量子计算复杂性理论综述

张焕国[1] 毛少武[1] 吴万青[2] 吴朔媚[3] 刘金会[1] 王后珍[1] 贾建卫[1]

[1](武汉大学计算机学院空天信息安全与可信计算教育部重点实验室 武汉 430072)

[2](河北大学计算机科学与技术学院 河北 保定 017002)

[3](石家庄学院计算机系 石家庄 050035)

摘 要 量子计算复杂性理论是量子计算机科学的基础理论之一,对量子环境下的算法设计和问题求解具有指导意义.因此,该文对量子计算复杂性理论进行了综述.首先,介绍了各种量子图灵机模型及它们之间的关系.其次,量子计算复杂性是指在量子环境下对于某个问题求解的困难程度,包含问题复杂性、算法复杂性等.于是,该文介绍了量子问题复杂性、量子线路复杂性、量子算法复杂性,并且介绍了量子基本运算和 Shor 算法的优化实现.第三,格被看做是一种具有周期性结构的 n 维点空间集合.格密码有很多优势,包括具有抗量子计算的潜力,格算法具有简单易实现、高效性、可并行性特点,格密码已经被证明在最坏条件下和平均条件下具有同等的安全性.因此该文介绍了格的困难问题,以及主要的格密码方案现状.最后,对今后值得研究的一些重要问题和量子计算环境下的密码设计与分析给出了展望.

关键词 量子计算;量子图灵机;量子计算复杂性;量子线路;量子环境下的密码

中图法分类号 TP301 **DOI 号** 10.11897/SP.J.1016.2016.02403

Overview of Quantum Computation Complexity Theory

ZHANG Huan-Guo[1] MAO Shao-Wu[1] WU Wan-Qing[2] WU Suo-Mei[3]

LIU Jin-Hui[1] WANG Hou-Zhen[1] JIA Jian-Wei[1]

[1](*Key Laboratory of Space Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan* 430072)

[2](*School of Computer Science and Technology, Hebei University, Baoding, Hebei* 071002)

[3](*Computer Department, Shijiazhuang University, Shijiazhuang* 050035)

Abstract The quantum computation complexity theory is one of the basic theories of quantum computer science, and it has guiding significance for the designing and solving some problems under the environment of quantum algorithms. Therefore, in this paper, the quantum computation complexity theory is reviewed. Firstly, this paper introduce the relationships between quantum Turing machine model and classical Turing model. Secondly, due to the quantum computational complexity is the degree of difficulty under the quantum environment for problem solving, including the complexity of the problem, the complexity of the algorithm and so on, this paper describes the quantum complexity of the problem, quantum circuit complexity, the complexity of quantum algorithms, and introduces the basic optimization for quantum computation and Shor algorithm. Thirdly, the lattice has n-dimensional periodic structure in space. Lattice based cryptography has many advantages, including post-quantum computation potential, lattice algorithm is simple, efficient, parallel and easy to implement, lattice cryptography has been shown to have

收稿日期:2015-09-26;在线出版日期:2016-03-30.本课题得到国家自然科学基金(61303212,61202386)、国家自然科学基金重点项目(61332019)和国家"九七三"重点基础研究发展规划项目基金(2014CB340600)资助.**张焕国**,男,1945 年生,教授,主要研究领域为信息安全、密码学、可信计算等.E-mail:liss@whu.edu.cn.**毛少武**,男,1986 年生,博士研究生,主要研究方向为信息安全、密码学.**吴万青**,男,1981 年生,博士研究生,主要研究方向为信息安全、量子密码.**吴朔媚**,女,1977 年生,讲师,主要研究方向为计算机密码.**刘金会**,女,1989 年生,博士研究生,主要研究方向为信息安全、密码学.**王后珍**,男,1981 年生,讲师,主要研究方向为信息安全、密码学.**贾建卫**,男,1988 年生,博士研究生,主要研究方向为信息安全、密码学.

equal safety under the worst conditions and average conditions. This paper describes some difficult problems about lattice, and the status of the main lattice cryptography scheme. Finally, the prospect about the cipher design and analysis of some important issues worthy of study and quantum computing environments is given.

Keywords quantum computation; quantum turing machine; quantum computation complexity; quantum circuit; cryptosystem under quantum environment

1 引 言

目前随着量子和生物等新型信息科学的建立和发展,涌现出许多新的研究领域.量子信息科学的研究和发展催生了量子计算机、量子通信和量子密码.它们的出现为量子信息理论研究和技术发展拓宽了范围.促使了一些新的量子理论和量子算法出现.例如,Deutsch 等人[1]首次给出了量子计算的模型,指出量子计算在计算方面优于电子计算.Simon[2]给出了称为 Simon 算法的例子.Grover[3]给出了一种标准搜索算法,复杂度是 $O(\sqrt{n})$.随后 Shor[4]给出了分解大整数问题和求解离散对数问题的有效量子算法.Mosca 等人[5]将 Shor 算法扩展到交换群,提出了隐藏子群问题(HSP).Hallgren 等人[6]指出存在有效的量子算法找到非交换群的正规子群等.

这些已知的量子算法大体上可以分为 3 类:第 1 类是基于量子 Fourier 变换的量子算法.该算法实际将求周期函数的周期问题归结为隐藏子群问题.例如,Shor 的因子分解算法和离散对数算法,这两个算法是对经典算法的指数加速;第 2 类是量子数据库搜索算法.例如,Grover 的量子搜索算法及其推广算法.该算法的计算复杂性是经典算法的开方加速,目前已经发展成为量子搜索算法体系;第 3 类是量子仿真算法,即量子模拟系统[7-10].

这些量子算法的出现对经典公钥密码产生了严重的威胁,主要表现在:(1)Grover 算法的作用相当于把密钥的长度减少一半,这对所有的密码都是一个威胁;(2)Shor 算法对基于大整数分解和离散对数问题的公钥密码产生了严重的威胁,譬如 RSA、ECC、ElGamal 密码等.Proos 和 Zalka[11]指出在 k 量子位的量子计算机上可以容易地求解 k 比特的椭圆曲线离散对数问题,其中 $N=5k+8\sqrt{k}+5\log_2^k$.对于整数因子分解问题,Beauregard 指出在 k 位量子计算机上可以容易地分解 k 比特的整数,其中 $N=2k$.据此分析,利用 1448 量子位量子计算机可以求解 256 位椭圆曲线离散对数问题.因此也就可破译 256 位椭圆曲线密码.利用 2048 量子位量子计算机就可以分解 1024 位的大合数.因此就可以破译 1024 位的 RSA 密码[12-13];(3)HSP 算法的出现对基于交换群的密码产生了本质的威胁.因此,凡是可归结到 AHSP 上的公钥密码都不能抵抗量子计算的攻击.可见量子算法的出现为密码分析提供了新的理论和工具.

除了在理论分析上取得了许多成果外,在量子计算机的物理实现上已经取得一些重要的成果.在国际上,2011 年 5 月 Nature 撰文指出加拿大 D-Wave 公司推出世界上首台 128 量子位商用量子计算机 D-Wave One 系统.著名军火商洛克希德马丁公司以 1000 万美元/台购买了 D-Wave One 用于 F35 战机分析,新武器开发和航天航空器系统测试等.2013 年初,加拿大 D-Wave 公司又推出 512 量子位的 D-Wave Two.谷歌公司以 1500 万美元/台购买了 D-Wave Two 用于加速信息搜索的速度和人工智能.但是加拿大 D-Wave 公司推出的 D-Wave 系列量子计算机是专用型的量子计算机,不是通用型的,只能处理某些特定的问题.2001 年 IBM 公司率先研制成功了 7qbit 的示例性通用量子计算机.证明了量子计算机原理的正确性和可行性.2011 年 9 月,Nature 撰文指出 UCSB 团队通过量子电路成功实现了冯诺依曼结构的 9 个量子位的量子计算机.2012 年 IBM 在美国物理年会上公布声称找到了可以大规模提升量子计算机规模的一种关键技术.2013 年美国 MIT 报告指出微软公司早在十年前就与加州大学圣巴巴拉分校合作开始研究量子计算机.2014 年 4 月,科学家获得 110 量子位的纠缠态远高于以前的 11 量子位.2014 年 9 月 3 日谷歌公司宣布投资 50 亿美元与 UCSB 的研究团队联合研制量子计算机.

综上所述,虽然量子计算机离大规模使用还有很长的距离.但是,一旦大规模的量子计算机成为现实,现有的许多公钥密码将不再安全.量子计算时代我们使用什么密码,是摆在我国面前的一个十分紧迫的重大战略问题!这样就迫切需要研究能抵

御量子计算的新型密码.抗量子计算的密码主要包括以下几类[12]：(1)基于量子物理的量子密码[14-19]；(2)基于生物学的 DNA 密码[20-22]；(3)基于量子计算不擅长计算的数学问题构建的密码[23-26].量子计算复杂性理论是量子密码体制安全性的理论基础，也是构造现代量子密码体制的理论依据.它给出求解一个问题是容易还是困难的依据，并由此对问题和算法的复杂性进行分类，进而根据困难问题设计量子计算环境下的安全密码.

由于量子计算机具有并行性[27]，所以它在许多方面具有比电子计算机更强大的计算能力[28].这使得现在广泛应用的许多密码在量子计算环境下将不再安全[4,11,29-30].量子计算复杂性理论是量子计算机科学的基础理论之一[31]，对量子环境下的算法设计和问题求解具有指导意义.因此，量子计算复杂性理论成为量子环境下密码安全的理论基础.本文对量子计算复杂性理论进行了综述.介绍了各种量子图灵机模型及它们之间的关系，并进行了量子线路模型与量子图灵机的比较.详细讨论了量子计算复杂性，包括量子算法复杂性，问题复杂性和量子线路复杂性.特别提出了一种新的量子计算数据复杂性.最后，对今后值得研究的一些重要问题和量子计算环境下的密码设计与分析给出了展望.

2　经典复杂性理论

在介绍量子复杂性之前，先简单地回顾一下经典的复杂性.算法复杂性理论研究基于算法求解问题所要花费的资源消耗，包括时间、空间资源(比特数、带数、逻辑门数)等的消耗[32].通过考察求解某个问题的不同算法复杂程度来衡量问题的难易程度.由此将问题划分为不同的类型，并对各种算法按其有效性进行分类.在表 1 中总结了常见的经典复杂性问题分类.在图 1 中给出了部分复杂性关系的一个简图.

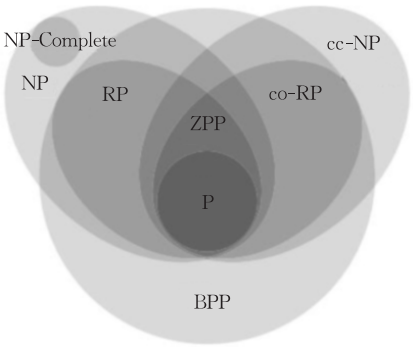

图 1　各种经典算法复杂性关系

表 1　经典复杂性分类

经典复杂性分类	定义
P	确定型单带图灵机在多项式时间内可判定的语言类
NP	某个非确定型多项式时间图灵机判定的语言类
NPC	NP 问题子集，可以通过多项式时间算法归约到一个 NP 问题上
PP	多项式时间的概率图灵机以严格大于 1/2 的概率接收的语言
ZPP	非确定型图灵机在平均多项式时间内接收的语言
PL	概率图灵机在多项式时间和对数空间以严格大于 1/2 的概率接收的语言
BPP	多项式时间的概率图灵机以错误概率 1/3 接收的语言类
RP	多项式时间非确定性图灵机以大于 $\varepsilon>0$ 的概率接收的语言类
EXP	存在指数时间的确定性图灵机接收的语言类
NEXP	存在指数时间的非确定性图灵机接收的语言类

算法是指可用来求解某一问题的过程.称一个算法求解一个问题，是指该算法可应用到问题的任一例子，并保证总能找到该例子的一个解.一个算法的有效性可以用执行该算法时所需的各种计算资源的量来度量.最典型、也是最主要的资源是所需的运行时间和内存空间.在复杂性研究中，衡量一个算法的效果，最广泛采用的标准是求解问题所花费的时间，称为时间复杂性.计算复杂性常用的符号 $O()$，$o()$，$\Omega()$，$\omega()$，$\Theta()$.利用这些记号可以将函数划分为不同的类.在复杂性理论中，对如此定义的同一类型的不同函数往往不加以区分.

3　量子图灵机模型

量子复杂性理论考虑的是在量子计算环境下评估解决某个问题的资源消耗情况.而这些资源的评估都是基于某个模型的.这样的模型有量子图灵机模型、量子线路模型[33]、量子查询模型[34]、量子通信协议模型[35]等.本节主要介绍了量子图灵机模型.利用量子图灵机模型，可以解释量子计算机求解的问题分类.量子图灵机的讨论类似于经典的概率图灵机(PTM).因此下面我们介绍一些量子图灵机的模型及它们之间的关系.

最早，Feynman[36]指出经典图灵机不能有效模拟量子力学过程，需要发展量子计算模型来模拟量子体系的演化.Deutsch[37]阐述量子图灵机概念，并提出了量子计算复杂性理论.基于此，Bernstein 和 Vazirani[38]在数学上首次对量子计算模型给予严格的形式化描述.

量子图灵机模型(QTM).设有限状态集 Q，而

$q_0, q_Y, q_N \in Q$ 分别是初始状态，接受状态和拒绝状态. 设带中所有字符的一个有限集合 Γ，它包含输入字符表子集 Σ. 用 Σ^* 表示 Σ 中的字符所组成的所有有限长字符串的集合，空白字符 $b \in (\Gamma - \Sigma)$. δ 是量子状态转移函数，满足

$$\delta: Q \times \Gamma \times \Gamma \times Q \times \{\leftarrow, \rightarrow\} \rightarrow C \tag{1}$$

其中 $\delta(q_1, a_1, a_2, q_2, d)$ 是格局. QTM 在状态 q_1 读取字符 a_1，沿方向 d，进入状态 q_2 将读取字符 a_2. 转移函数指定了无限维空间的格局叠加态的线性映射 M_δ（时间演化算子）.

随后，文献[39-40]对该模型进行了微调，增加了一个静止的读写头. 设量子图灵机（QTM）是一个七元组 $(Q, \Sigma, \Gamma, \delta, q_0, q_Y, q_N)$. 量子状态转移函数 δ 满足

$$\delta: Q \times \Gamma \times Q \times \Gamma \times \{\leftarrow, o, \rightarrow\} \rightarrow \bar{C} \tag{2}$$

其中 $\Sigma_{(q_2, a_2, d) \in Q \times \Gamma \times \{-1,0,1\}} \| \delta(q_1, a_1, q_2, a_2, d) \|^2 = 1$，$\bar{C}$ 应为复数集的子集，其实部与虚部是多项式时间可计算的. 存在确定性多项式时间函数 $f(n)$ 的算法精确计算复数 α 的实部和虚部，满足 $\| f(n) - \alpha \| < 2^{-n}$. $\leftarrow, \rightarrow$ 分别表示读写头移动方向. o 代表读写头不移动.

它的工作原理如下：设 S 是 QTM 的格局且 S 是有限线性组合上的满足欧几里德归一化条件的复内积空间，称 S 中的每个元素为 M 的一个叠加. 量子有限状态转移函数 δ 诱导一个时间演化算子 U_M: $S \rightarrow S$. M 以格局 c 起始，当前状态为 p，且扫描标识符 σ，下一动作 M 将会被置为格局叠加：$\psi = \sum_i \alpha_i c_i$. 其中每个非零的 α_i 都与一个量子转移函数 $\delta(q_1, a_1, q_2, a_2, d)$ 对应，c_i 是向 c 施行转化得到的新的格局. 通过线性时间演化算子 U_M 可以将这种操作扩展到整个 S 空间[41].

广义量子图灵机（GQTM）. Ohya 等人[42]在 2003 年提出了广义图灵机的概念，定义如下：设四元组 $M = (Q, \Sigma, H, \Lambda_\delta)$，其中字母表 Q 是处理器格局，Σ 是包含空字符串的字母表，H 是希尔伯特空间，Λ_δ 是量子态的转移函数. 设 $\Re(H)$ 是希尔伯特空间 H 密度算子的集合. 量子态的转移函数 $\Lambda_\delta: \Re(H) \rightarrow \Re(H)$ 的工作原理如下：给定格局 $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$，其中 $\sum_k \lambda_k = 1, \lambda_k \geq 0$ 且 $\psi_k = |q_k\rangle \otimes |A_k\rangle \otimes |i_k\rangle (q_k \in Q, A_k \in \Sigma^*, i_k \in Z)$，是希尔伯特空间 H 的一组基. 所以这个转移函数是 $\rho' = \Lambda_\delta(\rho) = \sum_k \mu_k |\psi_k\rangle\langle\psi_k|$ 且 $\sum \mu_k = 1, \mu_k \geq 0$. 需要注意的是，如果 Λ_δ 是一个幺正算子 U 那么 GQTM $M = (Q, \Sigma, H, \Lambda_\delta)$ 可以规约到 QTM[43].

随机预言量子图灵机（ROQTM）. 在 1996 年 Bennett 等人[41]提出了随机预言量子图灵机. ROQTM 有一个特殊的查询纸带，除了非空白的单元外纸带的所有单元都是空白. 同时含有两个不同的内部状态矢量：先验查询状态 q_q 和后验查询状态 q_a. 无论机器何时进行查询先验状态 q_q 都开始查询. 若查询串是空的，则不操作且机器直接转到后验查询状态 q_a. 若查询串非空，查询串可写为 $x \| b$，其中 $x \in \Sigma^*$，$b \in \Sigma$，$\|$ 表示串联，$\Sigma = \{0, 1\}$. 这种情况下，调用谕示 $A(x)$ 的结果将内部状态转到后验查询状态 q_a，然后查询纸带内容从 $|x \| b\rangle$ 变化到 $|x \| b \oplus A(x)\rangle$. 除了查询纸带和内部控制外其他部分不发生变化. 容易发现，若给定初始值 $b = 0$，即 $|b\rangle = 0$，则最终态为 $A(x)$. 与经典的随机预言计算机一样，若给定初始 $b = A(x)$，则最终查询态为 $|0\rangle$. 这表明调用谕示 $A(x)$ 将重置靶比特为 $|0\rangle$.

