计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201100141

Grover 算法改进与应用综述

刘晓楠　宋慧超　王　洪　江　舵　安家乐
数学工程与先进计算国家重点实验室(信息工程大学)　郑州 450000
(prof.liu.xn@foxmail.com)

摘　要　量子信息科学是一门新兴的交叉学科,它在信息领域中有着独特的性能,在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面可突破现有经典信息系统的极限。Grover 算法是一类典型的量子算法,能够对任意经典暴力穷举搜索问题实现二次加速,进一步推动了量子计算的发展,如何有效地改进和应用 Grover 算法成为量子计算的一个重要研究领域。文中综述了 Grover 算法的优化改进和应用,对 Grover 算法在不同领域应用及不同方面的改进进行了概述,并对 Grover 算法未来的改进和相关应用的若干研究方向进行了探讨。

关键词:Grover 算法;量子计算;相位改进;密钥搜索;数据挖掘
中图法分类号　TP385

Survey on Improvement and Application of Grover Algorithm

LIU Xiao-nan,SONG Hui-chao,WANG Hong,JIANG Duo and AN Jia-le
State Key Laboratory of Mathematical Engineering and Advanced Computing(PLA Information Engineering University),Zhengzhou 450000,China

Abstract　Quantum information science is a new interdisciplinary subject,which has unique performance in the field of information. It can break through the limits of the existing classical information systems in the aspects of improving computing speed,ensuring information security,increasing information capacity and improving detection accuracy. Grover algorithm is a typical quantum algorithm,which can realize quadratic acceleration for any classical brute force exhaustive search problem,further promoting the development of quantum computing. How to effectively improve and apply Grover algorithm has become an important research field of quantum computing. This paper summarizes the optimization,improvement and application of Grover algorithm,summarizes the application and improvement of Grover algorithm in different fields,and discusses some research directions of future algorithm improvement and related applications of Grover algorithm.

Keywords　Grover algorithm,Quantum computing,Phase improvement,Key search,Data mining

1　引言

随着科技的发展,经典的基于电子传输的微电子技术的发展已经遇到瓶颈,晶体管的集成密度和传输线宽已经发展到了极致,传统集成电路制作工艺的极限迫使经典计算速度不可能一直按照“摩尔定律”持续发展,经典计算逐渐进入了发展的困境。量子计算作为一种新型的计算理论模型,正在逐渐成为信息研究领域关注的焦点。利用量子机制进行信息处理已成为突破经典计算极限的一条重要的探索途径。量子计算机就是利用微观粒子状态来进行存储和处理信息的计算工具,其基本原理就是通过物理手段制备可供操控的量子态,并利用量子态的叠加性和相干性等量子力学相关特性进行信息的运算、保存和处理操作。

早在 20 世纪初,量子力学就已经成为物理研究领域的重点。Feynman[1] 于 1982 年提出利用量子计算模拟量子力学过程的思想。Deutsch[2] 于 1985 年首次提出了量子图灵机的概念,希望利用量子力学的特性来进行信息处理以获得计算性能的提升。从量子力学的基本原理出发,量子计算理论研究的一个重要方向就是量子算法。量子算法指运行量子计算机上,利用量子力学原理解决实际问题的计算方法。目前经证实已有许多量子算法相较于经典算法而言能取得显著的加速效果。

Shor[3] 于 1994 年基于 Fourier 变换提出了大数质因子分解算法,该量子算法可以在多项式时间内破解 RSA 密码体制,这使得依赖该密码机制的电子银行、网络等在理论上不再安全。Grover[4] 于 1996 年提出针对无序数据库的量子搜索

到稿日期:2020-11-20　返修日期:2021-02-26　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61972413,61701539);国家密码发展基金(mmjj20180212)
This work was supported by the National Natural Science Foundation of China(61972413,61701539) and National Cryptography Development Fund(mmjj20180212).
通信作者:宋慧超(quantumsong@163.com)

算法，可加速破译 DES 密码体系。该算法通过幺正变换可以把其中的某一个表征搜索结果的数据概率幅逐渐放大为 1，从而使其以很大的概率测得所要的结果。该算法实现了相比经典搜索开次方的加速比。

Grover 量子搜索算法对许多启发式搜索的经典算法起到了实质性的二次加速作用，Grover 算法在搜索时不需要考虑搜索问题的内部结构的性质，将注意力放在元素的指标上，因此具有很强的通用性。这两种算法的提出使人们认识到了量子计算巨大的优越性，促使更多的研究者开始关注量子算法的研究。这两个具有里程碑意义的算法也成为了目前整个量子算法研究领域的核心。

近年来，虽然关注量子算法设计的研究者越来越多，但几乎没有再出现新颖的量子算法框架，这也直接导致了具有核心作用的量子算法的匮乏。目前量子算法的研究主要围绕着现有的几种核心量子算法。本文将重点以 Grover 算法为核心展开深入讨论，介绍 Grover 算法的改进及其应用。

2 Grover 搜索算法的改进

自 Grover[4] 于 1996 年提出数据库的量子搜索算法以来，众多学者都致力于研究该量子算法，Grover 搜索算法也在研究的过程中不断被改进，经过多年的改进，Grover 量子搜索算法逐步完善，目前已经形成了一个比较完整的搜索算法体系，能够适应各种不同的搜索需求。1998 年，Grover[5] 又提出了更为一般化的量子搜索算法。

Grover 算法主要通过变换量子基态的概率幅，来令所查询目标项对应的量子基态的概率幅达到最大。图 1 是一个完整的 Grover 算法量子线路框架图，其中涵盖初始化至等权叠加态、中间的 Oracle($\boldsymbol{U}_w$)、平均反演算子($\boldsymbol{U}_s$)和最终的测量等模块。

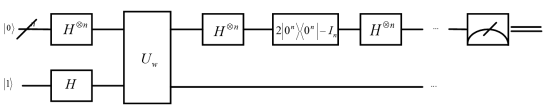

图 1 Grover 算法框架线路图

Fig. 1 Frame circuit diagram of Grover algorithm

(1)初始化制备等权叠加态，对输入基态进行 Hadamard 变换得到所有计算基态的等权叠加态，如式(1)所示：

$$|s\rangle=H^{\otimes n}|00\cdots0\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{1}$$

