives, course structure and content, teaching methods and practical means. Combined with their own teaching practice and based on the characteristics of quantum information physics, Wang Xiaoqian [11] analyzed the problems and reasons in quantum information physics teaching from three aspects: teaching content, teaching methods and examination methods, and puts forward the ideas of teaching reform. Li Yangyang [12] focuses on combining theoretical and practical application in teaching introduction to quantum computational intelligence. Peng Yonggang [13] shows how to design the classroom teaching of quantum information through several teaching examples. Economou [14] presents a simple educational program focused on quantum information for high-school and early undergraduate students. This program allows students to perform hands-on calculations with quantum circuits and algorithms, without requiring knowledge of advanced mathematics.

This paper combs and summarizes the teaching experience of quantum information course group from the perspectives of teaching and learning. Firstly, the teaching objectives and the teaching content design are explored in section 2. Secondly, teaching ideas and methods are discussed in section 3. Finally, section 4 focuses on how teachers help students learn quantum information course well.

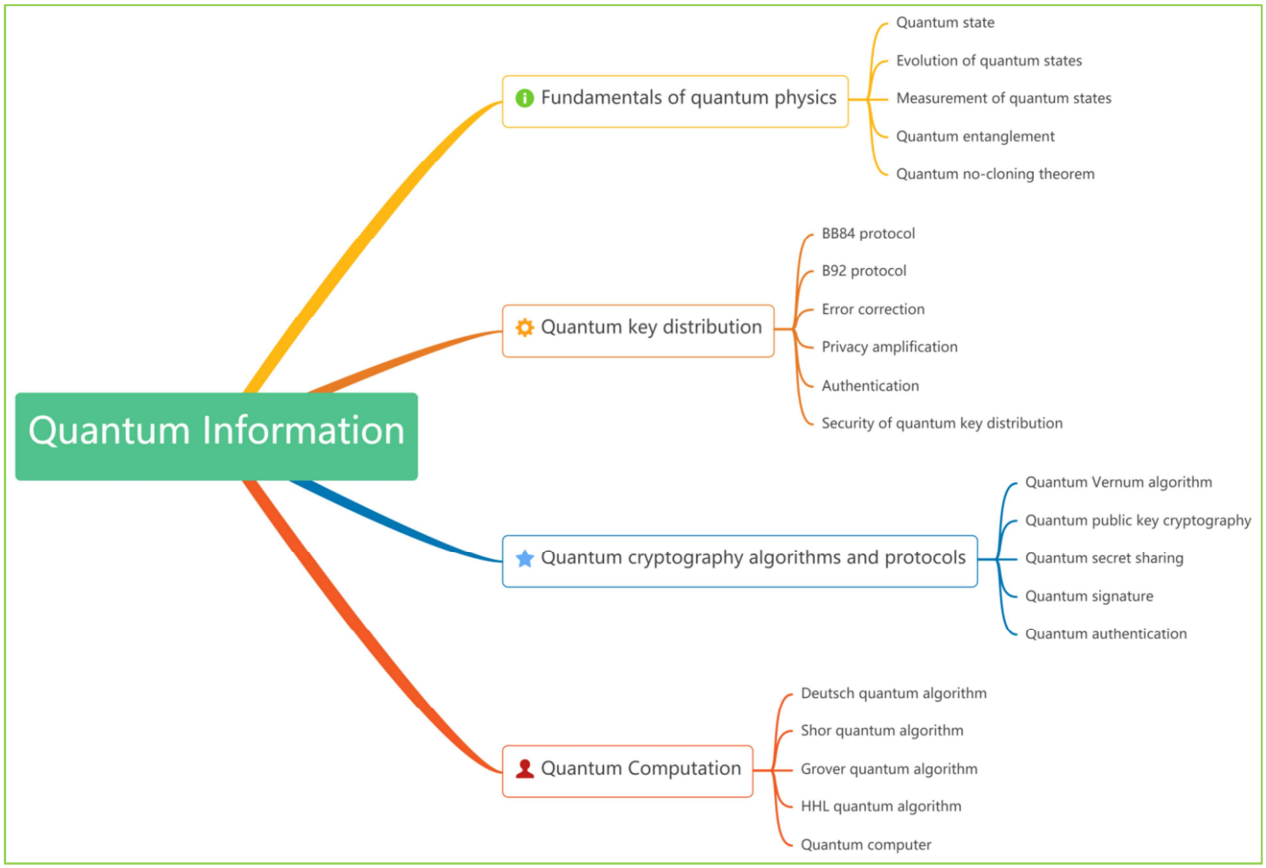

Figure 1. *Module and content design of quantum information course.*

2. Teaching Objectives and Content Design

Teachers are responsible for teaching activities [2]. Whether teachers prepare lessons adequately and the level of classroom teaching directly affects the quality and effect of teaching.