它的工作原理如下：当调用随机预言量子图灵机时，将酉变换 U 作用在查询纸带目录 $|z\rangle$ 上记作 $U|z\rangle$. U 定义在可数无限维希尔伯特空间上，由二进制串 $|\varepsilon\rangle, |0\rangle, |1\rangle, |00\rangle, |01\rangle, |10\rangle, |11\rangle, |000\rangle, \cdots$，组成. 其中 $|\varepsilon\rangle$ 表示空串. 对于谕示图灵机，一般的酉随机预言服从酉演化. 随机预言将输入映射到叠加态输出，不需要保长. 在 $U|z\rangle$ 中只有有限个基向量的振幅为 0. 同时 $U^2 = 1$，调用一个随机预言的结果可以通过进一步调用相同的随机预言进行复原. 另外，允许适当的干扰发生.

下面举了一个例子加以说明. 设图灵机的所有字符 $\Gamma = \{0, 1, b\}$，b 是空白符号，输入字符表子集 $\Sigma = \{0, 1\}$. 随机预言是一个酉运算 O，作用于计算机上定义为

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle \tag{3}$$

其中 $|x\rangle$ 是指标寄存器，$\oplus$ 是模 2 加法，随机预言的量子比特 $|q\rangle$，$q \in \Gamma$ 是单量子比特. 当 $f(x) = 1$，则翻转；否则不变. 通过制备 $|x\rangle|0\rangle$，应用随机预言，检查随机预言量子比特是否翻转到 $|1\rangle$，来判断 x 是否为搜索问题的一个解.

我们注意到有一些量子算法是带有随机预言模型的“Oracle”，譬如 Deutsch-Jozsa 算法[1]、Grover 搜索算法[3]、Shor 算法[4]等. 这个量子谕示作为一个黑盒，不考虑输入的具体细节. 在讨论这些问题的计算复杂性时需要构造谕示，并估计构造谕示需要的资源. 如果能构造这样谕示，称问题是可解的. 另外，

并不是所有的量子算法都需要谕示. 在文献[36,44]中 Ohya 等人给出了一些不需要谕示的例子. 因此 ROQTM 被视作带有随机预言模型“Oracle”的量子图灵机.

多带量子图灵机模型(MQTM). Yamakami 在 1999 年提出了多带量子图灵机的概念[45-47],具体如下:k 条带量子图灵机是一个五元组 $M=(Q,q_0,Q_r,\Sigma_1\times\Sigma_2\times\cdots\times\Sigma_k,\delta)$,每个 Σ_i 是带有空白符号 b 的有限字符集,Q 是包含初始状态 q_0 和终止状态 $Q_r=\{q_r^1,q_r^2,\cdots,q_r^k\}$ 的内部状态有限集合,δ 是从 $Q\times\Sigma_1\times\Sigma_2\times\cdots\times\Sigma_k$ 到 $C^{Q\times\Sigma_1\times\cdots\times\Sigma_k}$ 的多值量子转移函数. 令 $\overline{\Sigma}^k=\Sigma_1\times\Sigma_2\times\cdots\times\Sigma_k$. 即 $\delta:\overline{Q\times\Sigma}^k\to C^{Q\times\overline{\Sigma}^k}$. QTM 是由 Z 索引单元格的双向无限纸带,读写头沿着纸带向左,向右或者不移动,分别用 L,R,N 表示.

它的模拟能力有如下的结果. 在文献[45]中介绍了良构引理和完全引理作为刻画特征的依据. 设 M 是 k-带良构的 QTM. 如果输入 x 后 M 在时间 $T(x)$ 内停机,那么存在 $k+2$-带良构的 QTM M' 输入 $(x,1^{T(x)})$ 在时间 $2T(x)+2$ 内停机. 由文献[38]中命题 1 说明在二次多项式时间内可以通过一个单带 QTM 模拟 MQTM,记作 QTM$\leq_p$MQTM. 这与经典情况类似,QTM 与 MQTM 具有多项式等价的计算能力.

到此我们介绍了几种量子图灵机模型及其变形. 综上所述,它们在计算能力上是有联系和区别的. 具体地说,广义量子图灵机(GQTM)的计算能力涵盖了量子图灵机(QTM). 量子图灵机(QTM)的计算能力涵盖了随机预言量子图灵机(ROQTM). 在二次多项式时间内可以通过一个单带的 QTM 模拟 MQTM. 在图 2 中形象化地描述了它们之间的关系.

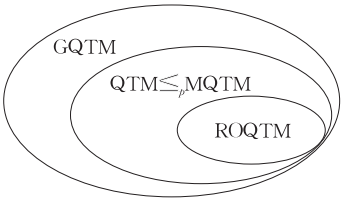

图 2　量子图灵机模型之间的关系

量子图灵机类似于经典计算下的概率图灵机,但是与经典图灵机(包括概率图灵机)并不相同. 一方面,量子图灵机可以看做是由量子读写头和一条无限长的带作为量子存储器组成的. “带”上的每个单元格均表示一个量子记数位,可以以“0”和“1”的叠加态形式存在,这样可以在带上同时对编码问题的许多输入进行计算,计算结果是所有输入对应结果的叠加,通过测量得到经典结果. 另一方面,它们之间的区别是状态转移函数的变化[45-46]. 量子图灵机含有复量子状态转移函数,进行 T 步计算只需要精度为 $O(\log T)$ 位的转移幅度就足够了[45]. 由于量子图灵机的运算结果不再按概率叠加,而是按概率振幅叠加,量子相干性在量子图灵机中起着本质性作用. 这是实现量子并行计算的关键,这个性质也是量子图灵机和概率图灵机的重要差异.

Feynman[36]证明了 QTM 可以有效地模拟经典的可逆图灵机,这意味着量子计算至少与经典计算有相同的计算能力. Deutsch[37]将这个结果形式化.

4　量子计算复杂性概论

一个问题的量子计算复杂性是由求解这个问题的量子算法的计算复杂性所决定. 量子计算复杂性是指在量子环境下对于某个问题求解的困难程度,包含问题复杂性、算法复杂性等. 由于求解一个问题的量子算法可能有多个,它们的量子计算复杂性也各不相同. 因此在理论上定义一个问题的量子计算复杂性为求解该问题的最有效量子算法的计算复杂性. 目前,研究的问题主要有两种:一是可行性检验问题,二是判定问题.

在经典的计算复杂性理论中,人们已经证明存在多项式时间通用图灵机求解可计算问题. 类似地,Bernstein 和 Vazirani[48]指出存在多项式时间通用量子图灵机求解可计算问题. 同时,他们提出了量子计算复杂性理论. 随后,许多学者提出了各种量子算法和量子复杂性证明作为量子计算复杂性的进一步解释. 譬如,Simon 定理说明量子计算优于经典计算,即存在具有有界错误概率的量子谕示图灵机求解问题的复杂性低于经典计算的复杂性[2]. Shor 算法和 Gover 算法分别验证了 Simon 定理的正确性[3-4].

但是对于任意(或趋近)无穷多的输入,量子图灵机(包含任意的概率图灵机)以有界错误概率求解问题需要(亚)指数时间复杂度[3]. 一方面,量子图灵机的出现降低了求解问题的计算复杂性;另一方面,不是所有的问题都在 BPP 内.

4.1　量子问题复杂性分类

由于量子计算机可以看做是经典计算机在量子环境下的推广. 于是,问题的经典复杂性 P、NP、ZPP、BPP 等可类似地推广到量子计算中,即有 QP、ZQP、BQP、NQP 等.

4.1.1 量子模拟 P 类问题

我们给出称之为 QP 问题的重要语言,具体定义如下[42]:QP=$\{L$:存在一个多项式时间 QTM M 使得 $L=L_M\}$,其中 $L_M=\{x\in\Sigma^*:M$ 接受 $x\}$. 若存在多项式时间 QTM M,它在编码策略 e 之下能够求解问题 Π,则判定问题 $\Pi\in$ QP,即 $L[\Pi,e]\in$ QP. 它被看作 P 类问题在量子环境下的模拟.

另外,EQP 类问题是指 QTM 以精确或者无错误的量子多项式时间接收的语言类,即 EQP⊂QP. 相应地,它的时间复杂性 EQPTime($T(n)$)是指由输入长度为 n,运行时间为 $T(n)$精确界定的 QTM 接收的语言类. ZQP 类问题是指 QTM 以至少 1/2 的概率在多项式时间内接收的语言类,即 ZQP⊂QP. BQP 类问题是指 QTM 在多项式时间内以 1/3 的概率接收的语言类. 它的时间复杂性 BQPTime($T(n)$)是指输入长度为 n,运行时间为 $T(n)$界定的 QTM 以概率 2/3 接收的语言类[49]. 它的计算能力有结果 BQP⊆PP[50].

4.1.2 量子模拟 NP 类问题

NP 问题在量子环境下有两种不同的模拟定义:一种类似于用 NDTM 定义 NP 问题的定义方式,即 NQP 是指由多项式时间的 NQTM 识别的语言类[51];另一种是多项式时间验证 NP 语言类的扩展,即 QMA[52]. 在经典计算理论中,这两种问题类的定义方式是等价的. 然而,在量子计算理论中这两个定义并不等价,文献[53]给出 NQP 和 QMA 两者满足的关系:NQP=$\bigcup_{\delta;Z^+\to(0,1]}QMA(1,c,0)$. 如果存在一个多项式时间的量子验证者 V,对于任意的输入 x,满足(1)$x\in A_{\text{yes}}$,存在 $k(|x|)$量子证明使得 V 至少以 $c(|x|)$的概率接受 x,(2)$x\in A_{\text{no}}$,对任意给定的 $k(|x|)$量子证明,使得 V 至多以 $s(|x|)$的概率接受 x. 问题 $A=(A_{\text{yes}},A_{\text{no}})$的复杂性记作 QMA$(k,c,s)$. 在 Milner 等人①的文章中说明了对于任意的多项式限制函数 $k\geq2$,任意 c 使得 QMA$(k,c,0)$=QMA$(1,c,0)$.

QMA 的定义如下:设问题 $A=(A_{\text{yes}},A_{\text{no}})$,$p$ 是一个多项式限制函数,函数 $a,b:N\to[0,1]$. 那么 $A\in\text{QMA}_p(a,b)$当且仅当存在一个多项式时间的线路族 $Q=\{Q_n:n\in N\}$,其中每一个 Q_n 有 $n+p(n)$ 个比特的输入和一个比特的输出,满足下面的性质:(1)完整性. 对于所有的 $x\in A_{\text{yes}}$,存在 $p(|x|)$个量子比特态 ρ 使得 Pr[Q 接受(x,ρ)]$\geq a(|x|)$;(2)可靠性. 对任意的 $x\in A_{\text{no}}$ 和 $p(|x|)$量子比特态 ρ 使得 Pr[Q 接受(x,ρ)]$\leq b(|x|)$.

NQP 问题定义如下:QTM 识别的语言 $L\in$NQP,当且仅当存在 QTM 和一个多项式函数 P 使得 $x\in L\Leftrightarrow$Pr(M 在 $p(|x|)$步内接受 x)$\neq0$. 在文献[54]中指出它的计算能力有如下的结果,NQP⊆PP⊆NQP^{NQP},$\text{NQP}_k=\text{coC}_=\text{P}$,$Q\subseteq k\subseteq C$.

另外在量子环境下可以模拟经典的 NPC 问题. 在文献[54]中介绍了一个特殊的语言分类,即 QAP. 定义如下 QAP=$\{\langle M,x,0^t\rangle|M$ 编码一个量子机器在 t 步内以非零概率接受 $x\}$. 文中指出 QAP 难于确定准确的概率接受问题. 而确定准确的概率接受问题是一个 NPC 问题. 这说明 QAP 的复杂性不低于求解 NPC 问题的复杂性,有 NPC⊂QAP.

除此之外,在文献[55]中给出了另一个量子模拟 NPC 问题的定义,即 QMA-complete 问题,简记为 QMAC. 在文献[56]中证明了量子环境下的团问题是 QMAC 问题. 在文献[53]中讨论了 NPC 问题的另一个量子模拟 NQP-complete 问题. 它不同于 QMAC 问题. 像这样的完全问题还有许多其他的形式,在文献[57]中讨论了更多的完全问题的情况,譬如 BQP-complete,QMA-complete,QMA(2)-complete,QSZK-complete,QIP-complete. 但目前的研究不是很充分,在这里我们不做过多地叙述.

4.1.3 其他类问题

在文献[58]中给出了 NC 的量子模拟 QNC 的定义,并指出 QNC=$\bigcup_k\text{QNC}^k$ 且 QNC⊂BQP. 在文献[59]中介绍了 AWPP 和 LWPP 类问题. AWPP 是 BPP 使用 Gap 函数代替接受概率产生的语言类. 在文献[50]中给出了它们的计算能力分类,即 BQP⊆AWPP⊆PP⊆PSPACE,EQP⊆LWPP. 在文献[60]中证明了 AWPP⊆APP 且 WPP⊆AWPP. 于是结合前面的结论有 BPP⊆BQP⊆AWPP⊆APP⊆PP. 另外,在文献[61]中得到结果 SPP⊆LWPP⊆WPP,其中 WPP 的介绍参见文献[62].

文献[63]介绍了 PostBQP 类问题. PostBQP 是指具有后选择能力的量子计算机在多项式时间内解决的问题,且证明了 PostBQP=PP. 文献[64]考虑了量子模拟 NP 困难问题的计算能力之间的关系,得到如下的结果 BPP⊆BQP⊆QCMA⊆QMA⊆PP,其中 QCMA 是一类特殊的 QMA(后来的文献如文献[49]把它也称作 MQA). 同时还得到了结果 MA⊆QCMA⊆QMA. 在文献[65]中作者研究了

① Milner K, Gutoski G, Hayden P, et al. Quantum interactive proofs and the complexity of entanglement detection. Preprint arXiv, 2013, 1308

WAPP，APP 计算能力的量子解释，给出了如下结果 $\mathrm{PostBPP_{FP}} \subseteq \mathrm{WAPP} \subseteq \mathrm{AWPP} = \mathrm{PostBQP_{aFP}} \subseteq \mathrm{APP}$. 其他的结果参见文献.

文献[66]认为到目前为止大部分的量子算法问题可以规约到量子采样. 现有的许多问题，譬如离散对数问题、图表同构等都属于 SZK 问题. 在文献[66]中指出了这些问题在量子环境下有如下结果 SZK⊆QSZK. 在文献[67]中作者讨论了 PQDP 类问题与 SZK 的关系，指出 SZK⊆PDQP⊆PSPACE，BQP⊆PDQP.

文献[68]介绍了 PQP 类问题. 它是指存在多项式时间的量子线路族 $Q=\{Q_n: n\in N\}$，其中每一个线路 Q_n 有 n 量子比特的输入和一个量子比特的输出，满足下面的性质：(1) 对于所有的 $x\in A_{\mathrm{yes}}$，使得 $\Pr[Q\text{ 接受}(x,\rho)]>1/2$；(2) 对任意的 $x\in A_{\mathrm{no}}$，使得 $\Pr[Q\text{ 接受}(x,\rho)]\leq 1/2$. 它的计算能力有结果 PQP=PP.

文献[68]解释了 QIP 类问题. 具体的定义如下，设 m 是多项式有界函数，$a,b: N\to[0,1]$ 是多项式时间可计算函数. 语言 $L\in \mathrm{QIP}(a,b,m)$ 当且仅当存在 m 个量子消息验证者 V，满足下面性质：(1) 完整性. 对所有的 $x\in L$，存在量子验证者 P 使得 V 以至少 $a(|x|)$ 的概率接受 x；(2) 可靠性. 对所有的 $x\notin L$，对每个量子验证者 P 使得 V 以至多 $b(|x|)$ 的概率接受 x. 对每个有界多项式函数 m，$\mathrm{QIP}(2)=\mathrm{QIP}(m,2/3,1/3)$. 并且定义 $\mathrm{QIP}=\bigcup_m \mathrm{QIP}(m)$. 关于 QIP 类问题的计算能力有如下一些结果. 文献[69]证明了 QIP=PSPACE，比文献[68]中的结果 QIP⊆PSPACE 更精确. 在文献[70]中指出 $\mathrm{QIP}(2)\subseteq$ PSPACE. 在文献[71]中证明了 $\mathrm{QIP}([\log,\mathrm{poly}],a,b)=\mathrm{QMA}$，$\mathrm{QIP_{log}}(a,b)=\mathrm{BQP}$.

于是，在图 3 中刻画了量子模拟的 QP、NQP 问题与经典复杂性之间的关系. 更详细的复杂性讨论结果总结在图 4 中.

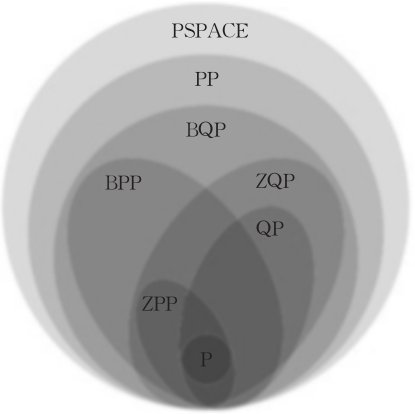

图 3　经典复杂性与量子复杂性之间的关系

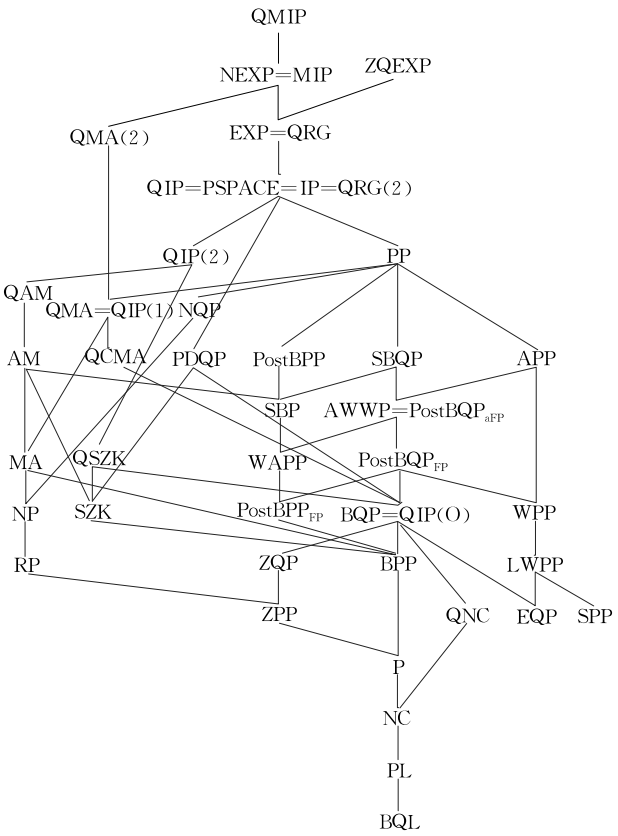

图 4　文中讨论的量子与经典复杂类总结关系

4.2　量子线路复杂性

在电子环境下，布尔电路可用于描述经典图灵机. 在量子计算出现以后，Deutsch[72] 首次提出量子线路模型. 于是布尔电路被推广到量子计算中，量子图灵机也可以采用量子线路进行描述. 随后，Yao[73] 指出量子图灵机模型和量子线路模型是等价的. 在某种情况下，它们多项式时间可以互相模拟，这开启了一个新的量子信息技术研究领域，量子线路复杂性理论.