(2)构造 Oracle，通过构造一个映射$\boldsymbol{U}_w$，该映射使得目标项的相位反转，但对于任何与目标项正交的其他项的符号不变，即若$|a\rangle$为目标项，$\langle a|v\rangle=0$，则$\boldsymbol{U}_w|a\rangle=-|a\rangle$，$\boldsymbol{U}_w|v\rangle=|v\rangle$。

(3)构造平均反演算子，通过构造一个幺正矩阵$\boldsymbol{U}_s$，该幺正矩阵可将目标状态振幅相对于平均振幅C_x做翻转，从而达到增大搜索到目标项概率的目的，其中C_x是所有态的平均振幅。

$$\boldsymbol{U}_s=2|s\rangle\langle s|-I \tag{2}$$

$$C_x=\frac{1}{N}\sum_x C_x \tag{3}$$

(4)重复迭代，步骤(2)和步骤(3)合称 G 变换，随着 G 迭代次数的增加，搜索到目标项的概率也会发生改变。理论上，当 G 迭代的次数在$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$附近时(其中，$N$ 为元素总数，M 为目标项元素的数量)，Grover 算法搜索到目标项的概率达到最优。

2.1 相位改进

多年来不断有学者通过优化 Grover 算法中的相位来改进 Grover 算法。Long 等[6-7] 提出在 Grover 搜索过程中可以使用任意相位翻转来增大几率。随后，Long 等又发现 Grover 搜索算法中的相位匹配不能用任意的角度旋转来代替，只能采用满足相位匹配条件的角度来替代，此外标准 Grover 算法的搜索成功概率并非 100%。

2001 年，针对 Grover 算法成功概率非 100% 的情况，Long 在文献[8]中对 Grover 算法进行了修正，经 $J+1$ 次迭代之后对系统进行测量，便可以确定地得到所要搜索的目标项。文献[9]提出了任意相位旋转的相位匹配条件的精确相位公式 $\tan(\varphi/2)=\tan(\theta/2)(1-2/N)$(其中，$N$ 为元素总数，φ 和 θ 是旋转相位)，并认为 $\varphi=\theta$ 是相位公式的一种近似情形。文献[10]利用 SU(2)群和 SO(3)群同构的性质，重新推导得出 $\varphi=\theta$ 仍是个精确的相位公式的结论。相位匹配实验已经被文献[11-13]所证实。2005 年，Grover[14] 又提出了固定点量子搜索。在该算法中，Grover 利用 $\pi/3$ 相位取代了 Grover 算法中的 π 相位。

文献[15]提出，当 $M/N>1/3$ 且$\varphi'=-\theta'=\pi/2$ 时，仅需一次迭代就达到不低于 25/27 的成功概率；针对目前 Grover 算法不能区分各搜索项的重要程度以及算法失效问题，其提出了一种基于目标加权的 Grover 算法，较好地体现了多个子目标在重要程度方面的差异性。文献[16]又提出了自适应相位匹配条件，即两次相位旋转的方向相反，大小根据目标量子叠加态和系统初始状态的内积决定。文献[17]提出了固定相位旋转 Grover 算法，该算法在已有的幅度放大算法中，将旋转相位由原来的 π 改为 1.916 84π，从而使算法的成功概率提高到了 99.58%。文献[18]提出的定点优化算法能够同时兼顾 Grover 算法的成功概率和运行时间两方面，可以在目标项未知时避免过度迭代而导致成功概率降低，并实现最佳实践缩放。

为直观对比多年来不同学者在 Grover 算法中通过对相位改进的研究所带来的对搜索成功概率的提升效果，在表 1 中罗列出不同参考文献中通过对相位改进所对应的成功概率的比较。

表 1 相位改进及对应成功概率比较

Table 1 Comparison of phase improvement and corresponding success probability

相位改进文献	成功概率/%
文献[4]	大于 50
文献[8]	100
文献[15]	92.59
文献[17]	99.58
文献[19]	93.43
文献[20]	99.38
文献[21]	97.82
文献[22]	87.88

2.2 初始态优化

将 Grover 算法初始化模块推广至任意初始态分布，极大地增加了其算法的普适性。1998 年，文献[22]提出具有任意初始分布的 Grover 量子算法，给出了标记态和非标记态幅度随时间演化的一阶线性微分方程，并给出了方程的精确解以及测量的最优时间和最大成功概率的新的表达式，证明了这些表达式的值依赖于标记态和非标记态初始幅度分布的均值和方差，而不取决于高阶矩。

2002 年，文献[23]又将 Grover 量子搜索算法推广到具有任意初始混合态的情形。通过计算搜索一个标记态的成功概率发现，这一概率尽管与初始纯态具有相同的形式，但强烈地依赖于系统的初始混合态，同时还发现 Von Neumann 熵不是衡量算法有效性的尺度。2005 年，文献[24]针对初态为 n 个量子位的任意纯态 $|\varphi\rangle$ 的情形，发现执行测量的最佳时间与 $|\varphi\rangle$ 无关。其根据 $|\varphi\rangle$ 的幅度导出了搜索成功的概率，发现这一概率不依赖于 r，在将成功概率看作一种纠缠测量的情况下，考查了这些结果的相关性，并将以前局限于只有一个标记态的 Grover 纠缠测量推广到了多个标记态的情况。

2.3 部分量子搜索

部分量子搜索算法是量子搜索算法的扩展，以减少搜索的信息量来换取搜索速度的提高，比标准的 Grover 单模式量子搜索数据的速度快，但文献[25]仅提出了对数据库进行部分搜索的搜索次数的最低限，未指出具体的搜索次数。文献[26]简化了 Grover 的部分搜索算法，比 Grover 单模式量子搜索算法少了 $0.34\sqrt{k}$ 次迭代（$k=M/N$，其中 M 是数据块数，N 是数据库中总的数据项）。

以上两个关于 Grover 算法的改进都是只针对单模式，文献[27]提出了多模式部分 Grover 算法，可以对多模式大容量数据库进行搜索，以减少搜索次数。文献[28-30]提出部分扩散操作来优化 Grover 算法，当搜索空间解的数目大于 $N/3$ 时，仅一次迭代就能以高于 90% 的概率搜索到目标项。

2.4 目标项个数未知

Grover 算法中搜索成功的概率随着迭代次数的改变而发生变化。当到达最优迭代次数时，搜索成功的概率达到最大，而后会出现随着迭代次数增加概率反而下降的情况，故选择合适迭代次数尤为重要。迭代次数 k 取决于 M（目标项个数）和 N（元素总数）。针对 M 未知从而无法选择合适迭代次数的问题，学者们在探索过程中给出了不同的解决方法。

