# 基于量子克隆的二面体群隐含子群问题量子算法的研究

金广龙 袁家斌
(南京航空航天大学计算机科学与技术学院 南京 210016)

**摘 要** 基于最短向量问题的格公钥密码体制是典型的抗量子计算密码体制。格的唯一最短向量问题可转化为二面体群的隐含子群问题。有效地求解二面体群的隐含子群问题可攻破基于格的唯一最短向量问题的公钥密码体制。Kuperberg提出了二面体群隐含子群问题的半指数级量子算法。通过研究Kuperberg量子算法,利用概率量子克隆,文中提出了二面体群隐含子群问题的多项式时间量子算法。

**关键词** 隐含子群问题,二面体群,最短向量问题,量子克隆,线性多项式
**中图法分类号** TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.08.040

## Quantum Cloning-based Quantum Algorithm for Dihedral Hidden Subgroup Problem

JIN Guang-long YUAN Jia-bin
(College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 210016, China)

**Abstract** Kuperberg presented a quantum algorithm for the dihedral hidden subgroup problem, but with sub-exponential time and query complexity. We presented a quantum cloning-based quantum algorithm for dihedral hidden subgroup problem with polynomial time and query complexity. Dihedral hidden subgroup problem is related to poly(n)-unique shortest vector problem. If the dihedral hidden subgroup problem is solved efficiently, the lattice-based cryptography can be breaken, which is secure against quantum computers.

**Keywords** Hidden subgroup problem, Dihedral group, Shortest vector problem, Quantum cloning, Linear polynomial

## 1 引言

随着信息科学与通信技术的飞速发展,信息的快速传递在为经济发展和生活带来便利的同时,也附带了安全隐患。网络信息安全成为越来越重要且不可忽视的一门技术,特别是在军事情报、国家机密、银行等方面显得尤为重要。而现实中存在着各式各样的信息安全威胁,譬如窃取、伪造、欺骗、篡改等等。为了应对各种安全威胁,出现了各种信息安全技术,其中最基础、最有效的就是密码技术。密码技术为信息与通信提供了各种安全性服务。

现代密码学中,密钥加密解密技术可分为对称密码体制和公钥密码体制。公钥密码在信息安全中担负着密钥协商、数字签名、消息认证等重要角色,已成为最核心的密码体制。公钥密码体制的安全性依赖于数学难题的困难性。例如,基于大整数分解的困难性——RSA公钥密码体制、基于离散对数问题的困难性——ElGamal密码体制和ECC等,这些公钥密码都被广泛地应用于各种安全性服务。最近几年,出现了另一种非常吸引人的密码技术——量子密码。相对于量子密码,对称密码体制与公钥密码体制都称为经典密码,经典密码的安全性都是基于数学上的技巧或者难题,而量子密码的安全性依赖于量子力学的一些特性。目前,各国团队在进行各种量子密钥分发实验,也提出了各种更安全、更有效的量子密码协议,为投入实际使用做准备。这些量子密码技术在理论上比公钥密码体制更安全,可以做到绝对安全的密钥分配协议。

量子密码与量子计算都属于量子信息科学(quantum information science)。量子信息科学是量子力学、计算机科学、信息科学等的交叉学科。它利用量子力学的独特性质对计算、编码、信息处理给予新的理念。最初学者们为了模拟物理系统时发现因需要处理的数据太大,经典计算机无法满足要求,所以想设计另一种计算模型来有效模拟物理系统,之后这个计算模型被称为量子图灵机。自从提出量子计算机之后,学者们利用量子算法对各种数学NP问题进行计算。虽然目前量子计算机只是一个量子计算模型,但在理论上通过求解特定问题后发现,量子计算机比经典计算机求解速度更快,甚至求解速度可提高到指数级。其中利用量子计算模型分析密码的安全性就是一个典型的例子。设计特定的量子算法,攻破公钥密码是一个密码分析的研究热点。因公钥密码的安全性依赖于数学问题的困难性,所以通过量子算法有效求解特定数学问题,就可攻破依赖于这些数学难题的公钥密码。

### 1.1 隐含子群问题

隐含子群问题(hidden subgroup problem)是现今量子计算中的一个研究热点。1994年Shor[1]提出了量子算法,其可在多项式时间内求解大整数分解问题(factoring)和离散对数