2.1. Teaching Objectives

The teaching goal is the result that teachers and students can achieve based on the existing foundation through teaching activities. The positioning of quantum information is not a comprehensive and in-depth description of the professional knowledge of quantum information. Students are expected to have a preliminary understanding of the overall picture and development context of quantum information. Therefore, quantum information mainly requires the students to master the basic concepts, principles and methods of quantum information. At the same time, let students understand the development frontier of quantum cryptography and quantum computing. For the security proof of quantum key distribution,

and the success rate analysis details of Shor quantum algorithm, students only are required to have preliminary knowledge of them.

2.2. Teaching Content

Prepare lessons is the foundation of good lessons. In order to tell a lesson well, the teacher should first grasp the teaching content on the whole and understand comprehensively. The teaching content is the main object of students to understand and master, mainly including the concept, principles, facts and views of a course [2]. Quantum information is an emerging research direction. The selection of teaching content is a process of continuous exploration. The course of quantum information mainly focuses on the combination point of quantum information technology and cyberspace security. Figure 1 shows the module and content design of quantum information course, which mainly including four modules.

The first module is the basic knowledge of quantum mechanics. This module provides students with a relatively complete introduction to the core concepts and description methods used in quantum information research. This part is relatively complete, but it is by no means exhaustive. Therefore, it is necessary to refine the core concepts used in quantum mechanics for quantum information, especially quantum cryptography and quantum computing, such as quantum state, evolution of quantum states, quantum measurement, quantum entanglement and quantum no-cloning theorem. The less used contents in quantum cryptography and quantum computing, such as the wave function and its calculation, are omitted and will not be taught.

The second module is quantum key distribution. This part is one of the most direct and close contents of the combination of quantum information and Cyberspace Security, and it is also one of the two key points of this course. Quantum key distribution is the most mature quantum cryptography technology, and has gradually become practical. This module comprehensively analyzes and explains the quantum key distribution technology from theoretical protocol to the engineering implementation. The module starts with the most basic BB84 [15] and B92 [16] quantum key distribution protocols. Then it analyzes the post-processing technologies in quantum key distribution, such as error correction, privacy amplification, authentication and so on. Secondly, the system implementation and the experimental verification of quantum key distribution are described. Finally, the theoretical and practical security of quantum key distribution is discussed. Through the systematic comparison between theory and practice, students can understand the thinking mode of the integration. Through the analysis of practical application cases of quantum key distribution, students can understand the ideas and methods of combining quantum key distribution with existing information security systems.

The third module is quantum cryptography algorithm and protocol. This module mainly introduces the theoretical contents of quantum symmetric cryptography (quantum Vernum algorithm), quantum public key cryptography, quantum secret sharing, quantum signature, quantum authentication and so on. Through the study of this module, students can have a comprehensive understanding of quantum cryptography. Quantum cryptography includes not only quantum key distribution, but also many branches related to other fields of cryptography.

The fourth module is quantum computing. This is another key content of quantum information course. Because the research progress of quantum computing is closely related to the security of classical cryptographic algorithms, quantum computing is a key content of cyberspace Security. This module mainly explains the basic concepts, characteristics and potential advantages of quantum computing. By introducing Deutsch algorithm, students can preliminarily understand the basic principle of quantum computing algorithm. Then, the basic principle of Shor algorithm for decomposing large composite numbers is analyzed. The algorithm can crack the RSA cryptographic algorithm and elliptic curve public key cryptography in quantum polynomials. Then, Grover quantum search algorithm is explained, which can accelerate the exhaustive search key attack of classical cryptographic algorithm. Finally, the research progress and the development trend of quantum computer are introduced. Quantum computing is more like a spear for the development of cyberspace security, while quantum cryptography algorithms and protocols are like a shield. By studying the content of quantum computing, students can effectively broaden their horizons and deeply understand the development opportunities and challenges brought by quantum information technology to traditional cryptography.