文献[31]在 Grover 算法的基础上提出了针对问题解个数未知情况下的 Boyer 算法，该算法节省了很多的量子线路，而其他很多同类量子算法都使用了量子计数技术[32]（需要指数级规模的线路）。2016 年，文献[34]针对目标分量数未知导致无法以高概率测量到目标项的问题，提出了迭代自适应 Grover 算法，只需在反演算子中添加一个判断相位的门电路，通过一次查询 Oracle 的开销实现 Grover 算法在最优迭代终止，其在搜索空间较小时比原算法搜索成功概率更大。

文献[35]提出了一种针对 Grover 算法中搜索目标项未知的改进算法，搜索效率取决于目标项的二进制字符串 0 或 1 的个数，而非二进制字符串的总长度。当字符串中 0 或 1 的个数非常少时，改进的复杂度是指数级的。文献[36]针对 Grover 算法中目标项个数未知所导致的无法确定合适迭代次数的问题，提出了新型量子计数改进方法。

表 2 列出了不同文献中当目标项未知时所需要消耗的量子资源及搜索成功的概率的比较。‘↓’表示偏下，‘↑’表示偏上，由于各改进算法间难以用具体资源消耗来具体描述，因此用中、高、低等来刻画不同算法间的比较关系。

表 2 M 未知时各改进算法量子资源消耗及成功概率比较

Table 2 Comparison of quantum resource consumption and success probability of each improved algorithm when M is unknown

算法	消耗	概率
文献[31]中的算法	中	中
文献[32]中的算法	高	高↓
文献[33]中的算法	中↓	高
文献[34]中的算法	低	中↑
文献[35]中的算法	中	高↓
文献[36]中的算法	中↑	高↓

2.5 优化搜索概率

Grover 算法通过改变迭代次数能以接近 1 的概率搜索成功，但是在某些情况下会存在 Grover 搜索算法失效的问题，即随着迭代次数的改变，搜索成功概率处于不理想的状态。文献[37]提出了当 $M>N/3$ 时可改变 $\boldsymbol{U}$ 和 $\boldsymbol{D}$（$\boldsymbol{U}$ 为选择性旋转变换矩阵，$\boldsymbol{D}$ 为概率幅变换矩阵）变换矩阵的改进 Grover 算法。当 $M>N/3$ 时，其仅需一次迭代就能以超过 90% 的概率获得正确解，解决了原 Grover 算法在多解时为达到同样成功率所需的迭代次数变化不规则的情况。

2004 年，文献[38]针对 Grover 算法多次搜索后仅达到过半的成功概率且无确定最佳搜索次数等问题，提出了一种确定多次数的计算方法，该方法可使 Grover 法逼近全概率地获得搜索目标。文献[39]针对 Grover 算法中解的个数增加导致搜索成功概率减小的问题，提出了基于扩大搜索空间的改进算法，同时为了在成功概率与迭代次数之间折中，增加了新参数使得算法可调。

2019 年，文献[40]针对迭代次数自适应 Grover 算法中存在的部分效率低下和目标分量占比过半时的时效问题进行改进，通过将搜索空间增加至 $4N$，来确保解个数占比恒小于 1/4。其最终通过仿真实验说明了改进算法的有效性和优势。2020 年，文献[41]结合量子算法和先验知识提出了一个最优的量子搜索算法，当求解的概率给定时，在给定的查询次数下获得最大的预期成功概率。该算法的量子优势随着解的分布更有偏向而增加。

2.6 其他方向的改进

除了以上有关 Grover 算法的改进，学者们经过多年对 Grover 算法的研究还提出了在其他方面的一些改进，同样对 Grover 算法的完善起到了不可或缺的作用。文献[42]解决了在低维空间查找局部最小元素的量子下界问题。文献[43]将经典穷举算法引入到了 Grover 算法中，可以有效地解决某些带有特定前提条件的量子搜索问题，进一步扩大了 Grover 算法的适用性范围。文献[44]提出的子集和问题的量子中间相遇算法结合了经典中间相遇攻击算法和 Grover 算法的特点。与原 Grover 算法相比，新算法在增加了存储复杂性的条

件下实现了降低计算复杂性的目标。2020 年,文献[45]提出了一种新的基于 Grover 线路的深度优化算法,通过将分治策略与深度优化相结合,来降低 Grover 算法的线路深度。

3 Grover 搜索算法的应用

3.1 Grover 算法在网络路由中的应用

随着对量子通信研究的不断深入,量子通信网络的发展也在快速进行。Grover 算法凭借着二次加速的优势开始应用在无线量子通信网络中。2014 年,文献[46]将 Grover 算法应用于无线路由问题中,在路由建立成功率和纠缠量子对数目的基础上减少了网络计算量,节省了网络资源,使路由快速收敛,能在限定跳数内搜索出目标路径。

文献[47]针对移动自组网(Mobile Ad Hoc Net Work, MANET)网络的特性,提出采用 Grover 算法来降低网络的计算量。文献[48]提出了基于 Grover 算法的无线 Mesh 网流量均衡路由算法,通过 Grover 迭代获得流量均衡路径,可以有效地平衡无线 Mesh 网流量,使每个用户获得的最小带宽最大化,执行效率也优于同类算法。2015 年,文献[49]将 Grover 算法应用于多约束路由算法,算法对路径采用了非线性路径长度的度量方法,提高了满足条件可行解的搜索范围和效率,能以更大概率获得最优解。与同类算法相比,该算法运行中涉及的不确定性参数较少,增加了算法普适性和实用性。2016 年,文献[50]提出了基于 Grover 思想的无线传感路由算法,该算法通过 Grover 算法降低网络多目标规划的计算量,解决了多目标决策的难题,有效地降低了计算量和网络传输时延,延长了网络生存时间。

表 3 列出了负载均衡最短路径树(LB-SPT)算法、综合解决(INT)算法、最短路径(SP)算法、蚁群(ANT)算法、Grover 搜索路由(GSR)算法在路由搜索时计算复杂度的对比,其中假设网络中有 N 个节点、M 条边,路径平均长度为 k,GSR 凭借二次加速在路由搜索中复杂度最低。