到稿日期:2013-10-25 返修日期:2014-01-06 本文受面向大型客机全球化协同研制的信息安全体系(2009AA044601)资助。
金广龙(1988-),男,硕士生,主要研究方向为信息安全、量子密码,E-mail:jinguanglong11@nuaa.edu.cn;袁家斌(1968-),男,博士后,教授,主要研究方向为信息安全、高性能计算、量子密码。

问题(discrete logarithm)。而大整数分解问题和离散对数问题为 RSA 公钥密码体制、Diffie-Hellman 密钥分配协议等提供了安全性依据。可见,Shor 算法的提出对这些公钥密码体制构成了严重的安全威胁。

大整数分解问题和离散对数问题都可归结为 Abel 群(交换群)的隐含子群问题。Abel 群的隐含子群问题在量子计算机上多项式时间内可得到求解,而在经典计算机上最好的算法的复杂度仍然是指数级。现在对隐含子群问题的研究主要集中在两个非 Abel 群、二面体群(dihedral group)和对称群(symmetric group)。

1998 年 Ettinger 和 Hoyer[2] 开始研究非 Abel 群的隐含子群问题,其目标是结构最简单的非 Abel 群——二面体群,并给出了二面体群的隐含子群问题(DHSP, dihedral hidden subgroup problem)的量子算法。虽量子算法的时间复杂度是多项式的,但求解二面体群的隐含子群要经过指数级运算,才能求解出隐含子群的生成元。虽然没有有效求解 DHSP,但其把 DHSP 简化为求解隐含子群的生成元$(s,1)$,为之后的研究提供了理论基础。

2001 年,Murphy[3] 对二面体群问题隐含子群问题进行了深入研究,将二面体群 $D_N$ 与 $D_{\frac{N}{2}}$ 的同构性质引入到二面体群隐含子群问题中,只要求解出$(s,1)$中 $s$ 的最低有效位就可求解 DHSP,为之后的研究打下了坚实的基础。

2002 年 Regev[5] 提出格上的唯一最短向量问题(poly(n)-uniqueSVP, Unique Shortest Vector Problem)可归结为二面体群的隐含子群问题。而格公钥密码体制的安全性依赖于最短向量问题的困难性。若有效解决 DHSP,对基于 poly(n)-uniqueSVP 的格公钥密码体制的安全性提出挑战。

根据 Ettinger 和 Hoyer[2] 和 Murphy[3] 理论,2003 年 Kuperberg[4] 提出了 DHSP 的半指数级二面体群隐含子群问题的量子算法,时间复杂度是 $2^{O(\sqrt{n})}$,空间复杂度也是 $2^{O(\sqrt{n})}$。其中利用了管道思想求解 $s$ 的最低有效位。该算法的时间复杂度小于目前已知的最快经典算法的时间复杂度 $\sqrt{2^{O(N)}}$。

2004 年,Regev[6] 改进了 Kuperberg 的量子算法,虽然使算法的空间复杂度降低为 $O(n)$,但提高了时间复杂度($2^{O(\sqrt{n\log n})}$)。Regev 把 DHSP 转化为子集合问题(Subset Sum Problem)的方式,降低了空间复杂度。

2010 年,Childs、Jao、Soukharev[7] 等人提出寻找椭圆曲线的 Isogeny 映射可归结为某种二面体群的隐含子群问题,又一次强调了解决二面体群的隐含子群问题的重要性。

2011 年,Kuperberg[8] 改进了 Regev 的 DHSP 量子算法,把时间复杂度降低为 $2^{O(\sqrt{\log n})}$。

### 1.2 量子克隆

量子不可克隆定理(no-cloning theorem)是量子力学的一个重要结论,它告诉我们一个未知的量子态无法以 1 的概率被精确地复制。这个定理对于量子密码的安全性是至关重要的,它能保证第三方不可以在不被发现或污染信源的情况下截取信道里的量子态。1982 年 Wootters 和 Zurek[9] 首次提出量子不可克隆定理,证明了无法精确克隆纯态(pure state)。1996 年,Barnum 等人[10] 证明了无法精确克隆混合态(mixed state)。虽然我们无法做到精确复制,但我们可以降低要求,也就是进行近似量子克隆(approximate quantum cloning)或概率量子克隆(probabilistic quantum cloning)。