量子线路是将布尔线路模型中的比特和逻辑门推广到量子线路模型中. 量子线路是多量子位的酉变换，将初始状态集合映射到某个终止状态. 通常的酉门可以分解为一个或者两个量子位的基础门. 线路图代表了一系列酉演化和测量，包含输入状态和输出测量. 线路图每次从左到右运行. 每个水平线代表量子信息向前传播一次. 每条线代表一个量子位的量子信息. 酉门由线上的盒子表示，门的符号写在盒子里[74-77].

量子线路模型是一个很好的量子计算模型. 它为量子算法的构造和量子计算机的物理实现提供了一个框架. 由于量子图灵机的操作是可逆操作，量子图灵机的逆操作变换处理相当于把每一个量子逻辑门用一个需要更多量子比特输入的量子逻辑门代

替.这意味着当量子图灵机对应的量子线路进行逆操作时,所付出的代价只是额外增加了按照线性增长的量子比特数目.量子线路模型通过组合一组基本的量子逻辑门,实现具有特定功能的线路.该模型可以清晰、直观地模拟量子信息处理的过程,对我们设计量子计算装置和新的量子算法都有很好的指导作用.这样的文章有很多,譬如文献[78-83].

量子计算复杂性理论中最重要的两个模型是量子图灵机模型和量子线路模型.在量子计算中,QTM计算过程是复杂的,尤其是表示数据的量子态的转换和控制变量处于基状态的过程是十分重要的.量子线路模型不用考虑这些方面,它更侧重于考虑输入的量子态在幺正运算的操作下得到的结果.它类似于均匀多项式线路,是可逆线路的推广.使用该模型能够更方便地描述量子算法.量子线路模型的主要优点是模型简单,描述问题比较直观,并且有利于理解和设计量子算法.在量子系统中,量子线路模型提供了非常方便的物理演化形式,如量子超密编码[84]、量子隐形传态[85]以及 Deutsch 算法[1]等.

4.3 量子算法复杂性理论

4.3.1 量子算法的时间复杂性

设 $T_M(x)$表示量子图灵机 M 对输入 x 计算得到一个最终格局所用时间,或者称时间复杂性;否则无定义.若 $T_M(x)$存在,且 $T_M(x)=T$,则 M 对输入 x 的计算在时间 T 停机.对所有输入 $x\in\Sigma^*$ 均停机的 QTM M,其时间复杂性函数 $T_M:Z_+\to Z_+:T_M(n)=\max\{t:\exists x\in\Sigma^*,|x|=n$,使得 QTM M 对输入 x 的计算需要的时间为 $t\}$.若存在一个多项式 $g(n)$,使得对所有的 $n\in N_+$,有 $T_M(n)\leq g(n)$.即若存在多项式 $g(n)$,对每个输入 x,QTM M 在时间 $g(f(\omega))$内精确停止,则 M 称为多项式时间 QTM.若函数 $g(n)$是指数形式的,那么 M 称为指数时间 QTM.

图 5 对多项式时间量子算法与指数时间量子算法的复杂度进行比较分析,其中 L^2 是多项式时间量子算法复杂度,另外两个是指数时间量子算法的复杂度.

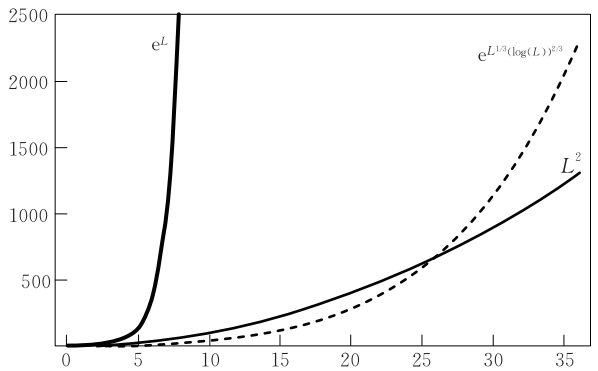

图 5 多项式时间量子算法与指数时间量子算法复杂度比较

关于多项式时间量子算法与指数时间量子算法,给出以下几点注记:

(1)定义的量子时间复杂性是在最坏情形下的度量.求解某一问题的一个量子算法,对于该问题的绝大多数例子是有效的.但是可能对问题的某个极端例子表现极差.从而导致这一量子算法是指数时间量子算法.

(2)关于问题的难解性.一个量子算法本质上并不依赖于特定的编码策略和具体的计算模型.这是因为这些定义划分在多项式变换下可相互规约.而不同的合理编码策略给出同一问题的描述,相应的输入长度(或长度的上界、下界)之间最多相差一个多项式倍数,且从一种编码容易转换到另一种编码.类似地,多项式时间界定的量子计算模型在单一时间单位内所完成的工作量,相对于多项式的复杂性函数是等价的.一般不具体提及特定的编码策略和量子计算模型,只简单地称某一算法是多项式时间量子算法或别的类型的量子算法问题等.

众所周知,经典算法复杂性是基于经典图灵机进行讨论的.类似地,量子算法复杂性是基于量子图灵机进行分类的.由前面所述,量子图灵机的定义有许多,最常使用的是随机预言量子图灵机.现有许多已知的量子算法都属于这个模型,譬如 Deutsch-Jozsa 算法[1]、Grover 搜索算法[3]、Shor 算法[4]等.谕示"Oracle"可以作为一个黑盒,使用者不必考虑它的细节.在考虑某个算法的量子复杂性时,必须考虑如何去构造这个谕示,且构造谕示需要多少资源(包括量子比特和量子逻辑门).如果可以用构造谕示得到有效的解,则称这个问题在量子环境下是可解的.

但是并不是所有的量子算法都需要使用谕示.有些量子算法就不使用谕示模型,譬如文献[36,39-40,86-87].目前我们只考虑带有谕示的量子图灵机模型.它的计算能力有如下的两个重要的结果.

定理 1[41]. 设 $Q(A)$是运行时间受限于 $T(n)=O(2^{n/2})$的随机谕示量子图灵机.从 $Q(A)$中随机唯一地选取谕示 A 的概率为 1,则基于 $Q(A)$的 BQP 问题中不包含 NP 问题,即 NP$\not\subset$BQP.

定理 2[41]. 设 $Q(B)$是运行时间受限于 $T(n)=O(2^{n/3})$的随机置换谕示量子图灵机.从 $Q(B)$中随机唯一地选取置换谕示 B 的概率为 1,则基于 $Q(B)$的 BQP 问题中不包含 NP$\not\subset$co-NP 问题,即 NP$\cap$

co-NP⊄BQP.

为了更直观地理解量子算法的优越性，在表 2 我们总结了一些困难问题的经典算法复杂性和量子算法复杂性.

表 2　一些困难问题的经典算法复杂性和量子算法复杂性

待解决问题	经典算法复杂度	量子算法复杂度
黑箱问题	$O(2^n)$	$O(1)$
因子分解[4]	$\exp(c(\log n)^{1/3}(\log\log n)^{2/3})$	$O((\log n)^2(\log\log n)(\log\log\log n))$
Simon 问题[2]	下上界分别是 $\Omega(n^{n/4})$，$\Omega(n^{n/2})$	$O(n)$
求阶问题[88]	$\Omega(n^{n/3}/\sqrt{n})$	$O(1)$
求解线性方程组[89]	$2^{n\sqrt{k}}$	$O(n)$
最短向量问题(SVP)[90]	$2^{O(n)}$	$2^{0.312n+o(n)}$
Feistel 结构和随机置换的区分[91]	$O(2^{n/2})$	$O(n)$
搜索问题[3]	$O(N)$	$O(N^{1/2})$
矩阵乘法验证[92]	$O(n^{2.376})$	$O(n^{5/3}\min(\omega,\sqrt{n})^{1/3})$
子集合问题[93]	$O(n2^{n/2})$	$O(n2^{n/3})$
碰撞问题①	$O(\sqrt{2^n/r})$	$O(\sqrt[3]{2^n/r})$

从表 2 中，我们可以看到，某些困难问题的经典算法的复杂性超过量子算法的计算复杂性. 某些 NP 类问题的量子算法可以多项式地规约为 QP 类问题. 基于这些问题所构造的密码在量子环境下，将不再安全. 而某些 NP 类问题的量子算法不能多项式地规约为 QP 类问题，则基于这些问题困难性构造的密码体系仍然不能被量子计算攻破[94]. 另外，由于 P⊆QP，使得在电子环境下不安全的密码在量子环境下一定是不安全的.

4.3.2　量子环境下的数据复杂性

在文献[95]中我们着重讨论了数据复杂性. 计算复杂性理论描述了计算对资源的消耗，如时间和空间资源. 目前的计算复杂性理论主要研究时间复杂性和空间复杂性. 除了时间和空间外，数据也是一种重要的计算资源. 在计算过程中，如果需要的数据量过大而实际上无法获得，那么计算也将不能完成. 数据复杂性的概念最早用于电子计算环境下对 DES 密码的差分攻击. 对于 8 轮以下的 DES 由于需要的选择明文数量较少，在 PC 机上几分钟就可以攻破. 但对于标准的 16 轮 DES 密码却不能攻破，因为需要 2^{47} 个选择明文，这在实际上是很难得到的. 这里影响差分攻击是否成功的重要因素是其数据复杂性.

与经典的情况类似，这里提出的量子环境下的数据复杂度包括输入数据复杂度和处理数据复杂度两方面. 输入数据复杂度是指完成某个量子算法所需输入的数据量. 处理数据复杂度是指运行该量子算法所要处理的数据量. 通常，我们采用其主要部分来描述计算复杂度. 譬如，在 Grover 搜索算法中需要将搜索算符执行 $2^{n/2}$ 次. 这说明 Grover 搜索算法的处理数据复杂度是很大的. 另外，在 Shor 算法中设待分解的合数是 n 位的，则它的输入数据复杂度是 $O(n)$. 又因为它的处理数据复杂性不大. 故 Shor 算法可以有效计算大合数的因子分解问题.

于是在标准量子谕示的意义下，我们给出量子计算情况下的数据复杂性的定义，且给出了基于数据复杂性分类的容易和困难问题定义.

定义 1.　令 QTM 是一个 n 量子比特的量子图灵机. QTM 的数据复杂性是一个函数 $f: N\to N$，其中 $f(n)$ 是 QTM 在运行时输入和处理的所有数据量之和. 令 $n=n_1+n_2$，则 $f(n)=f(n_1)+f(n_2)$，其中 n_1、n_2 分别是储存输入数据的储存器和运算处理数据的储存器的量子比特数，$f(n_1)$、$f(n_2)$ 分别表示输入数据量和处理数据量.

定义 2.　令 QTM 是一个 $n=n_1+n_2$ 量子比特的量子图灵机，其中 n_1，n_2 分别是储存输入数据的储存器和运算处理数据的储存器的量子比特数. 假设量子图灵机的数据输入能力和处理数据能力分别是 $g(n_1)$ 和 $g(n_2)$. 量子图灵机在时间 $T\in R^+$ 内运行解决某类问题的量子算法时，需要的数据总量为 $f(n)=f(n_1)+f(n_2)$，其中输入数据量是 $f_1(n_1)$，处理数据量是 $f_2(n_2)$.

(1) 若存在正整数 n_0 使得对所有的 $n=n_1+n_2>n_0$ 满足 $\lim\limits_{n\to\infty}(f_1(n_1)/g(n_1)+f_2(n_2)/g(n_2))=k$，$k$ 是正常数，则称该问题在量子图灵机环境下是容易计算的；

(2) 若 $\lim\limits_{n\to\infty}(f_1(n_1)/g(n_1)+f_2(n_2)/g(n_2))=\infty$，则称该问题在量子图灵机环境下是计算困难的.

在经典计算中，布尔函数是一种重要的函数. n

① Brassard G, Hoyer P, Tapp A. Quantum algorithm for the collision problem. arXiv preprint quant-ph/9705002, 1997

元布尔函数一共含有 2^{2^n} 种情况. 设 $C_t(f)$ 是计算布尔函数 f 的规模最小的布尔线路 C,且 C 中每个逻辑门的输入不大于 t. 如果 $t=2$,则用 $C(f)=C_2(f)$ 表示. 文献[96]中指出几乎所有的 n 元布尔函数 f 均满足 $C(f)=\Omega(2^n/n)$. 这说明只有少数的布尔函数存在有效的经典算法. 类似地,我们将这一结果推广至量子计算中.

布尔运算包括逻辑非、逻辑和与逻辑积. 在布尔线路中,所有的逻辑非门变换到最底层,作为一个输入变量. 因此,布尔线路中仅含有逻辑和和逻辑积运算. 通过适当地增加用于储存逻辑运算结果和表示逻辑非的量子比特数,量子线路能够成功地模拟布尔线路[97]. 不同的是,在布尔线路中每个逻辑门(逻辑和和逻辑积)的输入是两个经典比特,而量子线路图中每个量子逻辑门的输入是四个量子比特. 不失一般性,在量子计算中我们把这些逻辑运算视作由一组量子逻辑门构成的黑盒.

众所周知,量子门按照输入的量子比特数可以分成单比特、二比特及多比特量子门. 这些量子比特门构成一个集合组. 在这里我们忽略具体的量子逻辑门,只根据输入的量子比特数划分. 于是,量子线路中出现的量子逻辑门的数量称为量子线路的尺寸. 如果两个线路有相同的输入和输出,则称它们是等价的. 如果不存在含有更少量子比特门的等价量子线路,则称该量子线路的尺寸是最小的.

设 $N(n,S)$ 表示计算不同布尔函数的量子线路的数量,其中 n 表示量子比特数,S 表示量子线路中的量子逻辑门数.

引理 1[95]. 对任意的 S 有 $N(n,S)<S(2^n)^S$.

由引理直接得到下面的结果.

定理 3[95]. 设量子计算机有 n 个量子比特. 在标准谕示模型下,不存在多项式尺寸的量子线路计算所有的布尔函数.

在文献[95]中我们得到了与经典情况相似的结论,即不存在多项式规模的量子线路计算布尔函数. 虽然到目前为止,我们仍未能找到具体的布尔函数的布尔线路或量子线路的规模是超线性函数的. 但这表明即使在量子计算中,仍有许多的计算是量子计算不能有效完成的. 于是我们得到重要的结论,即输入数据复杂性很大的问题是抗量子计算的. 换句话说,若某个计算任务的输入数据量与计算所有的布尔函数的数据量是一个数量级的,则该问题是抗量子计算的.

不论是电子环境还是量子环境下,时间复杂性、空间复杂性[98]和数据复杂性都是重要的复杂性分类. 它们彼此之间是互相关联和影响的. 在算法运行过程中需要空间储存数据,这就涉及到空间复杂性. 有时算法运行需要的数据太大可能会超过储存能力. 另一方面算法运行时需要处理数据越多,则处理时间就越长. 此外,在量子计算中态之间的转换是复杂的. 譬如,经典态到量子态(或量子态到经典态)转换的过程是复杂的,而量子态之间的转换是容易实现的. 这对量子计算机的影响是很大的. 在量子计算内部的数据处理是量子态的,而显示给人看到的数据是经典态的. 所以在输入输出数据的环节,量子计算机的速度和量子计算机的处理速度相比是慢的. 在密码设计上,我们可以利用这个特点. 如果我们设计的密码使得攻击该密码需要极大的输入输出数据复杂性,则该密码就可以抵御量子计算的攻击.

4.4 量子基本运算和 Shor 算法的优化实现

量子计算的通用模型包括,一种是基于一系列门和测量来实现的,另一种仅包含量子测量. 目前大部分的量子计算研究重点是第一种.

下面通过实现量子计算机中两个量子比特 x_1 和 x_2 的与操作方案,解释一下量子计算的过程.

(1) 采用 3 个量子比特位的变换来表示 $|x_1,x_2,y\rangle$;

(2) 置第 3 个量子比特为 0,即 $y=|0\rangle$;

(3) 对 $|x_1,x_2,0\rangle$ 执行 U_{and} 操作,定义 $U_{\text{and}}:|x_1,x_2,0\rangle=|x_1,x_2,x_1\wedge x_2\rangle$,其中 $x_1\wedge x_2$ 表示 x_1 和 x_2 的经典与操作结果,而$\oplus$表示模 2 加;

(4) 对第 3 个量子比特进行$(|0\rangle,|1\rangle)$测量,测量结果作为 U_{and} 操作的结果.

通过对以上的运算策略进一步推广,已经证明量子计算机能够完成经典计算的任何任务[99]. 而加法作为经典计算的基础运算,在量子计算中能成功地被模拟. 在文献[100]中给出了包括加法、模加、模乘、模幂基本运算的量子线路图. 利用模幂运算可以实现 Shor 量子算法. 它使用一个线性增长的辅助储存器执行分解大因子算法.

在文献[101]中作者优化了原始的量子加法基本运算的量子线路图. 在此基础上,我们进一步优化了量子加法基本运算的量子线路图. 以 3 量子比特为例(见图 6),对比文献[101]给出的 3 位输入,2 位

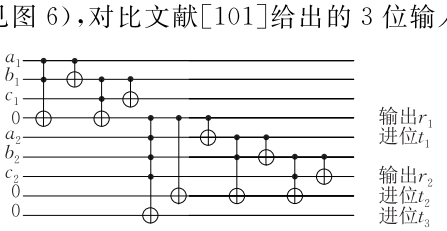

图 6 3 个两位数的量子加法

输出和 4 位输入，3 位输出的量子加法，我们的方案使用的量子比特数均比原方案少一个，且量子门更加简单.