表 3 在路由搜索中各算法的计算复杂度比较

Table 3 Comparison of computational complexity of algorithms in routing search

算法	复杂度
SP	$O(N^2)$
ANT	$O(cN^3)$
GSR[48]	$O(k\sqrt{N})$
LB-SPT[51]	$O(N^3)$
INT[52]	约 $O(N^{3/2}+N^2+kN)$

3.2 Grover 算法在机器学习中的应用

近年来,越来越多的学者开始研究量子计算和机器学习的结合领域,一是希望通过量子计算解决机器学习的运算效率问题,二是希望通过探索量子力学的性质来开发更加智能的机器学习算法。2000 年,文献[53]通过将 Grover 算法和神经网络融合,提出一种量子联想记忆模型,与传统 Hopfield 模型相比,在存储容量方面具有指数级的扩充。2003 年,研究人员[54]曾考虑借助 Grover 算法的二次加速效果处理 SVM 模型的优化计算问题。文献[57]将 Grover 算法应用至感知机的训练中,通过在线训练的方式,在每次判别训练数据是否被错误分类的过程中使用量子搜索算法可实现平方加速。2014 年,文献[58]提出基于 Grover 算法的人脸识别算法,通过将 Grover 算法融入到主成分分析中,使人脸识别的效率在经典基础上进行了二次加速。文献[59]提出的融合 Grover 算法思想的量子最近邻算法通过将一个未知点 u 分配给簇 A 或簇 B,使错误分配的概率和量子 Oracle 查询的数量最小化,从而实现加速效果。该算法弥补了文献[60]中的方法在许多实际问题中分配精度低的缺陷。

文献[63]将 Grover 算法中的 Oracle 算子以及相位估计算法嵌入到经典 K 近邻算法,该算法使用 Grover 算法一次性搜索出最相似的 k 个点。该算法可以明显降低经典计算复杂度,且在已有算法[59]基础上再次带来了 k 值的二次加速 $O(R\sqrt{kM})$(其中,R 为 Oracle 算子的执行次数,M 为样本全局个数)。

2020 年,文献[64]提出将 Grover 算法应用于求解 NP 完全数字划分问题,即给定 n 个权重为整数的对象,判定是否存在一个平衡比例的二分区问题。Grover 算法在划分问题的计算复杂度上提供了一个已知相变的量子加速,并在模拟性能上识别了相变的特征。

表 4 给出了机器学习中各算法复杂度的比较。其中,N 为训练样本数,n 为训练向量维度,m 为训练样本数,x 为训练集,k 为聚类簇总数,E 为边条数。

表 4 机器学习中各算法复杂度的比较

Table 4 Comparison of complexity of different algorithms in machine learning

算法	量子复杂度	经典复杂度
QSVM[54-56]	$O(\log(mn))$	$O(mn)$
QPCA[58]	二次加速	—
QK-NN[59]	$O(\log(mn))$	$O(mn)$
QK-means[60]	$O(k\log(mn))$	$O(mn)$
QD-L[61]	$O(\sqrt{N}E^2(\sqrt{k}+\max_x\sqrt{k}))$	$O(NEk)$
QK-medians[62]	$O(n^2/k)$	$O(n^{3/2}/\sqrt{k})$

3.3 Grover 算法在哈希函数中的应用

哈希函数问题在密码分析领域中得到了深入的研究,它将任意长度的输入数据压缩为较小的固定长度的输出数据。由于其函数本身的不可逆性,通过散列值获取原始消息异常困难,数字签名的安全性直接取决于哈希函数的安全性。通过用 Grover 算法求解哈希函数碰撞问题可极大降低计算复杂度。

文献[65]针对任意 r-to-one 函数碰撞搜索问题,提出了一种基于 Grover 的量子搜索算法,其基本思想是将给定集合中的元素随机分成两个子集,在确定某一子集元素后运用 Grover 量子搜索算法在另一子集中寻求碰撞,该算法相对于经典算法可以达到 $O(\sqrt[3]{N/r})$ 的加速。文献[66]将 Grover 搜索算法对缩放哈希函数的原像进行量子搜索,并提出了一套精确评估量子门数量和线路深度的方法。

文献[67]应用 Grover 搜索算法至生日攻击,该算法只需要 $O(2^{m/3})$ 的计算就能找到一个哈希冲突(其中,m 是哈希空间值的大小),大大地降低了算法的复杂度。实验结果证明,该算法在只需要 $O(2^{74.7})$ 期望评估的情况下就能明显提高攻击效率,比任何已知的经典算法都更有效。

表 5 列出了 NewFORK-256 在不同算法攻击下的复杂度

比较。Grover 是本团队在文献[67]中提出的攻击算法，通过表 5 中的数据对比发现，该算法的计算复杂度最低且成功率为 1。

表 5 NewFORK-256 在不同算法攻击下的复杂度比较

Table 5 Complexity comparison of NewFORK-256 under different algorithm attacks

算法	复杂度	成功率
改 Grover[67]	$O(2^{74.7})$	1.0
B-FA[68]	$O(2^{256})$	1.0
BA[69]	$O(2^{128})$	0.5
MITM[70]	$O(2^{112.9})$	0.5

3.4 Grover 算法在密钥搜索中的应用

Grover 算法凭借在无序搜索问题中的二次加速特性被广泛地应用在各种搜索问题中，其中在密码学中可将 Grover 算法用于密钥的求解。2009 年，文献[71]融合了 Grover 算法和中间相遇攻击的思想，提出了量子中间相遇搜索算法，并在 $O(56*2^{56})$ 内完成了对 3 个密钥的三重 DES 攻击，相对已有的攻击算法，该算法降低了算法的计算复杂度。

2010 年，文献[72]提出了将 Grover 算法应用于经典密码算法——AES 密钥搜索，并设计出了 AES 算法的密钥搜索量子线路，节省了计算时间和存储空间。文献[73]将传统的并行搜索思想与 Grover 算法相结合，采用多个芯片并行计算的思想，在对最好的经典算法进行二次加速的基础上提高了攻击效力。

2016 年，文献[74]利用 Grover 算法的快速搜索优点，提出了基于 Grover 算法的 ECC 扫描式攻击方法。该算法对于密钥长度为 l 的 ECC，计算复杂度由 2^l 降低到了 $\sqrt{2}\,l^{3/2}$，进一步提高了破解效率。文献[75]针对 ECC 的侧信道攻击中密钥出现错误比特，难以避免且无法快速修正的问题，提出将 Grover 量子中间相遇搜索算法应用于针对 ECC 的侧信道攻击中。该算法可以在 $O(\sqrt{l/M})$ 步修正规模为 l 且存在 M 错误比特的密钥，与传统搜索算法的计算复杂度 $O(l^{M+1})$ 相比，计算复杂度大幅度降低。文献[76]将基于 0.1π 相位旋转的 Grover 算法应用至 ECC 电压毛刺故障攻击中，最大化地提高了搜索正确密钥的成功概率，指数级地降低了复杂度，有效提升了量子计算对密码攻击的普适性和致命性。