目前,近似量子克隆机也大致分为 3 种量子克隆机,对于不同的量子信息协议,可以用不同的量子克隆机进行安全性分析。对任意未知量子态以同样的保真度(fidelity)进行克隆的量子克隆机叫通用量子克隆机(universal quantum cloning machine)。若要克隆的输入态的振幅已知而相位未知,则称之为相位协变量子克隆(phase-covariant quantum cloning)。若输入态的相位已知而振幅未知,则称之为实数态量子克隆(real state quantum cloning)。概率量子克隆机可对未知量子态进行精确克隆,以一定的概率得到与输入态相同的量子态。1998 年,Duan 等[11] 提出了概率量子克隆理论。1999 年,Pati[12] 便将概率克隆的情形进一步推广到多个拷贝的线性叠加上,使得这种克隆机器的能力更为强大。

## 2 基础理论

设 $D_N$ 是一个二面体群,其中 $N\geqslant 1$。$D_N$ 是正 $N$ 边形的对称群,元素由反射(reflection)和旋转(rotation)构成,其中旋转角度为$\frac{2\pi}{N}$。$D_N$ 的阶为 $2N$,元素有 $N$ 个旋转 $r^k$ 和 $N$ 个反射 $r^k s$,$0\leqslant k\leqslant N-1$,其中元素满足下列关系式。

$$\begin{cases} r^N=s^2=srsr=Id \\ r^{a_1}s^0r^{a_2}s^{b_2}=r^{a_1+a_2}s^{0+b_2} \\ r^{a_1}s^1r^{a_2}s^{b_2}=r^{a_1-a_2}s^{1+b_2} \end{cases}$$

二面体群 $D_N$ 同构于两个循环群的半直积(semi-direct product),即 $D_N\cong\mathbb{Z}_N\times_\varphi\mathbb{Z}_2$,其中 $\mathbb{Z}_N$、$\mathbb{Z}_2$ 是循环群。我们用 $(a,b)$ 表示 $r^a s^b$,其中 $a\in\mathbb{Z}_N$,$b\in\mathbb{Z}_2$,且满足 $(a_1,b_1)(a_2,b_2)=(a_1+(-1)^{b_1}a_2, b_1+b_2)$。元素 $(a,b)$ 的逆是 $(a,b)^{-1}=((-1)^{b+1}a,b)$。

设 $D_N$ 是一个二面体群,且 $H$ 是 $D_N$ 的一个子群,即 $H\subseteq D_N$,给定一个函数 $f:D_N\to S$,其中 $S$ 为任意一个集合。该函数 $f$ 在子群 $H\subseteq D_N$ 的陪集上是不变的,且在每个不同的陪集上都不同,即 $\forall g_1,g_2\in D_N$,$f(g_1)=f(g_2)\Leftrightarrow g_1H=g_2H$。隐含子群问题是找出关于函数 $f$ 的子群 $H$。

Ettinger 和 Hoyer[2] 指出 DHSP 的问题可简化为找到隐含子群 $H$ 的生成元的反射斜率 $s$(slope of the reflection)。

设 $G'=\mathbb{Z}_N\times_\varphi\{0\}$,显然 $G'$ 是 $D_N$ 的子群。通过循环群的隐含子群问题的量子算法,可以求 $G'$ 的关于 $f(x,0)$ 的隐含子群,其中 $x\in\mathbb{Z}_N$。设 $H'$ 为 $G'$ 的隐含子群,则 $H'=G'\cap H$,且 $H'=(r\mathbb{Z}_N)\times\{0\}$。若 $H'\neq H$,则至少存在一个反射 $(s,1)\in H$,假设存在不同于 $(s,1)$ 的反射 $(s',1)\in H$,则 $(s,1)(s',1)=(s-s',0)\in H'$,即 $(s',1)=(s,1)(s-s',0)\in(s,1)H'$。可知,$H=H'\cup(s,1)H'$,其中 $0\leqslant s\leqslant r-1$。最终二面体群的隐含子群问题简化为找到反射斜率 $s$。

事实上,只要求得反射斜率 $s$ 的最低有效比特位,就可以求次低有效比特位 $s$。由于 $D_{2^n}$ 同构于 $D_{2^{n-1}}$,通过同样的算法可获得 $s$ 的次低有效比特位,而算法中的函数取决于 $s$ 的最低有效比特位,若最低有效比特位是"0",则执行函数 $f'$:$D_{N/2}\to R$,其中 $f'(a,b)=f(2a,b)$;若结果是"1",则执行函数 $f''$:$D_{N/2}\to R$,其中 $f''(a,b)=f(2a+1,b)$,依此类推,我们最终可以求得所有 $s$ 的比特位,即可以得出 $s$。所以以有效的算法求得 $s$ 的最低有效比特位是整个 DHSP 量子算法的关键。