通过对比出现的量子加法路线图的构造，得到结论：量子加法的构造可用受控非门和 Toffoli 门连接而成. 做简单的推广粗糙地得到一个结果，对 $m(m\geq 3)$ 个数据的加法可以用一个 m 个数的一位加法和多个 $m+1$ 个数的一位加法元件组合而成，表达式为 $U_{(m,n)}=U_{(m+1,1)}^{n-1}U_{(m,1)}$. 设符号 S_{ij} 表示对第 i 位和第 j 位的元素进行加法运算. 设 T_n 表示含有 n 个量子比特参与运算的 Toffoli 门. 设 $U_{(m,n)}$ 表示 m 个 n 位量子比特数的加法. 例 $U_{(5,2)}=U_{(52)}U_{(6,1)}U_{(5,1)}=S_{56}S_{45}S_{34}S_{12}C_6^5T_5C_6^4T_4S_{45}S_{34}S_{23}S_{12}C_5^4T_4$. 这个例子不一定是最佳方案，得到的扩展方案与同类方案[101]比较，使用的量子比特数和量子门更少.

Shor 算法是重要的量子算法之一. Shor 算法的出现使得量子算法求解整数分解问题优于任何已知的经典算法. 这个标准的量子算法刺激了量子信息处理的研究与量子计算机的实际实现. 在过去的 20 年中，利用优化技术，Shor 算法的在各种不同的平台上进行了实现. 证明了量子求解整数问题的有效性.

但是，在实验方面 Shor 算法的执行需要很高的条件，一个充分大的量子寄存器和高保真的量子控制. 因此，这对于量子算法的优化和实验的简化都是一个重要的挑战. 量子算法的优化和实验的简化是可能的. 一般地，理论上的优化结果好于实验的结果①.

在 Shor 算法优化方面出现了很多的成果. Takahashi 利用 $2n+2$ 个量子比特构造了一个量子线路[102]，其中 n 是待分解数的比特长度. 该量子线路使用了 $O(n^3\log n)$ 量子逻辑门. 该线路比 Beauregard 的量子线路方案更优[103]. 不仅量子比特数减少一个，而且量子逻辑门少一半. Pavlidis 通过利用量子傅里叶变换构建更复杂的算术乘法器(累加器)，量子常数和常数的量子分频器来实现 Shor 算法. 它们可以有效地执行量子模乘运算. 这个量子线路需要 $9n+2$ 个量子比特[104]. 付向群等基于半经典量子傅里叶变换的方法，设计了一个新的量子线路. 该线路需要 $O((\log n)^3)$ 量子逻辑门，需要的量子比特数比初始方案多 2 个量子比特，但是实现速度增加 2 倍[105]. 随后，付向群等将这个结果进行了推广. 由于大维数量子寄存器生成的困难性，基于小维数量子寄存器实现大维数量子 Fourier 变换的方法，与 Parker 等人的实现线路相比，计算资源大体相同，所需量子寄存器的维数前者较后者多 $t-1$ 维，而实现速度提高了 t^2 倍，t 是窗口宽度[106].

Shor 算法的实验方面也有许多的成果. 在处理量子编码技术中，普遍使用的是量子光学电路. Politi 等在硅芯片上利用 4 单光子量子比特实现了分解 15 的 Shor 算法[107]. Crespi 实现了光子集成控制非(CNOT)栅偏振编码的量子比特[108]，对于逻辑真值表的量子门表现出其高的保真度. 这表明这个门的能力将可分离状态转换成纠缠的. 利用该技术可以实现 Shor 算法.

虽然 Shor 算法在理论上是一个成熟的算法，但是在实现上存在着距离. 由于量子算法是一个概率算法，并不能保证 Shor 算法每次都能成功. 通过优化可以提高算法的成功率，接近 1. 到目前为止，对 Shor 算法实现方法的优化都是基于算法实现所需的量子比特数，基本量子门数量和实现速度方面去研究 Shor 算法的优化.

在硬件实现方面，尽管已经出现了一些实现的方案，但是实现的位数较少，仅处于实验室阶段. 目前，对量子计算研究者而言还不能使用真正的量子计算机，更多地是使用经典计算机模拟量子算法进行验证实现. 量子计算的经典模拟对量子计算理论和量子算法正确性、可行性的研究具有重要意义. 可以通过经典模拟进行超前研究，但是经典计算机的计算速度和存储空间远不能满足量子计算机的需求，它的验证范围也有限. 这限制了经典模拟的发展. 如何构造更好的经典模拟环境，并有效地和目前计算机系统结合也是一个重要的研究内容. 目前使用的量子模拟器有 Mathemcatica notebook simulation、QCL、QCE、QDD 等. 模拟器主要是对目前比较成熟的量子算法的模拟，比如 Grover、Deutsch 以及小波变换等.

4.5　其他量子计算模型

除了上面讨论的以外，其他量子计算模型还有量子计数模型、量子查询模型、量子黑箱模型、量子通信模型等. 而单向量子模型[109]和绝热量子模型[110]的出现为量子计算研究带来了新思路. 而量子衍生算法[111]，量子遗传算法[112]等丰富了量子算法的应用领域. 单向量子模型用于量子水印技术[113]等，绝热量子模型[114]更多地用于分解大合数问题. 对偶量子模型可以允许在量子算法的设计中使用非酉算符[115]. 各种量子模型的出现对研究量子算法求解问题是有利的，丰富了研究的领域.

① Smolin J A, Smith G, Vargo A. Pretending to factor large numbers on a quantum computer. http://arxiv.org/. arXiv preprint arXiv:1301.7007, 2013

5 格密码的量子安全性

5.1 格理论及其困难问题

格理论的研究开始于 18 世纪. 它被作为一个算法工具用来解决数学和计算机科学中的一系列问题,这包括密码分析[116]和公钥密码设计[117]等.

格被看做是一种具有周期性结构的 n 维点空间集合. 格密码有很多优势. 首先,它具有抗量子计算的潜力. 其次,格算法具有简单易实现、高效性、可并行性特点. 它的运算简单,通常只涉及矩阵、向量之间的线性运算. 第三,格密码已经被证明在最坏条件下和平均条件下具有同等的安全性.

因此格密码可以作为抗量子密码领域的一个候选方案. 下面介绍格中的一些困难问题.

定义 3(格的定义). 给定 n 个线性无关的向量 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n\in R^n$,由它们生成的向量集合

$$L(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i,x_i\in Z\right\}$$

称为格. 向量 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n$ 称为格 L 的一组基. 任意一组基可以用一个实数矩阵 $\boldsymbol{B}=[\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n]\in R^{n\times n}$ 表示,矩阵的列向量由基向量组成.

使用矩阵表示后,一个格可以用矩阵的语言描述为 $L(\boldsymbol{B})=\{\boldsymbol{Bx},\boldsymbol{x}\in Z_n\}$,其中 $\boldsymbol{Bx}$ 表示一个矩阵与向量的乘法.

定义 4(q 元格). 给定正整数 q,m,n,矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$,可以得到下面两个 q 元格:

$$\Lambda_q(\boldsymbol{A})=\{\boldsymbol{y}\in Z^m,\boldsymbol{s}\in Z^n,\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}s(\mathrm{mod}q)\},$$

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{y}\in Z^m,\boldsymbol{Ay}=0(\mathrm{mod}q)\}.$$

第 1 个 q 元格由 $\boldsymbol{A}$ 的行向量生成,第 2 个格包含了所有与 $\boldsymbol{A}$ 的行向量模 q 正交的向量.

在格理论中有许多的困难问题. 首先介绍最短向量问题(SVP)及其变型问题. 其次,介绍另一个重要的格问题类,最近向量问题(CVP)及其变型问题.

定义 5(最短向量问题(SVP)). 对于一个 d 维格 $L\subseteq Z^n$ 给定一组基 $\boldsymbol{B}$,找到一个非零的向量 $\boldsymbol{u}\in L$ 满足

$$\|\boldsymbol{u}\|=\min_{\boldsymbol{v}\in L/0}\|\boldsymbol{v}\|.$$

格中的最短向量是不唯一的. 因为如果 $\boldsymbol{u}$ 是最短向量,$-\boldsymbol{u}$ 也是. 其中符号 $\|\ \|$ 表示范数.

1801 年 Gauss 在欧几里德范数中提出了范数的限定概念. 直到 2002 年 Kaib 和 Schnorr 将其推广到任意范数[118]. 1910 年 Minkowski 建立了二次型与丢番图近似之间的联系,其中一个中心问题就是证明格中最短向量的存在[119]. 1981 年 Van 证明了 SVP 在 l_∞ 范数下是 NP 难的[120]. 1998 年 Ajtai 证明了在 $l_p(p<\infty)$ 范数下的困难性①. 对大多数应用来说,最短向量定义在 l_2 范数上. 大多数情况下,不要求最短只要近似最短满足计算要求即可.

定义 6(近似最短向量 a-SVP). 给定近似因子 $\gamma>1$ 和一组基,找到一个非零向量 $\boldsymbol{u}\in L$,使得

$$\|\boldsymbol{u}\|=\gamma\lambda_1(L).$$

求解 a-SVP 问题最著名的算法是 LLL 算法,对近似因子 $\gamma=2^{o(n)}$,LLL 算法是个多项式时间算法求解近似 SVP.

目前,对近似因子 $\gamma=2^{\log n^{1/2-\varepsilon}}$($\varepsilon>0$ 是一个任意小的常量)的 a-SVP 在准多项式归约下是 NP 难的[121].

定义 7(Hermite 最短向量 HSVP). 给定 d 维格 $L\subseteq Z^n$ 的一组基 $\boldsymbol{B}$ 和一个近似因子 $\gamma>0$,找一个非零向量 $\boldsymbol{v}$ 使得其范数满足

$$\|\boldsymbol{v}\|\leq\gamma(vol(L))^{1/d}.$$

如果格的体积是易计算的,则确认正确的解也变得容易了. Hermite 常量确保 $\gamma\geq\gamma_d$ 时至少有一解,而 $\lambda_1(L)\leq\sqrt{\lambda_d}vol(L)^{1/d}$.

因为 LLL 算法可以找到一组基,使得第一个向量 $\|\boldsymbol{b}_1\|\leq\alpha^{(d-1)/4}\ vol\ (L)^{1/d}$,其中 $\alpha>4/3$. 因此 LLL 算法可以解决近似因子为 $\gamma=\alpha^{(d-1)/4}$ 的 HSVP 问题.

定义 8(最短长度问题 SLP). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$ 和一个近似因子 $\gamma>0$,找到一个值 $\lambda(L)$ 满足

$$\lambda_1(L)\leq\lambda(L)\leq\gamma\lambda_1(L).$$

当 $\gamma=1$ 时,$\lambda_1(L)=\lambda(L)$.

定义 9(唯一最短向量 u-SVP). 对于一个满秩格 $L\subseteq Z_n$ 的基 $\boldsymbol{B}$ 和一个间隙因子 γ,找到最短非零向量 $\boldsymbol{v}\in L$,其中 $\boldsymbol{v}$ 是惟一的(对其他任何向量 $\boldsymbol{x}\in L$ 满足

$$\|\boldsymbol{x}\|\leq\gamma\|\boldsymbol{v}\|,$$

且至多是向量 $\boldsymbol{v}$ 长度的 γ 倍的向量都平行于 $\boldsymbol{v}$).

定义 10(最短基问题 SBP). 给定一个 d 维格 $L\subseteq Z_n$ 的基 $\boldsymbol{B}$ 和一个近似因子 $\gamma>0$,找到一组基 $\boldsymbol{B}=[\boldsymbol{b}_1,\cdots,\boldsymbol{b}_d]$ 满足

$$\max_{1\leq i\leq d}\|\boldsymbol{b}_i\|\leq\gamma\max_{1\leq i\leq d}\|\boldsymbol{b}_i'\|,$$

① Micciancio D. Lattice Based Cryptography: A Global Improvement. http://eprint.iacr.org/. IACR Cryptology ePrint Archive, 1999, 1999: 5

其中 $\boldsymbol{B}'=[\boldsymbol{b}'_1,\cdots,\boldsymbol{b}'_d]\in\boldsymbol{B}(L)$ 是 L 的任意一组基. 当 $\gamma=1$ 时，$\max\limits_{1\le i\le d}\|\boldsymbol{b}_i\|=\max\limits_{1\le i\le d}\|\boldsymbol{b}'_i\|$.

定义 11(最短向量决策问题 GapSVP). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$，一实数因子 r 和一个近似因子 γ，决定 $\lambda_1(L(\boldsymbol{B}))\le r$ 或 $\lambda_1(L(\boldsymbol{B}))\ge\gamma r$. 即如果 $\lambda_1(L(\boldsymbol{B}))\le r$，结果直接返回 YES. 如果 $\lambda_1(L(\boldsymbol{B}))\ge\gamma r$，结果直接返回 NO. 否则，如果 $r\le\lambda_1(L(\boldsymbol{B}))\le\gamma r$，那么 YES 和 NO 都可被返回. 这个问题被称为 promise 问题. 对任何常量近似因子 γ，GapSVP 是 NP 难的.

定义 12(最短独立向量问题 SIVP). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$ 和一个近似因子 $\gamma>0$，找到一组 d 个线性无关向量 $\boldsymbol{u}_1,\cdots,\boldsymbol{u}_d$ 满足

$$\max_{i=1}^{d}\|\boldsymbol{u}_i\|\le\gamma\lambda_d(L).$$

此外，另外一个重要的格问题类是最近向量问题(CVP)及其变型问题.

定义 13(最近向量问题 CVP). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$ 和一个目标向量 $\boldsymbol{x}\in span(L)$，找到一个向量 $\boldsymbol{u}\in L$，满足

$$\|\boldsymbol{x}-\boldsymbol{u}\|=dist(\boldsymbol{x},L).$$

定义 14(近似最近向量问题 ACVP). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$，一个目标向量 $\boldsymbol{x}\in R$ 和一个近似因子 $\gamma\ge1$，找到一个向量 $\boldsymbol{u}\in L$，满足

$$\|\boldsymbol{x}-\boldsymbol{u}\|\le\gamma dist(\boldsymbol{x},L).$$

Henk 第一次提出 CVP 比 SVP 困难一些(对同一维数来说). 后由 Goldreich 扩展开来，提出一个预言，对各种范数解决 CVP 就可以解决 SVP(在相同维数下).

定义 15(有界距离译码 BDD). 给定 d 维格 $L\subseteq Z_n$ 的一组基 $\boldsymbol{B}$，一个距离参数 $\alpha>0$ 和一个目标向量 $\boldsymbol{x}\in span(L)$，找到一个向量 $\boldsymbol{u}\in L$ 满足

$$\|\boldsymbol{x}-\boldsymbol{u}\|=dist(s,L)<\alpha\lambda_1(L).$$

当目标向量距格不远于 $\alpha\lambda_1(L)$ 时，BDD 和 CVP 是一样的.

定义 16(最小整数解 SIS). 给定一个模 q，一个矩阵 $\boldsymbol{A}\in Z_q^{n\times m}(m\ge n)$ 和一个实数常值 v，找到一个非零向量 $\boldsymbol{u}\in Z^m$，满足 $\boldsymbol{Au}=0(\mathrm{mod}q)$，且 $\|\boldsymbol{u}\|\le v$.

v 的选择保证了解的存在. 这是因为 $\boldsymbol{x}=q\boldsymbol{e}_i$ 是 $\boldsymbol{AX}=0(\mathrm{mod}q)$ 的平凡解，所以 v 的选择通常小于 q.

2007 年 Micciancio 和 Regev 指出在一个随机格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 中解 SVP 问题至少和求解平均状况的 SIS 一样困难[122]，其中 v 的选择满足 SIS 的条件.

定义 17(非齐次最小整数解 ISIS). 给定 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组基，找到一个向量 $\boldsymbol{v}\in Z_q^n$ 满足

$$\boldsymbol{Av}=0(\mathrm{mod}q).$$

如果存在一个算法可以找到解且 $\|\boldsymbol{v}\|\le\beta$(对给定的范数界)，则称算法成功. 将上式右边的 0 替换为 y，则得到 SIS 问题的一个非齐次状态，记为 ISIS(q,m,β).

如果不存在有效的算法在多项式时间 t 内，以不小于 ε 的概率求解 SIS(ISIS)，则 SIS(ISIS)是 (t,ε)难的. ISIS 问题的 relation problem 定义为

$$R_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}=\{((\boldsymbol{A},\boldsymbol{y}),\boldsymbol{x})\in Z_q^{n\times m}\times Z_q^n\times Z^m,\ \|\boldsymbol{x}\|_{\infty}\le\beta,\boldsymbol{Ax}=\boldsymbol{y}[q]\}.$$

Kawachi 等得到了 ISIS$^{\infty}$ 问题的一个变型版本[123]，使得

$$R_{\mathrm{KTX}_{n,m,q,\omega}}=\{((\boldsymbol{A},\boldsymbol{y}),\boldsymbol{x})\in Z_q^{n\times m}\times Z_q^n\times\{0,1\}^m,\ wt(\boldsymbol{x})=\omega,\boldsymbol{Ax}=\boldsymbol{y}[q]\}.$$

文中指出对给定 m 和 $\beta=plon(n)$，任意的素数 $q\ge\beta\sqrt{\omega n(\log n)}$，近似因子 $\gamma=\beta\cdot O(\sqrt{n})$，求解平均情况下的 $\mathrm{SIS}_{q,n,m,\beta}$ 和 $\mathrm{ISIS}_{q,n,m,\beta}$ 问题，同最差条件下近似 SIVP_{γ} 和 GapSVP_{γ} 问题的困难性相同.

除了最短向量问题(SVP)、最近向量问题(CVP)之外，还有一类被称为带误差的学习问题(LWE). 它在密码学中有着广泛的应用. 下面简单介绍一下带误差的学习问题(LWE)及其变型问题.

定义 18(带误差的学习问题 LWE)[117]. 选取参数 $q\ge2$ 作为大整数模，$\boldsymbol{s}\in Z_q^n$ 是一个 n 维向量，χ 是 Z_q 上的一个概率分布，$A_{s,\chi}$ 是 $Z_q^n\times Z_q^n$ 的一个概率分布，分布样本选取如下：

(1) 从 Z_q^n 中随机均匀选取 a；

(2) 通过 χ 在 Z_q 上选取 $\boldsymbol{e}$；

(3) 返回元组 $(a,\langle a,\boldsymbol{s}\rangle+\boldsymbol{e})$.

给定 $n\ge1$，模 $q\ge2$，Z_q 上的一个概率分布 χ 和分布 $A_{s,\chi}$ 中的任意多个相互独立的样本，找到 $\boldsymbol{s}$.