表 6 列出了不同加密算法下计算复杂度的比较。其中，l 为密钥长度，k 为 DES 中的密钥个数，m 为每次 Grover 搜索到的正确密钥长度，M 为密钥中需要修正的错误比特长度。从表 6 中的数据来看，各算法对应的量子复杂度明显优于所对应的经典复杂度。

表 6 不同加密算法下计算复杂度的比较

Table 6 Comparison of computational complexity under different encryption algorithms

算法	量子复杂度	经典复杂度
3DES[71]	$O(2^{\sqrt{kl}})$	$O(2^{kl})$
AES[73]	$O(2^{\sqrt{l}})$	$O(2^{l})$
ECC[75]	$O(\sqrt{l/M})$	$O(l^{M+1})$
ECC[76]	$O(2^{2m/3})$	$O(2^{l})$

2013 年，文献[77]修正了文献[78]中使用融合 Grover 算法的中间相遇攻击算法的一些错误，并提出了一种针对 NTRU 改进量子中间相遇攻击算法，较大程度地降低了时间和空间复杂度，增加了攻击范围。

表 7 针对 NTRU 的不同算法的复杂度比较

Table 7 Comparison of complexity of different NTRU algorithms

算法	复杂度
C-MITM	$O(C_{N/2}^{d/2}/\sqrt{N})$
Our-GA[77]	$O(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor})+\overline{O}(\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}})$
Q-MITM[78]	$O(C_{N/2}^{d/2}\log C_{N/2}^{d/2})+\overline{O}(\sqrt{C_{N/2+1}^{d/2}})$
W-Attack[79]	$O(\sqrt{C_{N+1}^{d}})$

表 7 列出了针对 NTRU 的不同算法的复杂度比较。其中，$O(\cdot)$ 表示经典计算复杂度，$\overline{O}(\cdot)$ 表示量子计算复杂度。

3.5 Grover 算法在海量数据中的应用

如何从海量数据中尽快挖掘出所需信息是如今待解决的一大难题，经典的数据挖掘方法是基于目标变量依赖于其他变量的某些预定函数实现的，计算复杂且搜索速度慢。学者们尝试将 Grover 算法应用于数据挖掘中，以获得加速。2005 年，文献[80]将 Grover 算法应用于挖掘网络数据，使用该方法进行网络数据关联规则挖掘、权威页面挖掘和 Weblog 记录挖掘比任何经典方法都快得多。

文献[81]应用 Grover 算法至多维图像分割问题中，根据要分割的图像，选择合适的相位旋转角度和迭代次数，能够高效地实现图像分割。文献[82]提出了一种基于量子密码和 Grover 算法的数据中心安全管理方案。其利用量子 Grover 算法来寻找密钥处理过程的最优参数，以最小化整个密钥管理的计算复杂度。

文献[40]将改进后的 Grover 算法应用于求解粗糙集的核属性，可有效地解决之前算法部分效率低下和失效的问题。2018 年，文献[83]将 Grover 搜索算法应用在海量的 Weblog 中，以快速查找用户的 IP 地址，不仅保证了用户识别的准确率，同时大大提高了查询的效率。2020 年，文献[84]将 Grover 搜索应用于高能粒子物理领域中，利用 Grover 算法在粒子的高碰撞能量下所产生的海量数据中搜索目标粒子衰变产物的信息。最终通过搜索到的碰撞后粒子产物信息和探测器测得的相关信号，证明了碰撞后的粒子簇中希格斯玻色子的存在。

3.6 Grover 算法在其他领域中的应用

Grover 算法除上述应用外，还广泛应用于其他领域。2015 年，文献[85]基于 Grover 算法给出了求根问题的一个亚指数时间算法——RF-Grover 算法，该算法在 $O(\sqrt{M/k})$ 时间内能以至少 50% 的概率得到求根问题的其中一个解，这是对求根问题经典穷举算法的二次加速。文献[86]将 Grover 算法应用至 MIMO-OFDM 系统信号检测，通过利用 Grover 算法寻找最小判决值以判决发送序列，可以在有效降低复杂度的同时，达到与经典最佳接收算法基本相同的性能。

文献[87]基于 Grover 算法的思想提出了定点二重性量子搜索算法。该算法使用非幺正算符，平均需要 $N/4$（N 表示数据库中的数据量）步运算次数来定位标记的状态。2020 年，文献[88]将 Grover 算法应用至求解 K 着色问题，采用了

一种基于比较器的方法，还提出了一个可在任何含噪中等规模的量子设备上实现任意无权图和无向图的 K 着色问题的端到端自动化框架。文献[89]提出了将 Grover 搜索算法应用至字符串比较，通过设计一种特殊的 Oracle 结构，能够实现并行地比较字符串的所有字母，从而提高整体的性能。文献[90]结合经典加量子(Grover 算法)设计出对相关整数分解的量子线路，拓宽了 Grover 算法的应用领域。

4 存在问题与未来发展趋势

随着学者们对 Grover 算法的不断完善和对其应用领域的不断探索，Grover 算法凭借着其二次加速的优势在多种应用场景中发挥着重要的作用。本节结合 Grover 算法的加速特性、现有的应用领域和算法改进历程，列出了以下几个未来的改进方向和应用领域以供探讨。

4.1 Grover 算法最优迭代次数的改进

Grover 算法的核心是通过多次迭代来增加搜索到目标态的概率幅，每次迭代都耗费大量的量子资源，并且当 Grover 算法到达最优迭代后，增加迭代次数反而会出现搜索概率下降的问题，在浪费资源的同时搜索效果较差。当目标项个数给定时，可以通过计算确定最佳的迭代次数。当目标项个数未知时，已有的算法包括量子计数、迭代自适应等也能对最佳迭代次数进行估计。然而，传统的量子计数算法使得 Grover 算法的线路更加繁琐，迭代自适应中所提出的判断门相位的门电路在目前的算法平台上的模拟也存在限制，并且在获得解概率上没有任何提升。关于 Grover 算法最优迭代次数的改进仍是一个重要的研究方向，对该算法今后的应用领域的拓展意义重大。