## 3 多项式时间 DHSP 量子算法

首先制备初态$\frac{1}{\sqrt{2N}}\sum_{a,b}|a\rangle|b\rangle|f(a,b)\rangle$。测量第三个量

子寄存器后，第一、第二量子寄存器坍缩到量子态$\frac{1}{\sqrt{2}}(|x\rangle|0\rangle+|x+s\rangle|1\rangle)$，其中$x\in[0,N-1]$是任意值。设$|t\rangle=|x+s\rangle$，且$|x\rangle=|x_1x_2\cdots x_n\rangle$，$|t\rangle=|t_1t_2\cdots t_n\rangle$，$|s\rangle=|s_1s_2\cdots s_n\rangle$，其中$x_i,t_i,s_i=\{0,1\}$，$i=1,2,\cdots n$。设$t_i=x_i\oplus d_i$，又$t_i=x_i\oplus s_i\oplus c_{i+1}$，其中$c_{i+1}$是进位项，可知$d_i=s_i\oplus c_{i+1}$，显然最低有效比特位没有进位项，所以$s_n=d_n$。因此，通过求$d_n$，可以得到$s$的最低比特位$s_n$。

1. 对寄存器$\frac{1}{\sqrt{2}}(|x_1x_2\cdots x_n\rangle|0\rangle+|t_1t_2\cdots t_n\rangle|1\rangle)$的第一量子态进行$H^{\otimes n}$变换。得到的量子态是

$$\begin{aligned}&\frac{1}{\sqrt{2^{n+1}}}\{\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{x_1z_1\oplus x_2z_2\oplus\cdots\oplus x_nz_n}|z_1z_2\cdots z_n\rangle|0\rangle+\\&\quad\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{t_1z_1\oplus t_2z_2\oplus\cdots\oplus t_nz_n}|z_1z_2\cdots z_n\rangle|1\rangle\}\\&=\frac{1}{\sqrt{2^{n+1}}}\{\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{x_1z_1\oplus x_2z_2\oplus\cdots\oplus x_nz_n}|z_1z_2\cdots z_n\rangle\\&\quad|0\rangle+\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{(x_1\oplus d_1)z_1\oplus(x_2\oplus d_2)z_2\oplus\cdots\oplus(x_n\oplus d_n)z_n}\\&\quad|z_1z_2\cdots z_n\rangle|1\rangle\}\\&=\frac{1}{\sqrt{2^{n+1}}}\{\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{x_1z_1\oplus x_2z_2\oplus\cdots\oplus x_nz_n}|z_1z_2\cdots z_n\rangle\\&\quad|0\rangle+\sum_{z_1}\sum_{z_2}\cdots\sum_{z_n}(-1)^{x_1z_1\oplus x_2z_2\oplus\cdots\oplus x_nz_n}|z_1z_2\cdots z_n\rangle\\&\quad(-1)^{d_1z_1\oplus d_2z_2\oplus\cdots\oplus d_nz_n}|1\rangle\}\end{aligned}$$

2. 测量第一寄存器之后，设随机得到某一量子态$|z_{i1}z_{i2}\cdots z_{in}\rangle$，则整个寄存器坍缩为

$$\frac{1}{\sqrt{2}}|z_{i1}z_{i2}\cdots z_{in}\rangle(|0\rangle+(-1)^{d_1z_{i1}\oplus d_2z_{i2}\oplus\cdots\oplus d_nz_{in}}|1\rangle)$$