定义 19(带均匀误差的 LWE 问题(LWE_U)). 给定正整数 $m,n,q=q(n)>2$，输入对 $(\boldsymbol{A},\boldsymbol{b})$，其中 $\boldsymbol{A}\in Z_q^{m\times n}$，向量 $\boldsymbol{b}\in Z_q^m$，误差 $\boldsymbol{e}\in Z_q^m$ 服从均匀分布 Z_q^m，找到向量 $\boldsymbol{s}\in Z_q^n$ 满足等式 $\boldsymbol{b}=\boldsymbol{As}+\boldsymbol{e}$.

5.2　格问题的难解性

在 2002 年 Regev 将傅里叶变换应用到格困难问题及格密码的分析上[124]，考虑了最坏情况下的唯一最短向量问题(uSVP)解的情况，并提高了 Ajtai 和 Dwork 的格密码的安全性指标，同时在文章中给出了存在量子算法求解 n^c-uSVP 问题的充分条件. 在 2003 年 Aharonov 等人考虑了一个特

殊的最短向量问题 coGapSVP$_{\sqrt{n}}$，证明了该问题属于 QMA，即 NP 问题在量子环境下的模拟[125]. 在 2004 年 Aharonov 等人考虑了其他的格困难问题，近似最短向量问题（aSVP）和近似最近向量问题（aCVP），证明了这两个问题属于 NP⋂coNP，故在标准量子谕示模型中不存在有效的量子算法求解这两个格困难问题[126].

随后，在 2003 年 Regev 首次考虑了利用量子算法求解特殊的格困难问题[127]. 文中证明，在陪集抽样实验中如果存在算法求解二面体群的隐藏子群问题，那么存在算法求解唯一最短向量问题（uSVP）. 另外，文中讨论了二面体群陪集问题，指出如果存在带有失效参数 f 的算法求解二面体群陪集问题，那么存在量子算法求解 $\theta(n^{\frac{1}{2}+2f})$ 唯一最短向量问题. 结合这两点，作者给出了 $\theta(n^{2.5})$ 唯一最短向量问题到平均情况下的子集和问题的量子规约. 但是 Regev 提出的量子算法的时间复杂性是 $2^{O(\sqrt{\log N(\log\log N)})}$. 2004 年 Regev 修改了原来的量子算法，将量子空间复杂性降低到多项式规模，而时间复杂性仍是亚指数的[94]. 2015 年 Laarhoven 等人在改进的量子 Grover 算法基础上讨论了最短向量问题（SVP），提出新的量子算法的复杂度是 $O(2^{1.799n+O(n)})$[128]. 这一结果优于 Micciancio[129]、Nguyen[130]、Wang 等人[131]的经典算法复杂性. 同年，Laarhoven 等人在文献[132]中利用局部敏感的哈希函数（LSH）加速格基筛选，将求解最短向量问题（SVP）的时间和空间复杂度分别降低到 $O(2^{0.298n+O(n)})$ 和 $O(2^{0.208n+O(n)})$. Becker 等人在文献[133]中提出新的启发式算法求解最短向量问题（SVP）. 在不增加新的寄存器的情况下，该算法的时间复杂性和空间复杂性分别是 $O(2^{0.3122n+O(n)})$ 和 $O(2^{0.2075n+O(n)})$.

在 2005 年 Regev 提出了 LWE 问题，并讨论了它的难解性[117]，给出从 GapSVP 问题到 SIVP 问题的量子规约，其中 SIVP 问题是 SVP 问题的一个变型. 在量子规约下，LWE 问题与最坏情况下近似因子为 $O(n/\alpha)$ 的 SVP 问题一样困难，其中 α 是与扰动分布方差相关的实际参数. 2013 年 Lyubashevsky 等人[134]在环上考虑了 LWE 问题，假设不存在多项式的量子计算机求解最坏情况下的理想格问题，那么环 LWE 的分布是随机的.

5.3 基于格的密码学

这些格困难问题的出现为设计新的格密码方案提供了理论上的支持.

5.3.1 AD 公钥密码

1997 年 Ajtai 和 Dwork 提出第一个格密码方案[135]，简称为 AD. 该公钥密码体制是基于 $O(n^8)$－uSVP 的最坏情况困难性. 在 1997 年 Goldreich 等在文中针对 AD 密码体制的解密失败问题给出消除解密错误方案[118]，并且给出了一种新的密码体制将安全性提高到 $O(n^7)$－uSVP，但新方案并没有基于格的困难问题，这就失去了与之等价的安全性. 2004 年 Regev 提出了一个新的困难性相当于 $O(n^{1.5})$－uSVP 的公钥密码体制[124].

AD 密码体制是定义在欧氏向量空间集合上. 该安全参数 n 是向量空间的维数. 令 $m=n^3$ 且 $r_n=n^n$. 引入符号 B_n 表示 n 维立方体，$B_n=\{\boldsymbol{x}\in R^n:|x_i|\leq\frac{r_n}{2},\forall i\}$，且对于 $c>0$，将半径为 n^{-c} 的 n 维球记作 $S_n=\{\boldsymbol{x}\in R^n:\|\boldsymbol{x}\|\leq n^{-c}\}$.

私钥是从 n 维单位球中随机选择的向量 $\boldsymbol{u}$. 在 B_n 上定义的广义函数 H_n 有如下的结构：

（1）从 $\{\boldsymbol{x}\in B_n:\langle\boldsymbol{x},\boldsymbol{u}\rangle\in Z\}$ 中随机均一地选取元素 $\boldsymbol{x}$.

（2）从集合 S_n 中随机均一地选取误差向量 $\boldsymbol{y}_1,\cdots,\boldsymbol{y}_n$.

（3）输出 $\boldsymbol{v}=\boldsymbol{x}+\sum_{i=1}^{n}\boldsymbol{y}_i$.

同时从 H_n 中随机选取 $n+m$ 个向量 $\boldsymbol{w}_1,\cdots,\boldsymbol{w}_n,\boldsymbol{v}_1,\cdots,\boldsymbol{v}_m$ 作为公开密钥. 其中 $\boldsymbol{w}_i$ 满足从 $\boldsymbol{w}_i$ 到由 $\boldsymbol{w}_j$ 生成的超平面（$i\neq j$）的最小距离不小于 $\frac{r_n}{n^2}$.

加密过程：加密是逐比特进行的. 首先加密 0 比特，令 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n$ 从 $\{0,1\}$ 中随机选取并且归约向量 $\sum_{i=1}^{n}\boldsymbol{b}_i\boldsymbol{v}_i$ 模平行六面体

$$P(\boldsymbol{w}_1,\cdots,\boldsymbol{w}_n)=\Big\{\sum_{i=1}^{n}\lambda_i\omega_i:0\leq\lambda_i\leq1\Big\}.$$

将 n 维向量作为密文. 其次加密 1 比特. 从平行六面体 $P(\boldsymbol{w}_1,\cdots,\boldsymbol{w}_n)$ 中随机选取 n 维向量作为密文.

解密过程：对于密文 c，通过密钥 u 可以计算出明文. 如果 $dist(\langle c,u\rangle,Z)\leq n^{-1}$，那么密文解密为 0 比特；反之解密为 1 比特.

AD 密码体制存在以下 3 个方面的问题：

（1）解密失误. 由于 AD 密码存在解密失误的现象，所以必须保证解密错误以比较低的概率发生，否则大量解密错误会使 AD 无法使用. 减少扰动参数可以有效降低解密错误发生的概率，但扰动参数

太小，就可能泄露私钥信息. 因此 AD 密码是一种 IPKC.

(2) 效率问题. 由于 AD 是由逐比特加密的，1 比特的信息被加密成为实空间中的一个点. 数据扩展和内存需求很大.

但是由于 AD 已经被证明平均安全性与最坏安全性相同. 因此如果加密的明文不多，又要求具有较高的安全性，那么就可以考虑使用 AD 方案.

(3) 实用性问题. 为了使 AD 方案能够抵抗概率算法攻击，必须满足 $n>32$. 如果 $n=32$，那么公钥大小为 20 M 字节，并且每 1 比特的明文加密后将变成一个 6144 比特的密文. 如此大的公钥和加密数据扩充，使 AD 在普通的公钥密码应用中难以接受. 因此实用性大大受到限制[119].

5.3.2　GGH 公钥密码

在 1997 年 Goldreich、Goldwasser 和 Halevi[120] 设计了简称为 GGH 的密码体制，并给出了一个基于 CVP 问题的单项陷门函数，使用这种函数可以用来做为公钥加密后的数字签名. 这也是第一次基于格的签名. 它对 AD 加密体制进行了改进避免了解密失败的现象.

该体制有两个参数，分别是格维数 n 和安全参数 δ. 它们是由最近向量问题加密的困难性决定的. 私钥是由矩阵 $\boldsymbol{R}$ 给出. 矩阵 $\boldsymbol{R}$ 的列构成格 L 的一组基. 这些基构成合理的短整向量. 设计者在文中给出了集中构造 $\boldsymbol{R}$ 的方法. 公钥由公开的矩阵 $\boldsymbol{B}$ 构成，它的列表示 L 的不同的基. 与 $\boldsymbol{R}$ 不同的是，$\boldsymbol{B}$ 不能归约到 $\boldsymbol{R}$. 设计者给出了两种方法能随机地从 $\boldsymbol{R}$ 中生成 $\boldsymbol{B}$. 随后 Micciancio 提出更有效的厄米范式作为公开基(见本文第 12 页脚注①)[121].

加密过程：为了加密一个信息，将它进行编码为整向量 $\boldsymbol{m}\in Z^n$. 令误差向量 $\boldsymbol{e}$ 随机地取自集合 $\{-\sigma,\sigma\}^n$，计算密文 $c=\boldsymbol{B}\boldsymbol{m}+\boldsymbol{e}$.

解密过程：对于密文 c，解密得到明文 $m=\boldsymbol{B}^{-n}\boldsymbol{R}\lceil\boldsymbol{R}^{-n}c\rfloor$，其中符号$\lceil\bullet\rfloor$：$\boldsymbol{R}\to Z$ 运算规则是四舍五入. 对于 $\forall x=(\boldsymbol{x}_1,\cdots,\boldsymbol{x}_n)'\in R^n$，计算$\lceil x\rfloor=(\lceil\boldsymbol{x}_1\rfloor,\cdots,\lceil\boldsymbol{x}_n\rfloor)\in Z^n$.

分析过程：在 GGH 密码体制里，每个明文 m 对应格点 $m_L=\boldsymbol{B}\boldsymbol{m}$. 在加密过程中，明文 m 首先转换成对应的格点 m_L，然后通过增加误差向量 $\boldsymbol{e}$ 计算得到密文 c. 因此，通过选择 σ 和 $\boldsymbol{e}$ 使得 m_L 是最接近密文 c 的格向量. 为了得到明文 m_L(或者 m)，那就必须解决最短向量问题.

因此解密过程是由 Babai 的关于近似 CVP 问题四舍五入方法构成的.

在 1986 年 Babai 针对近似 CVP 问题提出两种方法，分别是四舍五入方法和最近平面算法[122]. 按照 Babai 的方法，当使用密钥 $\boldsymbol{R}$ 时效率很好，当使用公钥 $\boldsymbol{B}$ 解密时工作效率很差，即解密时按照 Babai 的方法使用密钥可以得到正确的格向量 $\boldsymbol{R}\lceil\boldsymbol{R}^{-1}c\rfloor$. 因为 $\boldsymbol{R}^{-1}m\boldsymbol{L}$ 是整向量，由 Babai 的方法知道 $\boldsymbol{R}\lceil\boldsymbol{R}^{-1}c\rfloor=\boldsymbol{R}\lceil\boldsymbol{R}^{-1}(m\boldsymbol{L}+\boldsymbol{e})\rfloor=\boldsymbol{R}(\boldsymbol{R}^{-1}m\boldsymbol{L}+\lceil\boldsymbol{R}^{-1}\boldsymbol{e}\rfloor)=m\boldsymbol{L}+\boldsymbol{R}\lceil\boldsymbol{R}^{-1}\boldsymbol{e}\rfloor$. 如果$\lceil\boldsymbol{R}^{-1}\boldsymbol{e}\rfloor=\boldsymbol{b}$ 是非零向量，那么 $\boldsymbol{R}\boldsymbol{b}$ 是非零的格向量. 此时，按照 Babai 的方法不能得到正确的格点，即恢复出错误的消息. 因而，当$\lceil\boldsymbol{R}^{-1}\boldsymbol{e}\rfloor=0$ 时加密是正确的. 同时，误差向量具有$(\pm\sigma,\cdots,\pm\sigma)$形式. 增加 σ 值意味着增加格向量 $\boldsymbol{m}\boldsymbol{L}$ 和密文 c 的距离，使得 CVP 问题更难于求解且解密错误的可能性增加. 另一方面按照 Babai 方法利用公钥 $\boldsymbol{B}$ 解密将会失败. 这是因为公钥 $\boldsymbol{B}$ 不能归约到密钥 $\boldsymbol{R}$ 上. 这意味着利用格基归约解决 CVP 问题等价于解决近似最短向量问题.

为了保证安全性，其公钥尺寸至少需要 1.8 MB，私钥尺寸也必须大于 1 MB. 这使得 GGH 密码体制的使用价值也不大.

5.3.3　NTRU 公钥密码

在 1996 年 Hostein、Pipher 和 Silverman[123] 提出了简称为 NTRU 的密码体制，同传统的公钥方法相比，它具有较小的密钥长度、较快的加密和解密时间等优势. 除此之外，在安全性方面也有优势，即存在潜在的抗量子计算能力. 这是因为到目前还没有有效的量子算法解决 NTRU 密码体制的基础——格问题. 在最近的十几年来，关于 NTRU 密码体制的安全性问题的研究已经变得十分活跃. 在国际上，NTRU 密码体制已经作为 IEEE P1363.1 标准[136]. 这也是到目前为止最好的基于格问题的公钥方案.

NTRU 密码体制包含加密和签名，这里只是介绍加密. 在介绍密码加密体系之前，先引入两个多项式函数的定义，选取整数 N，设多项式函数 $f=a_{N-1}x^{N-1}+\cdots+a_1x+a_0$ 和多项式函数 $g=b_{N-1}x^{N-1}+\cdots+b_1x+b_0$ 的次数小于 N. 定义 $h=f\otimes g=c_{n-1}x^{n-1}+\cdots+c_1x+c_0$，其中 $c_i=\sum_{i+k\equiv1}a_jb_k$. 这个和是对所有满足 $j+k\equiv i(\mathrm{mod}N)$的.

(1) 加密过程

通过预处理阶段，将明文 m 表示成次数小于 N 且系数的绝对值至多为 $(p-1)/2$ 的多项式，并选择一个小的多项式 φ 计算密文 $c=p\varphi\otimes h+m(\mathrm{mod}q)$.

(2)解密过程

计算 $a\equiv f\otimes c\equiv p\varphi\otimes g+f\otimes m(\mathrm{mod}q)$,其中多项式 a 的所有系数的绝对值至多为 $q/2$. 所以明文 $F_q\otimes a=pF_p\otimes\varphi\otimes g+F_p\otimes f\otimes m\equiv 0+1\otimes m=m(\mathrm{mod}p)$.

NTRU 密码体制的说明:因为在 NTRU 密码体制中次数是 $N-1$ 的多项式 f 和 g 定义的运算 $f\otimes g$ 需要 N^2 个乘法,所以在加解密一个长为 N 的明文时,需要运算 $O(N^2)$ 次的运算,因而密钥的长度为 $O(N)$. 当 NTRU 密码体制的参数 n 变为 $2n$ 时,加密过程中的两个 $n-1$ 次多项式变为两个 $2n-1$ 次的,加密 $2n\log 2p$ 比特的计算量从 $2n^2$ 变为 $4n^2$ 个,即 NTRU 密码体制的加密速度与 n 成反比.

(3)解密失败

在解密过程中,若 $a=p\varphi\otimes g+f\otimes m(\mathrm{mod}q)$ 不等于 $p\varphi\otimes g+f\otimes m$,而是存在一个非零多项式 u 使得 $a=p\varphi\otimes g+f\otimes m+qu$. 于是 $F_p\otimes a(\mathrm{mod}q)=m+quF_p(\mathrm{mod}q)$,其中 $(p,q)=1$. 当 p 不能整除 u 时 $qyF_p(\mathrm{mod}q)\neq 0$,解密失败.

在 NTRU 的技术报告上将解密失败分为越界错误和越距错误[137]. 越界错误是指多项式 $\varphi\otimes g+f\otimes m$ 的系数超出 $[-q/2,q/2)$,但是最大的系数和最小的系数之差不超过 q;如果最大的系数和最小的系数之差超过 q,称为越距错误. 同时越界错误可以用中心化方法纠正.

(4)NTRU 密码体制的攻击

到目前为止已经有各种各样的攻击方法针对 NTRU 密码体制,下面介绍一些已有的攻击方法:

设 $h=h_{N-1}x_{n-1}+\cdots+h_0$ 构造一个 $N\times N$ 矩阵

$$\boldsymbol{H}=\begin{pmatrix} h_0 & h_1 & \cdots & h_{N-1}\\ h_{N-1} & h_0 & \cdots & h_{N-2}\\ \vdots & \vdots & \ddots & \vdots\\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}.$$

用行向量分别表示多项式 $f=a_{N-1}x^{N-1}+\cdots+a_1x+a_0$ 和多项式 $g=b_{N-1}x^{N-1}+\cdots+b_1x+b_0$,记为 $\bar{f}=(a_0,\cdots,a_{N-1})$ 和 $\bar{g}=(b_0,\cdots,b_{N-1})$,那么 $\bar{f}\boldsymbol{H}=\bar{g}(\mathrm{mod}q)$.

设 $\boldsymbol{I}$ 为 $N\times N$ 单位矩阵,构造一个 $2N\times 2N$ 矩阵 $\boldsymbol{M}=\begin{pmatrix}\boldsymbol{I} & \boldsymbol{H}\\ 0 & q\boldsymbol{I}\end{pmatrix}$. 设 L 由矩阵 $\boldsymbol{M}$ 的行向量生成的格. 由于 $g\equiv f\otimes g(\mathrm{mod}q)$,所以存在多项式 y 有 $g=f\otimes g+qy$. 将 y 表示成一个 N 维的行向量 $\bar{y}$,那么 $(\bar{f},\bar{y})\boldsymbol{M}=(\bar{f},\bar{g})$,其中 $(\bar{f},\bar{y})$ 是 $2N$ 维行向量. 故有 $(\bar{f},\bar{g})$ 在格 L 中,由于 f 和 g 均有小的系数,使得 $(\bar{f},\bar{g})$ 在格 L 中是一个短的向量. 于是将 NTRU 密码体制建立在寻找最短向量问题(SVP 问题).