4.2 Grover 算法线路深度的改进

在 Grover 算法的实际模拟中，由于依赖于核心模块的多次迭代来提高概率幅，因此核心模块具体实现所消耗的量子资源对整个算法的模拟影响巨大。对于 Grover 来说，用于区分目标态的 Oracle 往往需要较深的线路，如何优化其线路深度，使其能在资源受限的量子平台上高效执行是目前各界关注的一大难题。实验结果证明，量子线路的深度改变对其实验结果的影响大于其宽度的变化。目前的一个优化方向是在构建 Oracle 时可通过引入辅助量子比特来减少线路的深度，即以线路宽度的增加来降低其整体的深度，从而达到优化实验线路、提高实验结果的目的。总之，有效改进 Grover 算法深度使其能落地应用是未来研究的一大重要方向。

4.3 Grover 算法在密码破译中的应用

Grover 算法的提出对 AES 产生了巨大影响，AES(高级加密标准)是用来取代旧的数据加密标准(DES)和三重 DES 的新一代的密码标准。AES 是一种迭代行分组密码，有着固定的轮函数和固定的分组长度(128 bit)，但密钥长度可变。Grover 算法凭借着其二次加速的量子优势用于分组密码量子密钥穷举搜索，能实现将密钥长度减半的攻击效果。通过分析 Pollard，针对 RSA 密码体系提出的 $p-1$ 因式分解算法中的核心模块，即将 N 的分解问题规约为寻找一个满足属性的 y 值，未来可尝试结合 Grover 算法搜寻 y 值来实现量子加速。因此，Grover 算法和密码学的结合同样也是一个非常有研究意义的方向，对量子密码学的发展也起到了重要的影响。

4.4 Grover 算法在人工智能中的应用

近年来，量子物理和人工智能在数据科学方面的结合引起了学术界的高度关注，形成量子机器学习前沿领域。利用量子计算叠加特性，量子机器学习可通过量子并行解决目前机器学习中数据量巨大、训练过程缓慢等难题，并有望从量子物理的角度提出新的学习模型。Grover 算法通过与经典的机器学习算法如主成分分析、神经网络、最近邻算法等的结合，成功地实现了量子加速效果。未来量子机器学习的研究方向不仅仅局限于以量子思想来优化现有的经典机器学习算法，还可以从量子计算的角度出发设计能在量子计算机上运行的量子算法，优化某些在经典计算机上不可计算的问题，从而大幅降低机器学习算法的计算复杂度。

结束语 本文对 Grover 算法的改进和应用进行了较为全面的综述。在改进方面分别对相位、初始状态、搜索概率、目标项个数未知等相关优化进行介绍，在应用方面分别对网络路由规划、海量数据挖掘、密钥求解、哈希函数碰撞等领域进行简单阐述。最后，对 Grover 算法的未来改进和应用发展方向进行了展望。

参 考 文 献

[1] FEYMAN R P. Simulating Physics with Computers[J]. International Journal of Theoretical Physics, 1982, 21(6): 467-488.

[2] DEUTSCH D. Quantum Theory, the Church-Turing Principle and the UniversalQuantum Computer[J]. Proceedings of the Royal Society of London, 1985, 400(1818): 97-117.

[3] SHOR P W. Algorithm for Quantum Computation: Discrete Logarithms and Factoring Algorithm[C]// Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, USA, 1994: 124-134.

[4] GROVER L K. A Fast Quantum Mechanical Algorithm for Database Search[C]// Proceedings 28th ACM Symposium on Theory of Computation. New York, 1996: 212-219.

[5] GROVER L K. A Framework for Fast Quantum Mechanical Algorithms[C// Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing(STOC '98). 1998: 53-62.

[6] LONG G L, ZHANG W L, LI Y S, et al. ArbitraryPhase Rotation of the Marked State Cannot Be Used for Grover's Quantum Search Algorithm[J]. Communication in Theoretical Physics, 1999, 32(3): 335-270.

[7] LONG G L, LI Y S, XIAO L, et al. Grover Quantum Search Algorithm and Its Improvement [J]. Nuclear Physics Review, 2004, 21(2): 114-116.

[8] LONG G L. Grover Algorithm with Zero Theore-tical Failure Rate[J]. Physical Review A, 2001, 64(2): 436-454.

[9] HOYER P. On Arbitrary Phases in Quantum Amplitude Amplification[J]. Physical Review A, 2000, 62(5): 052304.

[10] LONG G L, YAN H Y, LI Y S, et al. General Phase Matching Condition for Quantum Searching[J]. arXiv: quant-ph/0107013.

[11] BHATTACHARYA N, VAN LINDEN VAN DEN HEUVELL

H B,SPREEUW R J C. Implementation of Quantum Search Algorithm Using Classical Fourier Optics[J]. Physical Review Letters,2002,88(13):137901.

[12] PUENTES G,MELA C L,LEDSMA S,et al. Optical Simulation of Quantum AlgorithmsUsing Programmable Liquid-crystal Displays [J]. Physical Review A,2004,69(4):42319-042319.

[13] LONG G L,YAN H Y,LI Y S,et al. Experimental NMR Realization of a Generalized Quantum Search Algorithm[J]. Physics Letters A,2001,286(2/3):121-126.

[14] GROVER L K. Fixed-point Quantum Search[J]. Physical Review Letters,2005,95(15):256-259.

[15] LI P C,LI S Y. Phase Matching in Grover's Algorithm[J]. Physics Letters A,2007,366(1/2):42-46.

[16] LI P C,LI S Y. Phase Matching in Quantum Searching Algorithm with Weighted Targets [J]. Chinese Journal of Computational Physics,2008,25(5):623-630.

[17] YOUNES A. Fixed Phase Quantum Search Algorithm[J]. arXiv:0704.1585,2007.

[18] YODER T J,LOW G H,CHUANG I L. Fixed-Point Quantum Search with an Optimal Number of Queries[J]. Physical Review Letters,2014,113(21):210501.

[19] ZHONG P C,B W S. Research on Quantum Searching Algorithms Based on Phase Shifts[J]. Chinese Physics Letters,2008,25(8):2774-2777.

[20] LI X,LI P C. A Fixed-Phase Quantum Search Algorithm with More Flexible Behavior[J]. Journal of Quantum Information Science,2012,2(2):28-34.

