附件：

**推荐江苏省教育科学研究成果奖（高校自然科学类）公示**

|  |  |
| --- | --- |
| 项目名称 | 量子计算理论与应用的研究 |
| 主要完成人 | 陈汉武，刘志昊，樊继豪，阮越，谈佳宁，李志强 |
| 主要完成单位 | 东南大学 |
| 项目简介：  本项目申报的十篇代表性论文和专著的第一作者和通信作者均属于东南大学计算机学院量子计算与量子信息研究室的老师和研究生。2016-01-01至2017-12-31期间共发表学术期刊论文29篇，其中SCI收录21篇，EI收录11篇；完成专著一部和量子计算和量子信息题解一部，其中专著《量子可逆电路综合的方法与实践》由东南大学出版社2017-09出版，题解《量子计算和量子信息（-）-量子题解》由东南大学出版社2018-01出版。  量子可逆逻辑电路应用在量子程序设计语言执行逻辑的表达，是量子算法时间、空间、能耗、代价精确表述的主要手段。《量子可逆电路综合的方法与实践》以案例驱动，从具体问题解决方案入手，配合不同的数学方法，强调“物理问题/数学建模/算法设计/程序实践”计算逻辑思维的培养。全书所有的算法设计和程序实现取自本研究室多年的研究成果。该书在全国范围、关于量子可逆逻辑电路设计方法、目前应该是唯一的专著。  本项目中申报的代表性论文研究主要内容包括：量子安全通信协议、量子容错计算、量子图像压缩和分类、量子纠缠测度。  量子安全通信协议：本次项目申报的三篇代表性论文是基于量子信息理论的计算思维和解析：分析了基于异或操作和纠缠的控制型双向量子安全直接通信网络协议，指出该协议存在信息泄露问题，即一半的秘密消息被毫无知觉地将被泄露；分析了基于三维贝尔态和纠缠交换的量子对话协议，指出该协议存在协议泄露问题，通过代数计算说明了该协议的执行过程中将有四分之一的信息被毫无知觉的泄露了；分析了基于GHZ态和一次一密的量子广播通信与验证协议，指出该协议存在安全性漏洞，理论计算和分析表明，一个外部攻击者能采取截获-测量-重发攻击该协议而不会被发现。以上发现的问题对于今后量子安全通信协议的设计具有重要的指导意义和警示作用。  量子容错计算：对于量子信息时代的到来毋庸置疑是十分重要的。本次项目申报的三篇论文是在前期工作积累的基础之上，基于代数数论和实变函数的基础，1. 构造了几类最小距离大于q+1的q元纠缠辅助量子MDS码，突破了传统q元量子MDS码最小距离皆小于等于q+1的限制；2. 提出了量子张量积码的统一构造框架；3. 重新证明了经典扩展级联码与扩展差错定位码的等价性问题。  量子图像压缩和分类：利用量子特性编码图像，图像的存储效率和部分操作的时间效率有指数级提升。我们工作完成了：1. 分析主要量子图像格式的纠缠度量（施密特数）与图像空域冗余（K\_L 变换系数）间的关系，给出数理解析描述；2. 寻求矩阵乘积态参数表达的量子图像特征方法，通过截取矩阵乘积态参数定义和提取量子图像特征； 3. 分析计算量子图像特征的距离测度（迹距离）及信息熵（冯诺依曼熵），通过最优化方法给出基于特征的量子图像无损压缩和有损压缩方法。 (4)以大规模图像分类问题为原型，测试量子图像特征的有效性，为后续图像识别算法的研究提供数据支撑。  量子纠缠测度：量子信息的强大就是因为量子信息可以叠加、可以纠缠，因此研究量子态的纠缠度，研究纠缠度在算法演化中的作用和变化就显得十分重要：论文将n量子比特构建的希尔伯特空间的元素划分为三类，构建了一个三维子空间，从这个新视角出发，获得Grover迭代为三维空间中的暇旋转的结论。面对计数问题应用场景的多样性、以及初始振幅制备时门电路的噪音可能造成初始振幅分布非均衡的问题，文章分析现有的量子计数算法在初始振幅分布非均衡状态下失效的原因，进一步依据暇旋转算子的性质，通过分析初始振幅分布与暇旋转算子的本征态之间关系的数学解析表达，最终给出通用量子计数算法。 | |
| 客观评价和应用情况  多数引文都是在其论文的参考文献中列出我们的代表性论文名称，在文章论述中仅给予了简单的、正面性的评述。  代表论文2：CONSTRUCTIONS OF q-ARY ENTANGLEMENT - ASSISTED QUANTUM MDS CODES WITH MINIMUM DISTANCE GREATER THAN q + 1 / QUANTUM INFORMATION & COMPUTATION / Jihao Fan, Hanwu Chen, juan Xu  引文信息如下：  (1). Liangdong LuEmail authorRuihu LiLuobin GuoYuena MaYang Liu. Entanglement-assisted quantum MDS codes from negacyclic codes，Quantum Inf Process, March 2018, 17:69. IF：2.192  引用文字：“In [26],Fan et al. proposed several constructions of q-ary EAQMDS codes with minimum distance greater than q + 1 based on classical MDS codes.”  (2). Kenza GuendaSomphong, Jitman, T. Aaron Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. Designs, Codes and Cryptography, January 2018, Volume 86, Issue 1, pp 121–136. IF：1.009  引用文字“Fan, Chen and Xu [7] provided a construction of entanglement-assisted quantum maximum distance separable (MDS) codes with a small number of pre-shared maximally entangled states.”    (3). Jianzhang ChenYuanyuan Huang, Chunhui FengRiqing Chen. Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Information Processing, December 2017, 16:303， IF：2.192  引用文字“A construction of entanglement-assisted quantum MDS codes with a small number of preshared entangled states was provided by Fan et al. [22].”  代表论文3：Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad/ Chinese Physics B/ Zhi-Hao Liu and Han-Wu Chen，作为量子安全直接通信的典型而被引用。  引文信息如下：  (1). Multi-party Semi-quantum Key Agreement with Delegating Quantum Computation/INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS/Liu, Wen-Jie; Xu, Yong; Yang, Ching-Nung; Gao, Pei-Pei; Yu, Wen-Bin，JAN 2018，IF：0.964；  (2). Multi-party Semi-quantum Key Agreement with Delegating Quantum Computation/ INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS/Liu, Wen-Jie; Chen, Zhen-Yu; Ji, Sai; Wang, Hai-Bin; Zhang, Jun，OCT 2017， IF: 0.964  代表性论文4：Quantum Computation for Large-scale Image Classification（他引1次）Quantum Computation for Large-scale Image Classification/ QUANTUM INFORMATION PROCESSING / yue ruan; Hanwu Chen; Jianing Tan; Xi Li  引文信息：Wiśniewska J, Sawerwain M. Recognizing the Pattern of Binary Hermitian Matrices by a Quantum Circuit[C]//Asian Conference on Intelligent Information and Database Systems. Springer, Cham, 2017: 466-475.  引用文字：The basic idea was prepared to be utilized in the field of image processing [6, 10]  代表性论文5：Quantum Image with High Retrieval Performance/ QUANTUM INFORMATION PROCESSING / Ruan Yue, Chen Hanwu, Liu Zhihao, Tan, Jianing  引文信息：尚福华, 李盼池. 彩色图像的量子水印算法[J]. 信号处理, 2017, 33(11): 1424-1435.  引用文字：其他新颖的量子图像编码、检索、匹配、定位等方法［7-10］  代表性论文9：A Construction of Quantum Error-Locating Codes∗/ COMMUNICATIONS IN THEORETICAL PHYSICS / Ji-Hao Fan and Han-Wu Chen  引文信息：Pankaj Kumar Das, ERROR LOCATING CODES AND EXTENDED HAMMING CODE, MATEMATICKI VESNIK, MATEMATIQKI VESNIK 70, 1 (2018), 89-94, March 2018. IF：0.989  引用文字：“Many works have been done in the construction of QECCs, e.g., quantum Hamming codes,[6] quantum cyclic codes,[7,8] quantum MDS codes,[9,10] quantum concatenated codes[11] and other types of quantum codes.[12]” | |