Through the learning of the above modules, students will have a comprehensive understanding of quantum information. Due to the limitation of class hours, there are certain choices in the scope and depth of the course content during the actual teaching. In the course implementation, it will solve this contradiction by increasing class hours and refining content, and further optimize the teaching effect in combination with the discipline development needs of information security.

When preparing lessons, it should deeply understand the basic structure and technical details of each content, find out the relationship between the teaching content of each part, as well as the basic clues throughout this course. On this basis, formulate a detailed teaching implementation plan.

2.3. Textbook Selection and Slides Making

In terms of textbook selection, quantum computing and quantum information written by Nielsen and Chuang comprehensively introduces the content of quantum information. However, it is difficult to introduce to the undergraduate students. The quantum cryptography written by Guo Hong and others has a comprehensive introduction to the background knowledge and shows a clear logical framework of quantum cryptography. It is a rare good monograph and can be used as a good teaching reference. However, the book lacks relevant content of quantum computing. Quantum cryptography compiled by Zeng Guihua pays more attention to the explanation of quantum cryptography algorithm and protocol, and some contents are worth learning from.

Generally speaking, there is still a certain gap between the main content of these textbooks and the actual needs of cyberspace security.

Based on the above considerations, the course group has selected appropriate teaching contents and compiled teaching materials suitable for students majoring in cyberspace security. Furthermore, the course group wrote the textbook "Fundamentals of quantum cryptography".

At the same time, around the central problem of each class, the teacher consults relevant books and the latest literature. Then, the teacher clarifies the specific content of each teaching link and the logical relationship between them. Subsequently, the teacher converts the teaching content into the form of text, pictures, animation and video that students can easily understand and accept. Finally, the teacher wrote a lesson plan and showed it through slide courseware.

3. Teaching Ideas and Methods

3.1. Teaching Quantum Information from the Perspective of Cyberspace Security

Because there are few physics courses in cyberspace security specialty, there are no courses in quantum mechanics and quantum optics. This leads to students' weak foundation in quantum physics. When learning the basic principles of quantum information, students are unable to think from a physical point of view. Students may have great difficulties in understanding some concepts of quantum mechanics. Therefore, it is not easy for students to explain the teaching content from the perspective of quantum physics.

However, the students have studied linear algebra, cryptography and other information security courses, and the students have a good foundation in mathematics and cryptography. From the perspective of mathematics and cryptography, it is easier for students to understand the basic knowledge of quantum mechanics, the encoding and decoding process of quantum key distribution, quantum computing algorithms and other teaching contents.

For example, when explaining the basic concepts of quantum mechanics, quantum states can be understood as vectors in complex linear space. Similarly, quantum transformation is interpreted as linear transformation, and linear transformation corresponds to matrix. When explaining quantum key distribution, the teacher first introduces the problems and challenges faced by traditional key distribution from the manual key distribution and Diffie-Hellman key exchange protocol. Then further explain the quantum key distribution technology with higher security strength. When explaining Shor quantum large composite decomposition algorithm, the teacher first reviews the secure basis of RSA public key cryptography, that is, the difficulty of large composite decomposition. Then, the decomposition problem of large composite numbers is transformed into the periodic problem of exponential function. Finally, Shor quantum algorithm is used to solve the periodic problem in quantum polynomial time, and the quantum large composite decomposition algorithm is obtained.

3.2. Tracking the Research Frontier

At present, quantum information is one of the hot research fields in the international academic community. Countries have also invested a lot of human, material and financial resources to carry out the research of quantum key distribution and quantum computing. In the course of teaching, the history, current situation and the development direction of quantum information are introduced to arouse students' interest in this course. For example, when teaching quantum key distribution, students can be introduced to the latest scientific research work being carried out in China. China successfully launched the world's first "Mozi" quantum science experiment satellite on August 16, 2016, which can be used to carry out satellite ground quantum key distribution, so as to build a wide area quantum key distribution network. When teaching Shor quantum algorithm, one can introduce the fatal threat of the algorithm to RSA public key cryptography. At the same time, the teacher introduces the development status of quantum artificial intelligence and quantum precision measurement to students. The research of quantum computer is changing with each passing day. IBM, Google, BenYuan quantum and other technology companies have developed quantum computing prototypes.