[21] MA B W,BAO W S,LI T,et al. A Four-Phase Improvement of Grover's Algorithm[J]. Chinese Physics Letters,2017,34(7):33-37.

[22] BIRON D,BIHAM O,BIHAM E,et al. Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution [J]. Lecture Notes in Computer Science,1998,1509:140-147.

[23] BIHAM E,KENIGSBERG D. Grover's Quant-um Search Algorithm for an Arbitrary Initial Mixed State[J]. Physical Review A,2002,66(6):062301.

[24] SHAPIRA D,SHIMONI Y,BIHAM O,et al. Algebraic Analysis of Quantum Search with Pureand Mixed States[J]. Physical Review A,2005,71(4):42320-42320.

[25] GROVER L K,RADHAKRISHNAN J. Is Partial Quantum Search of a Database Any Easier? [J]. arXiv: quantph/0407122,2004.

[26] KOREPIN V E,GROVER L K. Simple Algorithm for Partial Quantum Search[J]. Quantum Information Processing, 2006,5(1):5-10.

[27] ZHOU R G. Multi-mode Partial Quantum Search Algorithm [J]. Journal of Southwest Jiao tong University:Natural Science Edition,2008,46(4):193-195.

[28] YOUNES A,ROWE J,MILLER J. A Hybrid Quantum Search Engine:A Fast Quantum Algorithm for Multiple Matches[J]. arXiv:quantph/0311171,2003.

[29] YOUNES A,ROWE J,MILLER J. Quantum Search Algorithm with More Reliable Behavior Using Partial Diffusion[C]// Proceedings of the seventh International Conference on Quantum Communication,Measurement and Computing. 2004:171-174.

[30] YOUNES A,ROWE J,MILLER J. Quantum Searching via Entanglement and Partial Diffusion[J]. Physica D Nonlinear Phenomena,2008,237(8):1074-1078.

[31] BOYER M,BRASSARD G,HOYER P,et al. Tight Bounds on Quantum Search[J]. WILEY-VCH Verlag Berlin GmbH,1998,46(4/5):493-505.

[32] BRASSARD G,HOYER P,TAPP A. Quantum Counting [C]// Proceedings of 25th International Colloquium Automata Language and Programming. Berlin:Springer-Verlag,1998(1443):820-831.

[33] SUZUKI Y,UNO S,RAYMOND R,et al. Amp-litude Estimation without Phase Estimation[J]. arXiv:1904.10246,2019.

[34] ZHU W N,CHEN H W. Grover Algorithm for Iteration Number Adaptive[J]. Chinese Journal of Electronics,2016,44(12):2975-2980.

[35] LIU J. An Optimum Algorithm for Quantum Search[J]. arXiv:2010.03949,2020.

[36] AARONSON S,RALL P. Quantum Approxim- ate Counting, Simplified[J]. arXiv:1908.10846,2020.

[37] SONG H,DAI K,WANG Z Y. AnImproved Quantum Search Algorithm[J]. Computer Engineering and Science,2002,24(5):4-7.

[38] CHEN H G,LI B,SHEN Z K. Search Times Calculation of Approximate Full Probability Grover Algorithm[J]. Computer Engineering and Applications,2004(3):58-59.

[39] ZHANG Y D,WEI G,WU L N. An Improved Grover Quantum Search Algorithm[J]. Signal Processing,2009,25(2):256-259.

[40] XIE X M,DUAN L Z,QIU T R,et al. Improved Quantum Search Algorithm and Its Application in Solving Nuclear Properties[J]. Computer Engineering and Applications,2020(14):57-61.

[41] HE X Y,ZHANG J L,SUN X M. Quantum Search with Prior Knowledge[J]. arXiv:2009.08721,2020.

[42] SUN X M,YAO A C. On the Quantum Query Complexity of Local Search in Two and Three Dimensions[J]. Algorithmica, 2009,55(3):576-600.

[43] JIN W L,CHEN X D. Phase Mismatch Quantum search algorithm[J]. Acta Electronica Sinica,2012,40 (1):189-192.

[44] BAO W S,SONG Z,ZHONG P C,et al. Quantum Meet-in-the-middle Search Algorithm for Subsets and Problems[J]. Chinese Journal of Electronics,2011,39(1):128-132.

[45] ZHANG K,KOREPIN V E. Depth Optimization of Quantum Search Algorithms beyond Grover's Algorithm[J]. arXiv:1908.04171,2020.

[46] PENG H,JING J. Research on Grover Routing Algorithm for Wireless Self-organizing Quantum Communication Network [J]. Journal of Zhejiang University of Technology,2014,42(6):612-615.

[47] MENG L M,SONG W B. MANET Routing Protocol Based on Grover Search Algorithm [J]. China Communications:English Edition,2013(3):145-156.

[48] LIU Y G. Traffic Equalization Routing Algorithm for Wireless Mesh Networks Based on Grover Search [J]. Computer Applications, 2014(7): 1956-1959.

[49] LIU Y G. Multi-constraint Routing Algorithm Based onGrover Search [J]. Communications Technology, 2015, 48(5): 594-597.

[50] DING W J, ZHOU K, ZHOU G M, et al. Research on Routing Algorithm of Wireless Sensor Network Based on Grover Fusion Theory [J]. Journal of Sensing Technology, 2016, 29(9): 1425-1429.

[51] BEJERANO Y, HAN S J, KUMAR A. Efficient Load-balancing Routing for Wireless Mesh Networks[J]. Computer Networks, 2007, 51(10): 2450-2466.

[52] HE J, CHEN J, CHAN S H G. Extending WLAN Coverage Using Infrastructure less Access Points[C]// HPSR 2005: Proceedings of Workshop on High Performance Switching & Routing. Piscataway: IEEE, 2005: 162-166.

[53] VENTURA D, MARTINEZ T. Quantum associative memory [J]. Information Sciences, 2000, 124(1/2/3/4): 273-296.

[54] ANGUITA D, RIDELLA S, RIVIECCIO F, et al. Quantum Optimization for Training Support Vector Machines [J]. Neural Networks, 2003, 16(5/6): 763-770.

[55] REBENTROST P, MOHSENI M, LLOYD S. QuantumSupport Vector Machine for Big Data Classification[J]. Physical Review Letters, 2014, 113(13): 130503.