穷举攻击. 攻击者试图试遍所有的密钥 f,使得 $f\otimes g(\mathrm{mod}q)$ 有小的值;或者试遍所有的多项式 g. 所以攻击者如果想恢复明文,需要试遍可能的多项式 φ 计算得到明文 $m=c-\varphi\otimes h(\mathrm{mod}q)$. 而多项式 g 的规模小于多项式 f 的规模,所以密钥的安全由多项式 g 的规模决定. 同时明文的安全由多项式 φ 的规模决定.

其次是中途相遇攻击. 作者指出存在分别针对多项式 φ 和密钥 f 的攻击. 随后在文献[138]中继续了这一工作. 简单地说,将密钥 f 分成两半 $f=f_1+f_2$,分别计算 $\boldsymbol{x}_1=f_1\otimes h$ 和 $\boldsymbol{x}_2=-f_2\otimes h$. 因为 $(f_1+f_2)\otimes h=g(\mathrm{mod}q)$ 和 g 是二进制的,所以 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 模 q 后只是 0 与 1 的不同. 假设 f 有偶数 d_f 个 1,f_1 有 $d_f/2$ 个 1,那么从 N 次多项式中任取一个向量 $\boldsymbol{x}_1$,其系数满足 $-q/2<(\boldsymbol{x}_1)_i\leq q/2$. 对于 $\boldsymbol{x}_1$ 的每一个系数定义一个比特 β_i,其中若系数 $\boldsymbol{x}_1>0$ 则 $\beta_i=1$ 反之 $\beta_i=0$. 进而定义一个 N-比特的字符串 $a_1=\beta_1:\beta_2:\cdots:\beta_N$. 设 $\bar{\beta}=1-\beta$ 表示比特 β 的余,$\bar{a}$ 表示 N-比特的字符串的补. 所以 f_1 被分为两个储存盒,分别储存 a_1 和 $\bar{a}_1$. 因为 $\boldsymbol{x}_1=-\boldsymbol{x}_2+g$,使得 a_1 对应 $\boldsymbol{x}_1=f_1\otimes h$ 和 $\bar{a}_2$ 对应 $\boldsymbol{x}_2=-f_2\otimes h$. 当 $f=f_1+f_2$ 时,使得 $a_1=\bar{a}_2$ 即存在多项式 f_1,f_2 在盒内检测出碰撞. 对于这些碰撞能从储存的盒中恢复出多项式 f_1,f_2. 同时在文中估计了这种攻击的复杂性 $\frac{1}{\sqrt{N}}\binom{N}{d_f/2}\binom{d_f}{d_f/2}-\frac{1}{2}$.

第 3 种是多种传输攻击. 如果数次发送同一个明文 m,但是使用同一个密钥和不同的随机多项式 φ 进行加密,攻击者可能恢复大部分的明文. 现在发送密文 $c_i\equiv p\varphi_i\otimes h+m(\mathrm{mod}q)$ 其中 $i=1,\cdots,r$. 攻击者计算 $(c_i-c_1)\otimes h-1(\mathrm{mod}q)$,从而得到 $p\varphi_i-p\varphi_1(\mathrm{mod}q)$. 因为多项式 φ_i 非常小,以至能恢复出确定的 $p\varphi_i-p\varphi_1$,从而得到多项式 φ_1 的一些系数. 如果 r 比较小,那么可以通过穷举搜索恢复出明文. 因此建议在加密过程中增加干扰,使得能抵御这种攻击方式.

第 4 种格攻击. 已知的攻击主要是针对公钥 h 和明文 m. 与利用公钥攻击一样,攻击者是利用类似的方法找到 α,使得相对容易找到目标向量 $(\alpha m,\varphi)$.

对于利用格基归约方法的攻击,就需要使格具有足够高的维数,使得格基归约算法失效. 但是这样的结果使得加解密算法变得很慢,效率降低. 已知当最短向量与 $2N$ 维格的 $2N$ 次根判别式相比很小

时，格基归约算法有很高的成功概率. 利用这种方法，利用公钥 h 攻击，如果攻击者能选择合适的实数 α，将矩阵 $\boldsymbol{M}$ 中的 $\boldsymbol{I}$ 替换为 $\alpha\boldsymbol{I}$ 使得目标向量 $(\alpha\bar{f},\bar{g})$ 相对更容易找到，这样就可以提高攻击的效率. 文献[137]中给出了参数选择的方法. 或者在格 L 中另找一个向量 $(\boldsymbol{s},\boldsymbol{t})$ 满足 $h\otimes\boldsymbol{t}=\boldsymbol{s}(\mathrm{mod}q)$，使它尽量短，那么解密时，有 $c\otimes\boldsymbol{t}=p\varphi\otimes\boldsymbol{s}+m\otimes\boldsymbol{t}(\mathrm{mod}q)$. 若 $p\varphi\otimes\boldsymbol{s}+m\otimes\boldsymbol{t}$ 的系数没有越界，即 $p\varphi\otimes\boldsymbol{s}+m\otimes\boldsymbol{t}(\mathrm{mod}q)$ 与 $p\varphi\otimes\boldsymbol{s}+m\otimes\boldsymbol{t}$ 相等，计算 $(p\varphi\otimes\boldsymbol{s}+m\otimes\boldsymbol{t})\otimes\boldsymbol{t}-1=m(\mathrm{mod}q)$，即可得到明文. 但是还不能证明 CS 格中的困难问题的计算复杂性低于普通的格. 而对其他参数进行限制，也可以降低攻击的效率. 譬如，在加密过程中如果 $p\varphi\otimes h+m(\mathrm{mod}q)$ 等于 $p\varphi\otimes h+m$，即多项式 $p\varphi\otimes h+m$ 系数的绝对值至多为 $q/2$. 攻击者在截获密文后直接计算 $p\varphi\otimes h+m(\mathrm{mod}p)$，可得到 $m_1=\dfrac{m}{(p,m)}$. 如果 p 与 m 互素，可以直接恢复出明文；如果 p 与 m 不互素，m 是 m_1 的整数倍，通过选择参数可以恢复出明文. 所以这要求 $p\varphi\otimes h+m(\mathrm{mod}q)$ 不能等于 $p\varphi\otimes h+m$.

在 2000 年 Jaulmes 和 Joux 发表论文提出一种选择密文攻击[138]. 选择密文 $e=ch+c$，其中 c 是整数，h 是公钥. 攻击者将密文发给 Bob，经解密有 $a\equiv f\otimes ch+cf(\mathrm{mod}q)=cg+cf(\mathrm{mod}q)$，其中多项式 f 和 g 的系数等于 0，1 或 -1，因而多项式 $cg+cf$ 的系数为 $0,\pm c,\pm 2c$. 选择适当的 c 值满足 $c<q/2<2c$.

假设多项式 $cg+cf$ 的所有项中只有 x_i 项的系数为 $2c$，则 $cg+cf(\mathrm{mod}q)=f+cg-qx_i$. 将结果 $-qx_i\otimes F_p(\mathrm{mod}p)$ 返给攻击者. 因为 $(p,q)=1$，于是得到 $x_i\otimes F_p$ 的逆元 $x_{n-i}\otimes f$. 所以能得到一组与 (f,g) 等价的密钥 $(x_{n-i}\otimes f,x_{n-i}\otimes g)$. 当多项式有多个系数为 $\pm 2c$，此事只要改变密文的形式，经过一系列的计算最终得到等价密钥 $(x_{n-i}\otimes f,x_{n-i}\otimes g)$. 同时在文中作者列举出了在一些参数下的攻击成功的概率.

在 2002 年 Han 等人针对 NTRU 密码体制提出了恢复密钥攻击[139]. 具体算法描述如下：

(1) 初始化密钥 $f=\sum_{i=0}^{N-1}f_ix^i$，输入密文 $c=\sum_{i=1}^{N-1}c_ix^i$ 和整数 ω 有

① $f_0=1$，$f_j=0$，其中 $1\leq j\leq N-1$；

② $c_j=0$，其中 $0\leq j\leq N-1$；

③ $\omega=1$.

(2) $\forall i=1,\cdots,N-1$ 有如下过程：

如果 $\omega<q/2$，那么令 $c_{i-1}=-f_{i-1}$，反之 $c_{i-1}=0$；

如果 $\omega>q/2$，那么令 $c_i=\omega-q/2$，反之 $c_i=0$；

解密密文 c；

④在解密过程中如果 $a\neq f\otimes c$，令 $f_i=1$，$\omega=\omega+1$ 并且忽略⑤到⑧；

⑤令 $c_i=-c_i$；

⑥解密密文 c；

⑦在解密过程中如果 $a\neq f\otimes c$，令 $f_i=-1$，$\omega=\omega+1$ 并且忽略⑧；

⑧令 $f_i=0$；

(3) 令 $f_i=f_{N-1-i}$，其中 $i=0,1,\cdots,N-1$；

(4) 返回 $f=\sum_{i=0}^{N-1}f_ix^i$.

该算法得到密钥 f 的错误率最多是 $2N/3q-1$，但是该算法在加密时需要使用 $O(N^2)$ 次，过程变的十分复杂.

在 2003 年 Howgrave-Graham 和 Proos 等人[140]在文中提出两种选择明文攻击 NTRU 密码体制. 这两种攻击一开始都要求寻找能破译密文的或可以构成解密失败的对 (m,φ). 第 1 种攻击要求固定多项式 φ 和选择不同的明文 m. 现在逐个将明文 m 的非零系数变为 0. 如果使得变化后的明文 $\bar{m}$ 能解密成功，保持这个系数不变，反之令该系数为 0. 将这一过程继续直到明文 m 能够导致解密失败. 此时多项式 $s=p\varphi\otimes g+m\otimes f$ 的系数至少有一个超出了 $[-q/2,q/2)$ 的范围，而它的系数为 $\bar{s}_1=p\sum_{i=0}^{N-1}\varphi_i\otimes g_{j-i}+\sum_{i=0}^{N-1}\varphi_i\otimes f_{j-i}$，其中 φ_i,g_i,f_i 表示多项式 φ,g,f 的第 i 项系数. 譬如当 $p=3$ 时，m_i 的值是 $0,\pm 1$，而 f_{j-i} 的值按照如下的方式定义：若 $\bar{m}_i=1$ 且将 $\bar{m}_i$ 变为 0 解密成功，则 $f_{j-i}=1$；若 $\bar{m}_i=-1$ 且将 $\bar{m}_i$ 变为 0 解密成功，则 $f_{j-i}=-1$；若 $\bar{m}_i=0$ 且将 $\bar{m}_i$ 变为 -1 解密成功，则 $f_{j-i}=1$；若 $\bar{m}_i=0$ 且将 $\bar{m}_i$ 变为 1 解密成功，则 $f_{j-i}=-1$，反之 $f_{j-i}=0$. 然后寻找新的解密失败的明文和 φ 来确定其他的系数. 具体的分析细节可以参见文献[140].

第 2 种攻击要求固定明文 m 和选择不同的多项式 φ. 与第 1 种方法相似，选择解密失败的对 (m,φ)，计算 $(\varphi\otimes g)_0=\sum_{i=0}^{N-1}\varphi_ig_{N-i}$，其中 $(\varphi\otimes g)_0$ 表示多项式 $\varphi\otimes g$ 的常数项系数. 当 $\varphi_i=-g_{N-1}\neq 0$ 时，称 φ 和 g 有正碰撞；当 $\varphi_i=-g_{N-i}\neq 0$ 时，称 φ 和 g 有负碰

撞.于是 φ 和 g 的净值碰撞等于正碰撞减去负碰撞,即 $(\varphi\otimes g)_0$ 等价于净值碰撞.因为大部分随机选取的 φ 与 g 有正的净值碰撞,通过分析 φ 中的 1 和 -1 能够恢复 g 的非零系数.在实践中当 $\varphi_i=1$ 时有 3 种情况:高频率 $g_{N-i}=1$;随机频率 $g_{N-i}=0$;低频率 $g_{N-i}=-1$.同样实践中对 $\varphi_i=1$ 时有 3 种情况.因此攻击者可以分析 φ_i 得到 g 的系数的值,进而得到密钥 f.具体的分析细节可以参见文献[140].

NTRU 密码体制的扩展:在 2005 年 Yao 和 Zeng 提出关于 NTRU 密码体制的非填充的扩展方案,可以消除解密失败[141].与传统的 NTRU 密码体制不同,选择公钥 $\boldsymbol{H}=F_q\otimes r_1(\mathrm{mod}q)$ 和 $L=pF_q\otimes r_2(\mathrm{mod}q)$,其中 $r_1=1+p\otimes\varphi$ 和一个随机多项式 r_2.

加密过程:选择随机多项式 r_3,计算密文 $c=m\otimes\boldsymbol{H}+L\otimes r_3(\mathrm{mod}q)$.

解密过程:收到密文以后,计算 $a\equiv c\otimes f\equiv m\otimes r_1+pr_2\otimes r_3(\mathrm{mod}q)$.通过选择 p 和 q 使得 a 的系数小于 q,即恢复出明文 $m\equiv a(\mathrm{mod}q)$.

参数的设置:同传统的 NTRU 密码体制一样,明文的系数在 $-\frac{p-1}{2}$ 和 $\frac{p-1}{2}$ 之间.为了不降低安全性,使得多项式 r_1 和 r_2 不可逆,且格的维数大于 100.于是多项式 $m\otimes r_1$ 最多有 $pN+1$ 项,多项式 $r_2\otimes r_3$ 最多有 N 项.为保证解密的正确性使得多项式 a 的系数在 $-\frac{p-1}{2}$ 和 $\frac{p-1}{2}$ 之间,必须满足 $pN+1+pN<q/2$,即 $q>4pN+2$.随后作者在文中对前面提到的攻击传统的 NTRU 密码体制的方法进行分析,通过分析指出可以抵御这些攻击.

比较而言,选择密文攻击是已知的效果比较好的攻击方法.为了保护密码的安全性,在 2000 年 Hoffstein 和 Silverman 针对选择密文攻击先后提出了 3 种填充方案[142].因为对于 NTRU 密码体制中没有有效的安全性证明,所以这 3 种填充方案对 NTRU 密码体制的弥补并不能从本质上得到解决,只是对漏洞进行弥补提高了安全性,以及需要很小的计算开销,具体的安全性说明可参见 Hoffstein 和 Silverman 的文献.

虽然有普遍的填充方案,但是相比较 RSA 和 ElGamal 密码体制而言,NTRU 密码体制的散列成本相对于加解密不能忽略不计[140].

下面介绍这 3 个填充方案:设哈希函数 $H:\{0,1\}^m\to\{0,1\}^n$.设明文 M 是 k_1 比特长的字符串.在加密过程中需要随机 k_2 比特长的字符串 R,其中 k_2 在 40 到 80 之间且 $k_1+k_2\leq m$.令符号 $\|$ 表示字符串的连接.

填充方案 1:在加密过程中,使用随机字符串 R 得到密文 $c=D(M\|R;H(M\|R))$.填充方案 2:令哈希函数 $F:\{0,1\}^{k_1}\mapsto\{0,1\}^{k_2}$ 且 $\oplus$ 表示按位异或,于是可以得到密文 $c=D((F(R)\oplus M)\|R;H(M\|R))$[140].填充方案 3:首先将明文 M 和随机字符串 R 分成相等大小的块,$M=\overline{M}\|\underline{M}$ 和 $R=\overline{R}\|\underline{R}$.令哈希函数 F 和 G 是集合 $\{0,1\}^{k_1+k_2}$ 到集合 $\{0,1\}^{k_1+k_2}$ 的映射,计算 $m_1=(\overline{M}\|\overline{R})\oplus F(M\|\underline{R})$ 和 $m_2=(M\|\underline{R})\oplus G(m_1)$,于是得到密文 $c=D(m_1\|m_2;H(M\|R))$.

关于 NTRU 密码体制的变种方案有很多.譬如,在 2002 年 Banks 和 Shparlinski 提出简称为 G-NTRU 的密码体制,希望借助大的密码空间达到较好的安全性[143];在 2005 年 Coglianese 和 Goi 提出简称为 MaNTRU 的密码体制,其加密效率更高且密钥长度增加[144];同年,Yu 等人针对解密错误提出一种补偿算法;在 2008 年胡予璞教授对该方案进行了改进[145],具体的内容可以参看相关的参考文献:2009 年 Vats 在矩阵环中证明了 Shamir 关于 NTRU 密码的一个结论①,指出如果在非交换系统设计中设计相应的 NTRU 变种密码,那么它在加密和解密计算过程中能抵御格的攻击;在 2014 年文献[146]针对 NTRU 公钥密码体制是容易受到多个传输攻击这个不足,通过研究指出线性化攻击技术能恢复出明文.

5.3.4 Regev 公钥密码

2004 年,Regev 在发表的文章中提出了一个简称为 Regev 密码体制,对于安全参数 n,设 $N=28n$ 和 $m=cmn^2$,其中 cm 是特定的常数.令 $\gamma(n)=\omega(n\sqrt{\log n})$ 或者当 n 趋于无穷时满足 $\gamma(n)/\sqrt{\log n}$ 趋于无穷.一方面,选择一个较小的函数 $\gamma(n)$ 产生强的安全保障.另一方面,这也使得解密更容易出错.可以选择函数 $\omega(n\sqrt{\log n})$ 是最小的 $\gamma(n)$ 函数使得解密出错的概率可以忽略不计.具体的文中建议选择 $\gamma(n)=n\log n$.设 $H=\{h\in[\sqrt{N},2\sqrt{N})\mid frc(h)<1/16m\}$,其中 $frc(x)=|x-[x]|$,$x\in R$,且对 $\forall x,y\in R$,$0\leq frc(x)\leq 1/2$,$frc(x)\leq|x|$ 和 $frc(x+y)\leq frc(x)+frc(y)$.随机选取 $h\in H$ 作为密钥.