3.3. Problem Oriented Heuristic Teaching Method

Heuristic teaching means that students' knowledge acquisition is not passively injected by teachers, but actively acquired through their own thinking or association under the guidance of teachers [1]. Through heuristic teaching, students can form the habit of asking and thinking about problems, and improve their ability to analyze and solve problems. This ensures the dominant position of students and teachers in teaching activities, and can give full play to their enthusiasm in the teaching process. This ensures the dominant position of students and the dominant position of teachers. This can give full play to the enthusiasm of teachers and students in the teaching process.

The specific method of heuristic teaching is: teachers ask questions, then guide students to think about problems, and finally solve problems. For example, when explaining the encoding and decoding process of BB84 quantum key distribution protocol, the teacher first asked the students: how to encode information on photons? Then, the answer is given: the transmitter uses the four polarization states of photons to represent 00, 01, 10 and 11 respectively, so as to load the information onto the photons. Then, the transmitter sends the photons carrying information to the receiver. At this point, the question is raised again: how does the receiver decode to obtain the information of the transmitter? Finally, the teacher guides the students to draw a conclusion: the receiver randomly selects the measurement base to measure the received photons. Then, the transmitter and receiver compare the base information and retain the measurement results

consistent with the base information. At this point, both parties get the same shared key.

Another example is that when explaining the Cascade error correction method [17], the teacher introduces it from a specific example. It is known that Alice and Bob's 16 bit filter key contains exactly one error. Question: how can one find and correct this error? It is easy for students to think that this error can be found quickly by using the combination of parity check and binary search. The steps of binary error correction method are summarized, and the advantages and disadvantages of binary error correction method are analyzed. The biggest problem of binary error correction method is to correct up to one bit error at a time. At this point, ask students: if there are multiple errors in the data, how should they be corrected? This leads to the Cascade error correction method proposed by Brassard. Then, a practical example is used to explain the workflow of Cascade error correction method. Finally, the error correction effect and running speed of Cascade error correction method are analyzed.

4. How to Help Students Learn Efficiently

It is an important task for undergraduate students to acquire professional knowledge and improve professional improve the professional quality. Students are not only the teaching objects, but also the main of teaching activities [2]. Whether students can efficiently acquire knowledge is the key indicator to measure the success or failure of classroom teaching activities.

4.1. Visualization of Abstract Theory

In view of the abstract and difficult to understand teaching content of quantum information, the course group organized all teachers to focus on discussion to find teaching content design methods that are easy for students to accept. At present, the teaching contents of quantum no-cloning theorem, BB84 quantum key distribution protocol, B92 quantum key distribution protocol, Cascade error correction method, authentication method, quantum public key cryptography, Deutsch algorithm, Shor quantum large sum decomposition algorithm, Grover quantum search algorithm and so on, have been vividly displayed in the form of pictures, animation and so on. This method is easy for students to understand and master.

4.2. Building Knowledge System of Quantum Information

In the teaching process, teachers create questions to stimulate students' curiosity and encourage students to participate actively. Teachers and students jointly complete the teaching tasks. Teachers and students discuss and exchange with each other in equal communication, inspire and guide students to express their views, and enable students to actively absorb and internalize their own knowledge. Enhance students' awareness of actively participating in classroom teaching, promote students' personality development, use their own learning methods and build their own knowledge framework.

For example, in the process of learning BB84 quantum key distribution protocol, teacher use one layer after another to help students gradually uncover the mystery of quantum key distribution. At the same time, every two of them are required to simulate the sending and receiving sides to complete the whole process of quantum key distribution. Using these methods enables students to deeply understand the principles and methods of using quantum technology to distribute keys.

4.3. Improving Students' Learning Enthusiasm

Learning enthusiasm is a subjective attitude that students take the initiative to acquire knowledge about their courses. At present, the first grade students in universities have the highest learning motivation, and the enthusiasm of learning in grades two or three and four is becoming weaker and weaker. Some college students have no interest in learning and are tired of learning. They are sleepy in class, which seriously affects the teaching quality and teaching effect. How to stimulate students' learning enthusiasm and improve students' learning initiative has become one of the difficult problems perplexing university education.