3. 对第二个寄存器进行 Hadamard 变换，然后进行测量，得到的测量结果为$y_i$。

我们得到$y_i$后，可算出$d_1z_{i1}\oplus d_2z_{i2}\oplus\cdots\oplus d_nz_{in}$，即当$y_i=0$时，$d_1z_{i1}\oplus d_2z_{i2}\oplus\cdots\oplus d_nz_{in}=0$；当$y_i=1$时，$d_1z_{i1}\oplus d_2z_{i2}\oplus\cdots\oplus d_nz_{in}=1$。通过概率量子克隆机得到$O(n)$个量子态$\frac{1}{\sqrt{2}}(|x\rangle|0\rangle+|x+s\rangle|1\rangle)$。循环步骤1到3，进行$n$次循环后，得到$n$个量子态$|z_{i1}z_{i2}\cdots z_{in}\rangle$，$i=1,2,\cdots,n$和$n$个$d_1z_{i1}\oplus d_2z_{i2}\oplus\cdots\oplus d_nz_{in}$的值，可建立线性方程组，只要系数矩阵的行列式$\begin{vmatrix}z_{11}&z_{12}&\cdots&z_{1n}\\z_{21}&z_{22}&\cdots&z_{2n}\\\vdots&\vdots&\ddots&\vdots\\z_{n1}&z_{n2}&\cdots&z_{nn}\end{vmatrix}$不等于0，则可以求出线性方程组$\begin{vmatrix}z_{11}&z_{12}&\cdots&z_{1n}\\z_{21}&z_{22}&\cdots&z_{2n}\\\vdots&\vdots&\ddots&\vdots\\z_{n1}&z_{n2}&\cdots&z_{nn}\end{vmatrix}\begin{vmatrix}d_1\\d_2\\\vdots\\d_n\end{vmatrix}=\begin{vmatrix}y_1\\y_2\\\vdots\\y_n\end{vmatrix}$的解，即$d_1d_2\cdots d_n$。

显然，$n$次循环后得到的系数矩阵的行列式不一定不等于0，所以我们每次循环的时候，只取满足特定条件的量子态$|z_{i1}z_{i2}\cdots z_{in}\rangle$，即进行第$i$次循环时，对于现有的$i$个量子态进行检测，若量子态向量$[z_{i1},z_{i2},\cdots,z_{in}]$与之前测量得到的$i-1$个向量线性无关，则继续下一步循环；若线性相关，则弃掉测量得到的量子态，重新进行第$i$次循环，直到测量得到$n$个线性无关的量子态后循环结束，求解线性方程组。求出$d_1d_2\cdots d_n$，得到$d_n$，即得到了$s$的最低有效比特位$s_n$。

## 4 算法性能分析

本文从成功概率、时间复杂度、空间复杂度、量子概率克隆4个方面来分析量子算法的性能。

成功概率：因总可以找到$n$个线性无关的向量，所以总成功概率等于1。测量得到的第$i$个量子态向量与之前$i-1$个量子态向量线性无关的概率$P_i=1-\frac{2^{i-1}}{2^n}\geqslant\frac{1}{2}$。

证明：设进行第$i$次循环时，前$i-1$个向量已线性无关。若测量后得到的向量是零向量，则$i$个向量不是线性无关的概率为1。若测量得到的结果不是零向量，则假设第$i$次测量得到的向量与前$i-1$个向量线性相关，即第$i$个向量由前$i-1$个向量线性表出，即$\alpha_i=k_1\alpha_1+k_2\alpha_2+\cdots k_{i-1}\alpha_{i-1}$，其中$k_j=0,1,j=1,2,\cdots i-1$。所以满足线性表出条件的向量共有$2^{i-1}-1$个，所以测量得到的向量由前$i-1$个向量线性表出的概率是$\frac{2^{i-1}-1}{2^n}$。所以进行第$i$次循环后，得到的$i$个向量线性无关的概率是$P_i=1-\frac{1}{2^n}-\frac{2^{i-1}-1}{2^n}=1-\frac{2^{i-1}}{2^n}$，当$i=n$时，$P_n=1-\frac{2^{n-1}}{2^n}=\frac{1}{2}$。证毕。

时间复杂度：求反射斜率$s$的最低有效比特位需要循环$O(n)$次，每次循环的运算次数是$O(n)$，因此求反射斜率$s$的最低有效比特位需要$O(n^2)$次运算，求反射斜率是$s$需要迭代$n$次，所以总运算次数是$O(n^3)$。