① Vats N. NNRU, a noncommutative analogue of NTRU. http://arxiv.org/. arXiv preprint arXiv:0902.1891, 2009

令 $x\in N, y\in R^+$，分布函数 $Tx,y(r)=\sum_{k=-\infty}^{\infty}\frac{1}{\sqrt{y}}\exp\left(\frac{-\pi}{y}(rx-k)^2\right)$，另一分布函数 $Q_y(r)=\sum_{k=-\infty}^{\infty}\frac{1}{\sqrt{y}}\left(\frac{-\pi}{y}(r-k)^2\right)$. 下面我们增加一个归一化因子将分布函数 Tx,y 扩展到非整数. 令实数 $h>0$ 和 $r\in[0,\cdots,1)$，重新定义 $Th,\beta(r)=\frac{1}{\int_0^1 Q_\beta(xh \bmod 1)\mathrm{d}x}Q_\beta(rh \bmod 1)$. 根据上面提到的分布函数，随机选取值 $x\in\{0,1,\cdots,h-1\}$ 和值 $y\in Q_\beta$. 如果 $\frac{x+y}{h}<1$，令 $z=\frac{x+y}{h}$. 反之，继续重复这一过程. 于是，选取 $\beta\in\left[\frac{4}{\gamma^2(n)},\frac{8}{\gamma^2(n)}\right)$ 并按照上面的过程选择 $x_1,\cdots,x_m$ 和 $y_1,\cdots,y_m$ 使得 $z_1,\cdots,z_m\in Th$. 对 $\forall i\in\{1,\cdots,m\}$，设 $a_i=|Nz_i|$ 和 i_0 是整数且使得 x_{i_0} 是奇数(这样的 i_0 概率存在的指数接近 1). 将 $(a_1,\cdots,a_m,i_0)$ 作为公钥.

加密过程：随机选取集合 $\{1,\cdots,m\}$ 的一个子集 S. 逐比特加密明文，加密 0 比特时计算 $\sum_{i\in S}a_i$ 模 N；加密 1 比特时计算 $\sum_{i\in S}a_i+\left|\frac{a_{i_0}}{2}\right|$ 模 N.

解密过程：令 $d=\frac{N}{h}$，如果 $frc\left(\frac{\omega}{d}\right)<\frac{1}{4}$，那么解密为 0 反之为 1，其中 $\omega\in\{0,\cdots,N-1\}$.

Regev 密码体制的公钥长度为 $O(\log N^2)$，逐比特加密的密文长度为 $O(\log N)$. 逐比特加密方案使加密速度过慢而且密文扩展比较大，使得工程实现不方便. 随后 2005 年 Ajtai[147] 和 Regev[117] 分别对该密码体制进行改进，使公钥长度和密文扩展为 $O(N)$，但是改进的算法安全性不再直接建立在格困难问题上.

5.3.5　Cai-Cusic 公钥密码

在 1998 年 Cai 和 Cusick[148] 提出了一种简称为 Cai-Cusick 密码体制. 它建立在近似 SVP 格问题上的密码体制，从单位球 $S_{n-1}=\{x\mid\|x\|=1\}$ 随机选取向量 $\boldsymbol{u}$ 和 $m+1$ 个字母的随机置换 σ 作为密钥. 由于允许指数小的舍入误差，不妨假设向量 $\boldsymbol{u}$ 的坐标是有理数，其分母是限制在非常大的整数的范围内. 设 $m=\lceil cn\rceil$，不妨令 $c=\frac{1}{2}$. 设 $H_i=\{\boldsymbol{v};\boldsymbol{v}\boldsymbol{u}=i\}$ 表示垂直于 $\boldsymbol{u}$ 的超平面. 公钥是参数 $b>0$ 和集合 $\{v_{\sigma(0)},\cdots,v_{\sigma(m)}\}$，其中 $\forall i\in Z^+$，$v_i\in H_i$ 满足 $v_ju=N_j\in Z^+$. 选择数列 N_j 使得 $N_0>b$ 和 $N_i>\sum_{j=0}^{i-1}N_i+b$，$i=1,\cdots,m$.

加密过程：加密 $m+1$ 位的明文 $P=(\delta_0,\cdots,\delta_m)$，其中 $\delta_i=0$ 或者 1，那么将 P 加上一个扰动进行计算得到密文 $\sum_{i=0}^{m}\delta_iv_{\sigma(i)}+1$，其中向量 $\boldsymbol{r}$ 是随机选取的且满足 $\|\boldsymbol{r}\|\leq\frac{b}{2}$.

解密过程：通过使用密钥 $\boldsymbol{u}$ 计算下面的内积 $S=\boldsymbol{u}(\sum_{i=0}^{m}\delta_iv_{\sigma(i)}+\boldsymbol{r})=\sum_{i=0}^{m}\delta_{\sigma-1(i)}N_i+\boldsymbol{u}\boldsymbol{r}$.

下面使用贪心算法能高效地从 S 中恢复出 $\delta_{\sigma-1(i)}$，并且使用秘密的 σ 得到 $\delta(i)$. 如果 $\delta_{\sigma-1(m)}=1$，那么 $S\geq N_m-\frac{b}{2}$；若 $\delta_{\sigma-1(m)}=0$，那么 $S\leq N_0+N_1+\cdots+N_{m-1}+\frac{b}{2}$. 因为 $N_m>\sum_{i=0}^{m-1}N_i+b_i$，用 $S_1=S-\delta_{\sigma-1(m)}N_m$ 代替原来的 S，重复这一过程直到得到 $\delta_{\sigma-1(i)}$. 使用秘密的置换，得到明文 $\delta_0,\cdots,\delta_m$.

在 Cai-Cusick 密码体制中的 $m+1=O(N)$ 位明文是加密的密文 n 维向量，而不是仅仅一个比特的明文.

在 2011 年 3 月，《IEEE Transactions on Information Theory》刊登了中国国家数学与交叉科学中心潘彦斌和邓映蒲关于 Cai-Cusick 格密码体制的论文，其审稿意见认为该密码体制已被完全攻破. 潘彦斌和邓映蒲给出了它的一个唯密文攻击，时间复杂性是多项式的，从而彻底攻破了该存在有十多年的密码体制.

6　展　望

目前，虽然出现了一些量子算法，但是量子计算的理论研究还很不充分. 现有的量子算法应用于解决经典可计算问题，而对于不可计算问题在量子环境下却没有进行充分讨论，如停机问题. Kieu 考虑了量子可计算性的概念，并且借助量子连续变量和量子绝热演化，提出了一个解决 Hilbert 第 10 问题(停机问题的一个等价问题)的量子算法. Calude 和 Pavlov 在数学意义上构造了一个解决有无穷多堆硬币情况下的零售商问题(停机问题的一个等价问题)的量子设备. 如果算法在物理上能够实现，则量子计算为解决经典的不可计算问题提供了新的方

法[149-150].这将对计算科学和密码学产生巨大的影响.

Bernstein 和 Vazirani 指出 Deustch 算法感兴趣的是可计算性问题而不是计算复杂性.但是,Deustch 认为,他所构造的通用量子图灵机模型并不能计算非递归函数,即他构造的模型在计算能力上不与 Church-Turing 论题矛盾[151].而以后提出的 QTM 直接或间接地建立在 Deustch 提出的量子图灵机模型的基础上.这说明,从现有的 QTM 的角度不可能突破 Church-Turing 论题.考虑新的 QTM,可能对这个问题有帮助.Etesi 等人从另外的角度告诉我们,对量子可计算理论的研究,似乎应该从数学,物理学甚至更多不同学科的角度去研究[152].

目前广泛使用的公钥密码 RSA、ELGamal、ECC 等分别依赖于大整数质因子分解,离散对数问题,椭圆曲线上的离散对数问题.然而在量子计算机上求解这些问题存在多项式时间量子算法.量子计算机的发展,将对这些公钥密码体制构成严重的威胁.量子计算复杂性理论有助于我们构造一些抗量子密码,进而确保量子计算环境下的密码安全.尽管量子计算复杂性理论在理论方面取得了一定的研究成果,但是,人们对量子计算的复杂性以及量子计算机实现的研究还处于初级阶段,还有许多问题有待更深入的研究.

关于量子计算求解 NPC 问题有一个有趣的观点,量子计算可以被看作格局叠加态上的许多线性算子.若量子计算机采用非线性时间演化,则能够在多项式时间求解 NPC 问题.文献[153]采用非线性量子逻辑门,给出了求解 NPC 问题的一个量子算法.文中证明,若量子计算机能够用非线性算子设计格局叠加态上的算子,则能够在多项式时间求解 NPC 问题.这也是一个十分重要的问题,如果这个问题能够得到正面的解决将对密码学产生致命的影响.现在被认为是抗量子计算的密码都将受到挑战.

另外,在图理论和组合理论中某些著名的 NP 问题存在量子算法[154].这些量子算法至少相对于经典算法是加速的.量子计算机是否能在多项式时间内求解所有的 NP 类问题呢?在量子算法方面,自 Shor 因子分解和 Gover 搜索算法提出后,虽然各国众多的研究者在该领域进行了大量的研究.但目前,还没有发现其他解决经典问题的新量子算法.在量子问题复杂性关系,及其与古典问题复杂性关系方面,还有许多不确定包含关系.如 NPC 与 QP、BQP 的关系?三个复杂类 NQP、EQP 和 BQP 中有两个是相同的吗?等等.

由于量子算法的出现,使得在经典计算下的 P 类问题在量子环境下仍是容易求解的,即 $P\subseteq QP$.一些在经典计算下是困难的问题,譬如大整数分解和离散对数问题等,在量子计算下是容易求解的.而另外一些 NP 类问题即使在量子计算下仍然是困难的.在第 4 节我们介绍了 NP 问题在量子环境下的模拟定义分为两类,NQP 和 QMA.但它们并不是最困难的问题分类,从关系图 4 中看到在它们之上还有 PP,QMA(2)等问题分类.如果我们把量子模拟的 NQP 和 QMA 问题作为困难问题对待,就像 NP 类问题在经典计算中的作用一样,那么我们可以看到 NEXP 类问题即使在量子环境下也是困难的.Plandowski 在 1999 年证明了带有常数的字方程式可满足性问题是 NEXPTIME 困难的,而 NEXP 也被称作 NEXPTIME 的[155].这样的问题还有其他的定义.这对设计抗量子计算的密码而言是一个好消息.从而设计者可以在经典环境下选择更困难的问题设计抗量子计算的密码.关系图 4 有利于对困难问题的理解和密码的设计.这是基于对问题复杂性做出的分析.另一方面,从算法复杂性的角度考虑.根据我们提出的数据复杂性定义,如果某个计算任务需要处理的数据量规模等价于计算布尔函数的数据量 $O(2^{2^n})$,那么该计算任务是不能完成的,即使是在量子计算环境下.这也为设计抗量子计算的密码提供了一种新的思路[111].

当今互联网信息化时代,各个国家都十分重视密码学的理论和技术研究.目前流行的公钥体制主要包括基于大整数分解问题的 RSA 和基于椭圆曲线上离散对数问题的公钥体制,即 ECC.这些体制有一个共同的弱点,即不能抵抗量子攻击.因此,一旦实用的量子计算机出现,这些体制将可能被攻破,从而被淘汰.而且随着计算机技术的飞速发展,这些体制也逐渐遭受一些新的威胁.因此,寻找新的公钥体制,特别是能抵抗量子攻击的公钥体制,便成为一件重要而迫切的工作.

量子计算复杂性理论的发展为设计实际应用的公钥密码奠定基础.此外,设计能够走向实际应用的抗量子计算的公钥密码也是密码学的一个关键技术.而格密码被认为是后量子时代最主要的公钥体制代表之一,它以能抵抗量子攻击、平均安全性可以建立在格问题最坏情况复杂性及快速的加解密速度等优点受到了广泛的关注.

现有的研究表明,还没有出现有效的量子算法

解决格上的困难问题.目前最好的结果都需要指数级的资源消耗,并且能够走向实际应用的公钥密码不多.这都需要进一步的研究.

参 考 文 献

[1] Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 1992, 439 (1907): 553-558

[2] Simon D. On the power of quantum computation//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, 1994: 116-123

[3] Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters, 1997, 79(2): 325-328

[4] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5): 1484-1509

[5] Mosca M, Ekert A. The hidden subgroup problem and eigenvalue estimation on a quantum computer//Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication. California, USA, 1999: 174-188

[6] Hallgren S, Russell A, Ta-Shma A. The hidden subgroup problem and quantum computation using group representations. SIAM Journal on Computing, 2003, 32(4): 916-934

[7] Schack R. Using a quantum computer to investigate quantum chaos. Physical Review A, 1998, 57(3): 1634-1635

[8] Terraneo M, Georgeot B, Shepelyansky D L. Strange attractor simulated on a quantum computer. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, 2003, 22(1): 127-130

[9] Schindler P, Müller M, Nigg D, et al. Quantum simulation of dynamical maps with trapped ions. Nature Physics, 2013, 9(6): 361-367

[10] Munhoz P P, Semiao F L. Multipartite entangled states with two bosonic modes and qubits. The European Physical Journal D, 2010, 59(3): 509-519

[11] Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information and Computation, 2003, 3(4): 317-344

[12] Zhang Huan-Guo, Guan Hai-Ming, Wang Hou-Zhen. Research on the quantum cryptography system. China's Cryptography Development Report 2010. Changsha: Electronic Industry Press, 2011: 1-31(in Chinese)
(张焕国,管海明,王后珍. 抗量子密码体制的研究现状. 中国密码学发展报告 2010. 长沙:电子工业出版社, 2011: 1-31)

[13] Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography. New York, USA: Springer-Verlag, 2004

[14] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalor, India, 1984: 10-12

[15] Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 1993, 70(13): 1895

[16] Bennett C H, DiVincenzo D P, Smolin J A, et al. Mixed-state entanglement and quantum error correction. Physical Review A, 1996, 54(5): 3824

[17] Leung D W. Quantum vernam cipher. Physics, 2000, 2(1): 14-34

[18] Shi J J, Shi R H, Guo Y, et al. Batch proxy quantum blind signature scheme. Science China Information Sciences, 2013, 56(5): 1-9

[19] Xiao F Y, Chen H W. Construction of minimal trellises for quantum stabilizer codes. Science China Information Sciences,2013, 56(1): 1-11

[20] Gehani A, LaBean T H, Reif J H. DNA-Based Cryptography. DNA Based Computers V. Providence, USA: American Mathematical Society, 2000

[21] Lu Mingxin, Lai Xuejia, Xiao Guozhen, et al. A symmetric key cryptography with DNA technology. Science in China Series F: Information Sciences, 2007, 50(3): 324-333

[22] Lai Xuejia, Lu Mingxin, Qin Lei, et al. Asymmetric encryption and signature method with DNA technology. Science China: Information Sciences, 2010, 53(3): 506-514

[23] Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems//Bellare M ed. Advances in Cryptology—CRYPTO 2000. Berlin: Springer, 2000: 147-165

[24] Bernstein D J, Buchmann J, Dahmen E. Post-Quantum Cryptography. New York: Springer-Verlag, 2000

[25] Wang H Z, Zhang H G, Wang Z Y, et al. Extended multivariate public key cryptosystems with secure encryption function. Science China Information Sciences, 2011, 54(6): 1161-1171

[26] Mu L W, Liu X C, Liang C L. Improved construction of LDPC convolutional codes with semi-random parity-check matrices. Science China Information Sciences, 2014, 57(2): 1-10

[27] Heckey J, Patil S, Javadiabhari A, et al. Compiler management of communication and parallelism for quantum computation. ACM Sigplan Notices, 2015, 50: 445-456

[28] Perez-Garcia B, Francis J, Mclaren M, et al. Quantum computation with classical light: The Deutsch Algorithm. Physics Letters A, 2015, 379(s28-29): 1675-1680

[29] Cheung D, Maslov D, Mathew J, et al. On the design and optimization of a quantum polynomial-time attack on elliptic curve cryptography//Kawano Y, Mosca M eds. Theory of Quantum Computation, Communication, and Cryptography. Berlin: Springer, 2008: 96-104

[30] Peev M, Nölle M, Maurhardt O, et al. A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography. International Journal of Quantum Information, 2005, 3(1): 225-231

[31] Krovi H, Russell A. Quantum Fourier transforms and the complexity of link invariants for quantum doubles of finite groups. Communications in Mathematical Physics, 2015, 334(2): 743-777

[32] Jozsa R. Classical simulation and complexity of quantum computations//Ablayev F, Mayr E W eds. Computer Science Theory and Applications. Berlin Heidelberg: Springer-Verlag, 2010: 252-258

[33] Diao Z, Zubairy M S, Chen G. A quantum circuit design for Grover's algorithm. Zeitschrift Für Naturforschung A, 2014, 57(8): 701-708

[34] Zheng S, Qiu D. From quantum query complexity to state complexity//Calude C S, Freivalds R, Kazuo I eds. Computing with New Resources. Switzerland: Springer International Publishing, 2014: 231-245

[35] Yan C, Xu C X, Zhang S B, et al. Quantum secure direct communication and authentication protocol with single photons. Chinese Science Bulletin, 2013, 58(36): 4571-4576

[36] Feynman R P. Simulating physics with computers. International Journal of Theoretical Physics, 1982, 21(6-7): 467-488

[37] Deutsch D. Quantum theory, the church-turing principle and the universal quantum computer. Royal Society, 1985, 400(1818): 97-117

[38] Bernstein E, Vazirani U. Quantum complexity theory// Proceedings of the 25th Annual ACM Symposium on Theory of Computing. New York, USA, 1993: 11-20

[39] Yimsiriwattana A, Lomonaco Jr S J. Distributed quantum computing: A distributed Shor algorithm//Defense and Security. International Society for Optics and Photonics, 2004: 360-372

[40] Dash T, Nayak T. Comparative analysis on turing machine and quantum turing machine. Journal of Global Research in Computer Science, 2012, 3(5): 51-56

[41] Bennett C H, Bernstein E, Brassard G, et al. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 1997, 26(5): 1510-1523

[42] Ohya M, Volovich I V. New quantum algorithm for studying NP-complete problems. Reports on Mathematical Physics, 2003, 52(1): 25-33

[43] Iriyama S, Ohya M. On generalized quantum turing machine and its applications. Open Systems & Information Dynamics, 2004, 16(2-3): 195-204

[44] Ohya M, Volovich I V. Quantum computing and the chaotic amplifier. Journal of Optics B Quantum and Semiclassical Optics, 2003, 5(6): 639-642

[45] Yamakami T. A foundation of programming a multi-tape quantum turing machine//Kutylowski M, Pacholski L, Wierzbicki T eds. Mathematical Foundations of Computer Science 1999. Berlin Heidelberg: Springer-Verlag, 1999

[46] Ozawa M, Nishimura H. Local transition functions of quantum Turing machines. RAIRO-Theoretical Informatics and Applications, 2000, 34(05): 379-402

[47] Carpentieri M. On the simulation of quantum turing machines. Theoretical Computer Science, 2003, 304(1): 103-128

[48] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Washington, USA, 1994: 124-134

[49] Spakowski H, Thakur M, Tripathi R. Quantum and classical complexity classes: Separations, collapses, and closure properties. Lecture Notes in Computer Science, 2003, 200(1): 1-34