As for the course of quantum information, some students have utilitarian ideas in their study. They think that their future work has nothing to do with quantum information. Learning quantum information is not helpful to their future work. Therefore, they don't want to work hard to learn this course. But can everyone's knowledge learned in college be directly applied to their work? The answer is: most people don't directly use the knowledge learned at the undergraduate stage.

For example, one of the authors majored in basic mathematics at the undergraduate stage, mainly studying courses such as mathematical analysis, advanced algebra, probability theory and mathematical statistics. In the master's research stage, he majored in applied mathematics, mainly studying and studying the model design of aircraft, automobile and industrial parts. After graduation, I came to the university to engage in the teaching and scientific research of quantum information, which is not directly related to his major. However, the logical thinking ability and self-study ability obtained through professional course training at the undergraduate and postgraduate stage, have benefited me all my life. The ability to raise, research and solve problems helped him succeed in his career.

Therefore, many courses offered at the undergraduate stage seem useless, but they can improve the ability to analyze and solve problems, improve the humanistic and scientific literacy, expand the vision of looking at problems, and broaden the ideas of analyzing and solving problems. These abilities and qualities will enhance the level and taste of one's life and enable one to better complete the work tasks. Therefore, the teacher hopes students can correct their learning attitude and improve their learning enthusiasm and initiative.

5. Conclusion

China's 14th five-year plan and the outline of long-term goals for 2035 point out that it should accelerate the development of quantum information technology, and cultivate a high-level talent team of quantum information. Incompatible with the rapid development of quantum information, there is a serious shortage of quantum information practitioners. It is urgent to set quantum information course at the undergraduate stage. Quantum information course is an important part of cultivating quantum information technology talents.

This paper combs and summarizes the teaching experience of quantum information from the perspectives of teaching and learning. The most important thing is to determine the teaching objectives and reasonably design the teaching content according to the characteristics of students. The second thing is to determine the appropriate teaching ideas and teaching methods. The last thing is helping students build their own quantum information knowledge system and improve their learning enthusiasm. It is hoped that the teaching experience in this paper can have a certain reference value for teachers who teach quantum information.

References

[1] Gong Shaowen. Ten Questions on How to Tell a Class Good. Proceedings, 2004.

[2] Pei Dina. Teaching Theory. Beijing: Education Science Press, 2007.

[3] James M. Lang. Small teaching: Everyday Lessons from the Science of Learning. John Wiley & Sons, Inc, 2016.

[4] Zhang Huanguo, Han Wenbao, Lai Xuejia, et al. Survey on cyberspace security. Scientia Sinica Information, 2016, 46 (2): 125-164.

[5] Zeng Guihua. Quantum cryptography, Beijing: Science Press, 2006.

[6] Xu Dingguo. Introduction to quantum information. Xidian University Press, 2015.

[7] Guo Hong, Li Zhengyu, Peng Xiang. Quantum cryptography. Beijing: National Defense Industry Press, 2016.

[8] Kollmitzer C. Applied quantum cryptography. Beijing: Science Press, 2015.

[9] Nielsen M A, Chuang I L. Quantum computation and quantum information. Beijing: Higher Education Press, 2003.

[10] Chen Wei, Yin Zhenqiang, Han Zhengfu, et al. Quantum information course for the undergraduate students of cyber security. Chinese Journal of Network and Information Security, 2019, 5 (3): 81-88.

[11] Wang Xiaoqian, Gou Lidan, Feng Yuling, et al. Research on the teaching reform of the course "quantum information physics". Education Modernization, 2018, 8 (32): 64-71.

[12] Li Yangyang, Shang Ronghua, Jiao Licheng. Exploration on Introduction to Quantum Computational Intelligence. Computer Education, 2011, 15: 55-57.

[13] Peng Yonggang. Understanding for teaching quantum informatics to undergraduate students. Physics and Engineering, 2012, 22 (3): 1-4.

[14] S. Economou, T. Rudolph, and E. Barnes. Teaching quantum information science to high-school and early undergraduate students. https://arxiv.org/abs/2005.07874v1, 2020.

[15] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. Proceeding of the IEEE International Conference on Computers, Systems, and Signal Proceeding (IEEE, New York), 1984, 175.

[16] Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 1992, 68 (21): 3121.

[17] Brassard G., Salvail L. Secret-Key Reconciliation by Public Discussion. Eurocrypt 1993. Lecture Notes in Computer Science, vol 765, 410-423.