空间复杂度：显然整个量子算法只需$O(n)$个量子寄存器即可进行运算，因此空间复杂度为$O(n)$，而求解线性方程组时需要存储$O(n^2)$个数据。

概率量子克隆：设对一组线性无关的量子态$S=\{|\varphi\rangle,|\psi\rangle\}$进行量子克隆的变换为$U(|\varphi\rangle|0\rangle|m_p\rangle)=\sqrt{\eta_0}|\varphi\rangle|\varphi\rangle|m_0\rangle+\sqrt{1-\eta_0}|\theta_{ABP}^0\rangle$，$U(|\psi\rangle|0\rangle|m_p\rangle)=\sqrt{\eta_1}|\psi\rangle|\psi\rangle|m_1\rangle+\sqrt{1-\eta_1}|\theta_{ABP}^1\rangle$，其中$|m_p\rangle,|m_0\rangle,|m_1\rangle$为辅助态，且$|\theta_{ABP}^0\rangle,|\theta_{ABP}^1\rangle$与$|m_p\rangle,|m_0\rangle,|m_1\rangle$正交。对第三个量子态进行测量后得到的结果是$|m_0\rangle$或$|m_1\rangle$时，可知正确地复制了第一个量子态，且测量结果是$|m_0\rangle$或$|m_1\rangle$的概率各为$\eta_0$和$\eta_1$。若$\eta_0=\eta_1$，则$\eta_0=\eta_1\leqslant\frac{1}{1+\langle\varphi|\psi\rangle}$。

推广到一组$N$个线性无关的量子态$S=\{|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_N\rangle\}$，则克隆变换为$U(|\varphi_i\rangle|0\rangle|P_0\rangle)=\sqrt{\eta_i}|\varphi_i\rangle|\varphi_i\rangle|P_0\rangle+\sum_{j=1}^{N}c_{ij}|\theta_{AB}^j\rangle|P_j\rangle$，其中$|P_0\rangle,|P_1\rangle,\cdots,|P_N\rangle$是相互正交的辅助态。对第三个量子态进行测量后，若得到的量子态为$|P_0\rangle$，可知正确地复制了第一个量子态，且正确地克隆的概率为$\eta_i$。

**结束语** 本文通过改进 Kuperberg 的二面体群隐含子群的量子算法，提出了基于量子克隆的二面体群隐含子群的多项式量子算法。通过概率量子克隆，在得到足够多的量子态的前提下，以高概率得到满足条件的量子态，通过线性方程组求出反射斜率$s$的最低有效比特位，最后可求出$s$的每一位比特位。

二面体群隐含子群问题的多项式时间量子算法的提出将撼动基于 poly(n)-uniqueSVP 的格的抗量子密码体制的基石，更对非 Abel 隐含子群问题量子算法的研究和其他问题的

（下转第218页）

些接口内由用户实现的方法不会带来太大的开销，那么这种执行管理机制是非常高效的。

为了测试所提出的非功能属性管理机制在实际应用程序上的作用，使用一个 XMD[13] 分子动力学程序作为被测对象，分别使用原始的 CCA 并行构件制作工具和提出的扩展体系结构实现了一个辐照损伤程序，测试时变换了粒子数和迭代次数作为不同的输入数据。这个程序包括 4 个功能构件，一个驱动构件调用一个读入命令构件读入输入数据，发送给一个临近表构件和一个集成构件。临近表构件生成临近表并进行作用力的计算，集成构件分发粒子到不同的域。临近表构件有 1 个性能接口、1 个资源需求接口和 1 个部署接口共 3 个非功能接口。这个构件属于计算密集型构件，本测试定义它需要一个频率大于 2.5GHz 的 CPU 来执行计算。非功能构件之一的资源需求构件得到这个资源需求并发送给部署构件，部署构件根据性能预测的结果生成最佳部署策略并执行。使用一个用原始的 CCA 并行构件制作工具制作的具有同样分子动力学模拟功能的构件程序作为对照。测试结果如图 15 所示。从图中可以看出，提出的非功能属性管理机制在实际应用程序上起到了提高程序性能的作用。

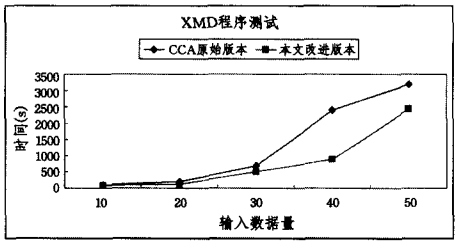


图 15 XMD 程序测试

**结束语** 本文对 CCA 并行构件体系结构进行扩展，提出了一种对于并行构件的 9 种非功能属性进行统一管理的机制，将这种管理机制中被功能构件所共享的部分实现为 9 个非功能构件；还定义了特定于某个功能构件的管理部分，这部分被实现为 9 个可选的非功能接口；实验部分给出了一些实现这些管理功能的具体的并行构件程序的例子。实验表明，提出的管理机制提高了并行构件的性能，同时对并行构件的执行管理也非常有效，且不会带来过多的开销。