[56] LI Z, LIU X, XU N, et al. Experimental Realization of a Quantum Support Vector Machine [J]. Physical Review Letters, 2015, 114(14): 140504.

[57] WIEBE N, KAPOOR A, SVORE K M. Quantum Perceptron Models[J]. arXiv: 1602.04799, 2016.

[58] RUAN Y, CHEN H W, LIU Z H, et al. Quantum Principal Component Analysis Algorithm [J]. Journal of Computer Science, 2014(3): 666-676.

[59] WIEBE N, KAPOOR A, SVORE K M. Quantum Algorithms for Nearest-Neighbor Methods for Supervised and Unsupervised Learning [J]. Quantum Information & Computation, 2014, 15(3): 318-358.

[60] LLOYD S, MOHSENI M, REBENTROST P. Quantum Algorithms for Supervised and Unsupervised Machine Learning[J]. arXiv: 1307.0411, 2013.

[61] WIEBE N, KAPOOR A, SVORE K M. Quantum deep learning [J]. arXiv: 1412.3489, 2014.

[62] AIMEUR E, BRASSARD G, GAMBS S. Quantum Clustering Algorithms[C]// Proceedings of the 24th International Conference on Machine Learning. Corvallis, USA, 2007: 1-8.

[63] CHEN H W, GAO Y, ZHANG J. Quantum K-Nearest Neighbor algorithm [J]. Journal of Southeast University (Natural Science edition), 2015, 45(4): 647-651.

[64] GAILTA, OGNJEN M, VICTORIA B, et al. Number Partitioning with Grover's Algorithm in Central Spin Systems[J]. arXiv: 2009.05549, 2020.

[65] BRASSARD G, HOYER P, TAPP A. Quantum Algorithm for the Collision Problem[J]. arXiv: quantph/9705002, 1997.

[66] SERGI R, EMANUELE B, JOSE I L, et al. Quantum Search for Scaled Hash Function Preimages[J]. arXiv: 2009.00621, 2020.

[67] DU F W, WANG H, MA Z, et al. Quantum Collision Search Algorithm Against New Fork-256[J]. Journal of Electronics, 2014(4): 366-370.

[68] DIFFIE W, HELLMAN M E. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard[J]. Computer, 2006, 10(6): 74-84.

[69] BELLARE M, KOHNO T. Hash Function Balance and Its Impact on Birthday Attacks[C]// Eurocrypt Conference. 2004: 401-418.

[70] SAARINEN M J O. A Meet-in-the-Middle Collision Attack Against the New FORK-256[J]. Indocrypt, 2007(2): 10-17.

[71] ZHONG P C, BAO W S. Quantum Metathesis Search Algorithm of Triple DES [J]. Science Bulletin, 2009, 54(19): 3003-3007.

[72] YE F, YUAN J B. Key Search Quantum Circuit Design of AES Encryption Algorithm [J]. Journal of Southwest Jiao tong University, 2010(2): 302-306.

[73] DUAN B J, YUAN J B, YANG J, et al. Research on Parallel Quantum Search Attack of Packet Encryption Algorithm [J]. Small Microcomputer Systems, 2011(9): 1908-1912.

[74] CHEN Y H, JIA H H, JIANG L Y, et al. ECC Scanning Attack Based on GroverAlgorithm [J]. Information Network Security, 2016(2): 28-32.

[75] JAI H, WANG C, GU J, et al. Correction of ECC Attack Error Bit Based on Grover Quantum Meet-in-the-middle Search Algorithm [J]. Information Network Security, 2016(6): 28-34.

[76] WANG C, CAO L, JIA H, et al. ECC Voltage Burr Attack Algorithm Based on 0.1 Rotational Phase Grover algorithm [J]. Journal of Communications, 2017, 38(8): 1-8.

[77] WANG H, MA Z, MA C G, et al. An Efficient Quantum Meet-in-the-middle Attack against NTRU-2005[J]. ChinSciBull, 2013(58): 3514-3518.

[78] XIONG Z, WANG J, WANG Y, et al. An Improved MITM Attack against NTRU[J]. Int. J. Sec. App., 2012(6): 269-274.

[79] WANG X, BAO W S, FU X Q. A Quantum Algorithm for Searching a Target Solution of Fixed Weight[J]. Chinese ence Bulletin, 2011, 56(6): 484-489.

[80] MU W J, YOU Z H, ZHAO M H, et al. Mining Web Data with Quantum Grover Search Algorithm[J]. Computer Applications, 2005, 25(10): 2310-2311, 2317.

[81] LI H S. Research on Key Technologies of Quantum Image processing [D]. Chengdu: University of Electronic Science and Technology of China, 2014.

[82] ZHAO H Y, WANG X Q, MA Y. Big Data Security Authentication Scheme Combining Quantum Cryptography with Grover Search [J]. Journal of Xiangtan University, 2016, 38(4): 76-79.

[83] ZHU W N, LIU Z H. User Recognition Algorithm Based on Quantum Computing[J]. Acta Electronica Sinica, 2008, 46(1): 24-30.

[84] ANTHONY E, OLIVER K. Application of a Quantum Search Algorithm to High-Energy Physics Data at the Large Hadron Collider[J]. arXiv: 2010.00649, 2020.

[85] SUN G D, SU S H, XU M Z. Quantum Computing Algorithm for Root Problem [J]. Journal of Beijing University of Technology, 2015(3): 366-371.

[86] ZHOU L Z, LI F. Signal Detection of Communication System

Based on Grover Algorithm [J]. Computer Engineering, 2010, 36(15): 250-252.

[87] HAO L, LIU D, LONG G L. An N/4 Fixed-point Duality Quantum Search Algorithm [J]. Science China, 2010, 53(9): 1765-1768.

[88] AMIT S, DEBASRI S, AMLAN C. Circuit Design for K-coloring Problem and It's Implementation on Near-term Quantum Devices [J]. arXiv: 2009.06073, 2020.

[89] VIKRAM M. Quantum String Comparison Method[J]. arXiv: 2005.08950, 2020.

[90] SONG H C, LIU X N, WANG H, et al. Integer Decomposition Based on Grover Search Algorithm[J]. Computer Science, 2021, 48(4): 20-25.

LIU Xiao-nan, born in 1977, Ph.D, associate professor, master's supervisor, is a member of China Computer Federation. His main research interests include quantum algorithm and high-performance parallel computation.

SONG Hui-chao, born in 1996, postgraduate. His main research interests include quantum algorithm and so on.