| 论文、论著目录和（或）主要知识产权证明目录  （按照推荐书表格列出主要内容，不需再做表格）   1. 量子可逆电路综合的方法与实践/ 东南大学出版社/ 陈汉武，李志强 （专著） 2. **CONSTRUCTIONS OF q-ARY ENTANGLEMENT - ASSISTED QUANTUM MDS CODES WITH MINIMUM DISTANCE GREATER THAN q + 1 / QUANTUM INFORMATION & COMPUTATION / Jihao Fan, Hanwu Chen, juan Xu。 IF：1.563** 3. **Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad/ CHINESE PHYSICS B / Zhi-Hao Liu and Han-Wu Chen. IF：1.223** 4. **Quantum Computation for Large-scale Image Classification/ QUANTUM INFORMATION PROCESSING /** **yue ruan; Hanwu Chen; Jianing Tan; Xi Li. IF：2.192** 5. **Quantum Image with High Retrieval Performance/ QUANTUM INFORMATION PROCESSING /** **Ruan Yue, Chen Hanwu, Liu Zhihao, Tan, Jianing. IF：2.192** 6. **On the Equivalence of Generalized Concatenated Codes and Generalized Error Location Codes/ IEEE TRANSACTIONS ON INFORMATION THEORY / Ji-Hao Fan and Han-Wu Chen. IF：2.679** 7. **Cryptanalysis of Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement/ IEEE COMMUNICATIONS LETTERS / Zhihao Liu and Hanwu Chen. IF：1.988** 8. **Cryptanalysis and improvement of efficient quantum dialogue using entangled states and entanglement swapping without information leakage / QUANTUM INFORMATION PROCESSING / Zhihao Liu and Hanwu Chen. IF：2.192** 9. A Construction of Quantum Error-Locating Codes∗/ COMMUNICATIONS IN THEORETICAL PHYSICS /Ji-Hao Fan and Han-Wu Chen. IF：0.989 10. **Generalized Quantum Counting Algorithm for Non-uniform Amplitude Distribution/ QUANTUM INFORMATION PROCESSING / Jianing Tan; Yue Ruan; Xi Li; Hanwu Chen. IF：2.192** | |
| 完成人情况：  （摘自“完成人情况表”中的部分内容，公示姓名、排名、行政职务、技术职称、工作单位、完成单位、对本项目技术创造性贡献）样式如下：   1. 姓名，排名1，主任，教授，工作单位：清华大学，完成单位：北京大学，是该项目主要负责人，对发现点1、2、3均有重要贡献，具体\*\*\*\*   1. 陈汉武，排名1， ，教授，工作单位：东南大学，完成单位：东南大学，是整个项目研究思路的提出者、制定者、组织者和实施者，是该项目主要负责人。是第1篇代表性论文（专著）的第一作者和通讯作者，是第2、3、4、5、9、10篇代表性论文的通信作者，是第6、7、8篇代表性论文的第二作者。  2. 刘志昊，排名2， ，副教授，工作单位：东南大学，完成单位：东南大学，是项目的第二完成人，是第3篇代表性论文的第一作者，是第7、8篇代表性论文的第一作者和通信作者，是第5篇代表性论文的作者之一。  3. 樊继豪，排名3， ，讲师，读博单位：东南大学，完成单位：东南大学，是项目的第三完成人，是第2、9篇代表性论文的第一作者，是第6篇代表性论文的第一作者和通信作者。  4. 阮越，排名4， ，讲师，读博单位：东南大学，完成单位：东南大学，是项目的第四完成人，是第4、5篇代表性论文的第一作者，是第10篇代表性论文的第二作者。  5. 谈佳宁，排名5， ，博士生，读博单位：东南大学，完成单位：东南大学，是项目的第五完成人，是第10篇代表性论文的第一作者，是第4、5篇代表性论文的作者之一。  6. 李志强，排名6，主任，教授，工作单位：扬州大学，完成单位：东南大学，是项目的第六完成人，是第1篇代表性论文（专著）的第二作者。 | |
| 合作关系证明（如有就提供） | |

|  |
| --- |
| 知情同意证明（如有就提供）：  （指未列入项目主要完成人的代表性论文（专著）第一作者及通讯作者出具的知情同意证明，扫描图片即可）  注：代表性论文和专著的第一作者和通讯作者均以列入完成人名单。 |