## 参 考 文 献


[1] 唐龙业，王宇，王志坚. 面向服务的构件规约[J]. 计算机科学，2013，40(2)：180-185

[2] 张振领，贾仰理，谢圣献，等. 基于协议的实时构件行为一致性验证[J]. 计算机科学，2012，39(6)：125-128

[3] 周静静，盛鑫芽. CCA 环境下构件化线性解法器的设计[J]. 计算机科学，2011，38(5)：127-128

[4] Abernethy R，Morin R，Chahin J. COM/Dcom Unleashed[M]. IN，USA：Sams Indianapolis，1999

[5] Vinoski S. CORBA：integrating diverse applications within distributed heterogeneous environments [J]. Communications Magazine，IEEE，1997，35(2)：46-55

[6] Burke B，Monson-Haefel R. Enterprise JavaBeans 3.0[M]. CA，USA：O'Reilly Media，Inc，2006

[7] Bernholdt D E，Allan B A，Armstrong R，et al. A Component Architecture for High-Performance Scientific Computing [J]. International Journal of High Performance Computing Applications，2006，20(8)：163-202

[8] Kohn S R，Kumfert G，Painter J F，et al. Divorcing language dependencies from a scientific software library[C]// Proceedings of the Tenth SIAM Conference on Parallel Processing for Scientific Computing，2001. Philadelphia，PA，USA：SIAM Press，2001：10

[9] Mahéo Y，Guidec F，Courtrai L. Middleware support for the deployment of resource-aware parallel Java components on heterogeneous distributed platforms[C]// Proceedings of the 30th EUROMICRO Conference，2004. Washington，DC，USA：IEEE Computer Society，2004：144-151

[10] Furmento N，Mayer A，McGough S，et al. A Component Framework for HPC Applications[C]// Proceedings of the 7th International Euro-Par Conference Manchester on Parallel Processing，2001. London，UK：Springer-Verlag，2001：540-548

[11] Zhao Lei，Jarvis S A，Spooner Daniel P，et al. Predictive Performance Modelling of Parallel Component Compositions[J]. Cluster Computing，2007，10(2)：155-166

[12] Malony A，Shende S，Trebon N，et al. Performance Technology for Parallel and Distributed Component Software[J]. Concurrency and Computation：Practice and Experience，2005，17(3)：117-141

[13] XMD-Molecular Dymamics for Metals and Ceramics. Sourceforge[EB/OL]. http://xmd.sourceforge.net/，2013-03-01


(上接第 185 页)

量子多项式时间算法的探索具有重要的意义。

## 参 考 文 献


[1] Shor P. Algorithms for Quantum Computation：Discrete Log and Factoring [C]// Proceedings of the 35th Symposium on Foundations of Computer Science. 1994：124-134

[2] Ettinger M，Hoyer P，Knill E. Hidden subgroup states are almost orthogonal [J/OL]. arXiv：quant-ph/9901034，1999

[3] Murphy J. Analysing the Quantum Fourier Transform for finite groups through the Hidden Subgroup Problem [D]. Montreal：McGill University，2001

[4] Kuperberg G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem [J/OL]. arXiv：quant-ph/0302112

[5] Regev O. Quantum computation and lattice problems [C]// Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science. 2002：520-529

[6] Regev O. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space [J/OL]. arXiv：quant-ph/0406151

[7] Childs A M，Jao D，Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time [J/OL]. arXiv：1012：4019

[8] Kuperberg G. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem [J/OL]. arXiv：1112.3333

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

[10] Barnum H，Caves C M，Fuchs C A，et al. Non-commuting mixed states cannot be broadcast[J]. Phys. Rev. Lett，1996，76：2818-2821

[11] Duan L M，Guo G C. Probabilistic cloning and identification of linearly independent quantum states [J]. Phys. Rev. Lett，1998，80(22)：4999-5002

[12] Pati A K. Quantum superposition of multiple clones and the novel cloning machine [J]. Phys. Rev. Lett，1999(83)：2849-2852