[50] Fortnow L, Rogers J. Complexity limitations on quantum computation. Journal of Computer and System Sciences, 1999, 59(2): 240-252

[51] Lm A, Huang M, Demarrais J. Quantum computability. SIAM Journal on Computing, 1997, 26(5): 1524-1540

[52] Janzing D, Wocjan P, Zeier R, et al. Thermodynamic cost of reliability and low temperatures: Tightening landauer's principle and the second law. International Journal of Theoretical Physics, 2000, 39(12): 2717-2753

[53] Tanaka Y. Exact non-identity check is NQP-complete. International Journal of Quantum Information, 2010, 8(5): 807-819

[54] Fenner S, Green F, Homer S, et al. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. Proceedings of the Royal Society A, 1999, 455(1991): 3953-3966

[55] Kitaev A Y, Shen A H, Vyalyi M N. Classical and quantum computation. American Mathematical Monthly, Boston, MA, USA, 2003: 110-257

[56] Beigi S, Shor P W. On the complexity of computing zero-error and Holevo capacity of quantum channels. Quantum Physics, 2007

[57] Kobayashi H, Matsumoto K, Yamakami T. Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur//Proceedings of the 14th International Symposium. Kyoto, Japan, 2003: 189-198

[58] Moore C, Nilsson M. Parallel quantum computation and quantum codes. SIAM Journal on Computing, 2002, 31(3): 799-815

[59] Fenner S, Fortnow L, Kurtz S. Gap-definable counting classes. Journal of Computer and System Sciences, 1994, 48(1): 116-148

[60] Fenner S A. PP-lowness and a simple definition of AWPP. Theory of Computing Systems, 2003, 36(2): 199-212

[61] Kobler J, Schoning U, Torán J. Graph isomorphism is low for PP. Computational Complexity, 1992, 2(4): 301-330

[62] Spakowski H, Tripathi R. Degree bounds on polynomials and relativization theory//Levy J-J, Mayr E W, Mitchell J C eds. Exploring New Frontiers of Theoretical Informatics. Springer US, 2004: 97-110

[63] Aaronson S. Quantum computing, postselection, and probabilistic polynomial-time. Proceedings of the Royal Society of London A Mathematical Physical and Engineering Sciences, 2005, 461(2063): 3473-3482

[64] Aharonov D, Naveh T. Quantum NP—A survey. Physics, 2002

[65] Morimae T, Nishimura H. Quantum interpretations of AWPP and APP. Computer Science, 2015

[66] Aharonov D, Ta-Shma A. Adiabatic quantum state generation and statistical zero knowledge//Proceedings of the 35th Annual ACM Symposium on Theory of Computing. New York, USA, 2003: 20-29

[67] Aaronson S, Bouland A, Fitzsimons J, et al. The space "just above" BQP//Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science. Cambridge, USA, 2016: 271-280

[68] Watrous J. Quantum computational complexity//Meyers R A ed. Encyclopedia of Complexity and Systems Science. New York: Springer-Verlag, 2008: 7174-7201

[69] Jain R, Ji Z, Upadhyay S, et al. QIP=PSPACE. Journal of the ACM, 2011, 58(6): 30-58

[70] Jain R, Watrous J. Parallel approximation of non-interactive zero-sum quantum games//Proceedings of the Annual IEEE Conference on Computational Complexity. Paris, France, 2008: 243-253

[71] Beigi S, Shor P, Watrous J. Quantum interactive proofs with short messages. Theory of Computing, 2010: 101-117

[72] Deutsch D. Quantum computational networks. Proceedings of the Royal Society A Mathematical Physical and Engineering Sciences, 1989, 425(1868): 73-90

[73] Yao C C. Quantum circuit complexity//Proceedings of the 34th Symposium on Foundations of Computer Science. Palo Alto, USA, 1993: 352-361

[74] Juliá-Díaz B, Burdis J M, Tabakin F. QDENSITY—A mathematica quantum computer simulation. Computer Physics Communications, 2006, 174(11): 914-934

[75] Kempe J, Vidick T. Quantum algorithms//Benatti F, Fannes M, Floreanini R, Petritis D eds. Quantum Information, Computation and Cryptography. Berlin Heidelberg: Springer-Verlag, 2010: 309-342

[76] Gerdt V P, Prokopenya A N. The circuit model of quantum computation and its simulation with mathematica//Adam G, Buša J, Hnatič M eds. Mathematical Modeling and Computational Science. Berlin Heidelberg: Springer-Verlag, 2012: 43-55

[77] Childs A M, Leung D W, Nielsen M A. Unified derivations of measurement-based schemes for quantum computation. Physical Review A, 2005, 71(3): 032318

[78] Daskin A, Grama A, Kais S. A universal quantum circuit scheme for finding complex eigenvalues. Quantum Information Processing, 2014, 13(2): 333-353

[79] Pan J, Cao Y, Yao X, et al. Experimental realization of quantum algorithm for solving linear systems of equations. Physical Review A, 2013, 89(2): 1150-1154

[80] Alfailakawi M, Ahmad I, Alterkawi L, et al. Depth optimization for topological quantum circuits. Quantum Information Processing, 2014, 14(2): 447-463

[81] Wu Wan-Qing, Zhang Huan-Guo, Mao Shao-Wu, Wang Hou-Zhen. Quantum algorithm to find invariant linear structure of MD hash functions. Quantum Information Processing, 2015, 14(3): 813-829

[82] Wang Dong, Chen Han-Wu, Zhu Wan-Ning, et al. Unitary matrix of multiple-valued quantum purmutation gate. Chinese Journal of Computers, 2012, 35(3): 639-644 (in Chinese)
(王冬，陈汉武，朱皖宁等. 多值逻辑量子置换门的酉矩阵表示. 计算机学报，2012, 35(3): 639-644)

[83] Wu Wan-Qing, Zhang Huan-Guo, Wang Hou-Zhen, Mao Shao-Wu. Polynomial-time quantum algorithms for finding the linear structures of Boolean function. Quantum Information Processing, 2015, 14(4): 1215-1226

[84] Bennett C H. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 1992, 69(20): 2881-2884

[85] Braunstein S L, Kimble H J. A posteriori teleportation. Nature, 1998, 394(6696): 840-841

[86] Ohya M, Masuda N. NP problem in quantum algorithm. Open Systems & Information Dynamics, 2000, 7(1): 33-39

[87] Iriyama S, Ohya M. Generalized quantum turing machine and its use to find an algorithm solving NP-complete problem //Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies. Rome, Italy, 2010: 1-5

[88] Cleve R. The query complexity of order-finding. Information and Computation, 2004, 192(2): 162-171

[89] Harrow A W, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Physical Review Letters, 2009, 103(15): 150502

[90] Laarhoven T, Mosca M, van de Pol J. Solving the shortest vector problem in lattices faster using quantum search//Gaborit P ed. International Workshop on Post-Quantum Cryptography. Berlin: Springer, 2013: 83-101

[91] Patarin J. Generic Attacks on Feistel Schemes//Boyd C ed. Advances in Cryptology-ASIACRYPT 2001. Berlin Heidelberg: Springer-Verlag, 2001: 222-238

[92] Buhrman H, Spalek R. Quantum Verification of Matrix Products. Philadelphia, USA: ACM Press, 2004: 880-889

[93] Bao W S, Song Z, Zhong P C, et al. Quantum mechanical meet-in-the-middle algorithm for subset sum problem. Acta Electronica Sinica, 2011, 39(1): 128-132

[94] Regev O. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space//Proceedings of the Annual Symposium on the Foundations of Computer Science. Philadelphia, USA, 2004: 124-134

[95] Wu Wan-Qing, Zhang Huan-Guo, Mao Shao-Wu, et al. A public key cryptosystem based on data complexity under quantum environment. Science China Information Sciences. 2015, 58(11): 1-11

[96] Du Ding-Zhu, Ge Ke-Yi, Wang Jie. Introduction to Computational Complexity. Beijing: Higher Education Press, 2002

[97] Cleve R. An introduction to quantum complexity theory. Collected Papers on Quantum Computation and Quantum Information Theory, 1999, 26(5): 103-127

[98] Meyers R E, Deacon K S, Tunick A. Space-time quantum imaging//Proceedings of the SPIE 2013. London, UK, 2013: 1508-1534

[99] Loepp S, Wootters W K. Protecting Information: From Classical Error Correction to Quantum Cryptography. New York, USA: Cambridge University Press, 2006

[100] Vedral V, Barenco A, Ekert A. Quantum networks for elementary arithmetic operations. Physical Review, 1996, 54(1): 147-153

[101] Wu Kun, Ma Lei. Study on construction of quantum full-summator. Chinese Journal of Quantum Electronics, 2004, 21(1): 27-30(in Chinese)
(吴昆, 马雷. 量子全加器构造的探讨. 量子电子学报, 2004, 21(1): 27-30)

[102] Takahashi Y, Kunihiro N. A quantum circuit for Shor's factoring algorithm using $2n+2$ qubits. Quantum Information and Computation, 2006, 6(2): 184-192

[103] Beauregard S. Circuit for Shor's algorithm using $2n+3$ qubits. Quantum Information and Computation, 2003, 3(2): 175-185

[104] Pavlidis A, Gizopoulos D. Fast quantum modular exponentiation architecture for Shor's factoring algorithm. Quantum Information and Computation, 2014, 14(7-8): 649-682

[105] Fu X Q, Bao W S, Zhou C. Speeding up implementation for Shor's factorization quantum algorithm. Chinese Science Bulletin, 2010, 55(32): 3648-3653

[106] Fu Xiang-Qun, Bao Wan-Su, Zhou Chun, et al. t-bit semi-classical quantum Fourier transform. Chinese Science Bull, 2011, 56(26): 2250-2255(in Chinese)
(付向群, 鲍皖苏, 周淳等. t 比特半经典量子 Fourier 变换. 科学通报, 2011, 56(26): 2250-2255)

[107] Politi A, Matthews J C F, O'Brien J L. Shor's quantum factoring algorithm on a photonic chip. Science, 2009, 325(5945): 1221

[108] Crespi A, Ramponi R, Osellame R, et al. Integrated photonic quantum gates for polarization qubits. Nature Communications, 2011, 2(10): 193-198

[109] Barz S, Kashefi E, Broadbent A, et al. Demonstration of blind quantum computing. Science, 2012, 335(6066): 303-308

[110] Ukai R, Iwata N, Shimokawa Y, et al. Demonstration of unconditional one-way quantum computations for continuous variables. Physical Review Letters, 2011, 106(24): 240504

[111] Zhang Yi, Lu Kai, Gao Ying-Hui. Quantum algorithm and quantum inspired algorithms. Chinese Journal of Computers, 2013, 36(9): 1835-1842(in Chinese)
(张毅, 卢凯, 高颖慧. 量子算法与量子衍生算法. 计算机学报, 2013, 36(9): 1835-1842)

[112] Wang Yu-Ping, Li Ying-Hua. A novel quantum genetic algorithm for TSP. Chinese Journal of Computers, 2007, 30(5): 748-755(in Chinese)
(王宇平, 李英华. 求解 TSP 的量子遗传算法. 计算机学报, 2007, 30(5): 748-755)

[113] Wang S, Song X, Niu X. Quantum cosine transform based watermarking scheme for quantum images. Chinese Journal of Electronics, 2015, 24(2): 321-325

[114] Crowley P J D, Duric T, Vinci W, et al. Quantum and Classical in Adiabatic Computation. Physical Review A, 2014, 90(4): 1-9

[115] Aharonov D, Van Dam W, Kempe J, et al. Adiabatic quantum computation is equivalent to standard quantum computation. SIAM Review, 2008, 50(4): 755-787

[116] Schnorr C P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming, 1994, 66(1-3): 181-199

[117] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009, 56(6): 84-93

[118] Goldreich O, Goldwasser S, Halevi S. Eliminating decryption errors in the Ajtai-Dwork cryptosystem//Kaliski Jr B S ed. Advances in Cryptology. Lecture Notes in Computer Science 1294. Berlin Heidelberg: Springer-Verlag, 1997: 105-111

[119] Nguyen P Q, Stern J. The two faces of lattices in cryptology //Silverman J H ed. Cryptography and Lattices. LNCS 2146. Berlin Heidelberg: Springer-Verlag, 2001: 146-180

[120] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems//Kaliski Jr B S ed. Advances in Cryptology—CRYPTO'97. Berlin Heidelberg: Springer-Verlag, 1996: 112-131

[121] Micciancio D. Improving lattice based cryptosystems using the hermite normal form//Silverman J H ed. Cryptography and Lattices. Berlin Heidelberg: Springer-Verlag, 2001: 126-145

[122] Babai L. On Lovasz lattice reduction and the nearest lattice point problem. Combinatorica, 1986, 6(1): 1-13

[123] Hostein J, Pipher J, Silverman J. NTRU: A new high speed public key cryptosystem//Buhler J P ed. Algorithmic Number Theory (ANTS III). Lecture Notes in Computer

Science 1423. Berlin Heidelberg: Springer-Verlag, 1998: 267-288

[124] Regev O. New lattice based cryptographic constructions. Journal of the ACM, 2004, 51(6): 899-942

[125] Aharonov D, Regev O. A lattice problem in quantum NP// Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS'03). Washington, USA, 2003: 210-219

[126] Aharonov D, Regev O. Lattice problems in NP ∩ coNP. Journal of the ACM, 2004, 5(5): 362-371

[127] Regev O. Quantum computation and lattice problems. SIAM Journal on Computing, 2003, 33(3): 520-529

[128] Laarhoven T, Mosca M, Pol J V D. Finding shortest lattice vectors faster using quantum search. Designs Codes and Cryptography, 2015, 77(2-3): 1-26

[129] Micciancio D, Voulgaris P. Faster exponential time algorithms for the shortest vector problem. Electronic Colloquium on Computational Complexity, 2010, 16: 1468-1480

[130] Nguyen P Q, Vidick T. Sieve algorithms for the shortest vector problem are practical. Journal of Mathematical Cryptology, 2008, 2(2): 181-207

[131] Wang X, Liu M, Tian C, et al. Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem// Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. Hong Kong, China, 2011: 1-9

[132] Laarhoven T, Weger B D. Faster sieving for shortest lattice vectors using spherical locality-sensitive hashing//Lauter K, Rodríguez-Henríquez F eds. Progress in Cryptology-LATINCRYPT 2015. Switzerland: Springer International Publishing, 2015: 101-118

[133] Becker A., Laarhoven T. Efficient sieving in (ideal) lattices using cross-polytopic LSH. International Association for Cryptologic Research, 2015: 823-849

[134] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Journal of the ACM, 2013, 60(6): 3-18

[135] Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence//Proceedings of the 29th Annual ACM Symposium on Theory of Computing. New York, USA, 1997: 284-293

[136] IEEE. P1363.1 Public-Key Cryptographic Techniques Based on Hard Problems over Lattices, June 2003

[137] Silverman J H. Almost inverses and fast NTRU key creation. Katholieke University Leoven, Netherlands: Technical Report 014, 1999

[138] Jaulmes E, Joux A. A choosen-ciphertext attak against NTRU//Bellare M ed. Advances in Cryptology-CRYPTO 2000. Berlin: Springer-Verlag, 2000: 20-35

[139] Han D, Hong J, Han J W, et al. Key recovery attacks on NTRU without ciphertext validation routine//Proceedings of the 8th Australasian Conference on Information Security and Privacy. Wollongong, Australia, 2003: 274-284

[140] Howgrave-Graham N, Nguyen P Q, Pointcheval D, Proos J, et al. The impact of decryption failures on the security of NTRU encryption//Boneh D ed. Advances in Cryptology-CRYPTO 2003. Berlin Heidelberg: Springer-Verlag, 2003: 226-246

[141] Yao Jun, Zeng Guihua. Enhanced NTRU cryptosystem eliminating decryption failures. Journal of Systems Engineering and Electronics, 2006, 17(4): 890-895

[142] Hoffstein J, Silverman J. Optimizations for NTRU. In Publickey Cryptography and Computational Number Theory. Berlin, Germany: American Mathematical Society, 2000: 11-15

[143] Banks W D, Shparlinski I E. A variant of NTRU with non-invertible polynomials//Menezes A, Sarkar P eds. Progress in Cryptology-INDOCRYPT 2002. Berlin Heidelberg: Springer-Verlag, 2002: 62-70

[144] Coglianese M, Goi B M. MaTRU: A new NTRU-based cryptosystem//Maitra S, Madhavan C E V, Venkatesan R eds. Progress in Cryptology-INDOCRYPT 2005. Berlin Heidelberg: Springer-Verlag, 2005: 232-243

[145] Chi Y W, Hua M X, Ke H D. Study on NTRU decryption failure. Journal of the China Railway Society, 2005, 2: 454-459

[146] Xu J, Hu L, Sun S, et al. Cryptanalysis of countermeasures against multiple transmission attacks on NTRU. IET Communications, 2014, 8(12): 2142-2146

[147] Ajtai M. Representing hard lattices with $O(n \log n)$ bits// Proceedings of the 37th Annual ACM Symposium on Theory of Computing. New York, USA, 2005: 94-103

[148] Cai J Y, Cusick T W. A lattice-based public-key cryptosystem. Information and Computation, 1998, 151(1-2): 17-31

[149] Calude C S, Pavlov B. Coins, quantum measurements, and Turing's barrier. Quantum Information Processing, 2002, 1(1-2): 107-127

[150] Kieu T D. Quantum algorithm for Hilbert's tenth problem. International Journal of Theoretical Physics, 2003, 42(7): 1461-1478

[151] Miszczak J. Models of quantum computation and quantum programming languages. Bulletin of the Polish Academy of Sciences: Technical Sciences, 2011, 59(3): 305-324

[152] Etesi G, Németi I. Non-Turing computations via Malament-Hogarth space-times. International Journal of Theoretical Physics, 2002, 41(2): 341-370

[153] Abrams S, Lloyd S. Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. Physics Review Letter, 1998, 81(18): 3992-3995

[154] Guo H, Long G L, Li F. Quantum algorithms for some well-known NP problems. Communications in Theoretical Physics, 2002, 37(4): 424-426

[155] Plandowski W. Satisfiability of word equations with constants is in NEXPTIME//Proceedings of the Annual ACM Symposium on Theory of Computing. New York, USA, 1999: 721-725

ZHANG Huan-Guo, born in 1945, professor. His research interests include information security, cryptography, trusted computing, etc.

MAO Shao-Wu, born in 1986, Ph. D. candidate. His research interests include information security, cryptography.

WU Wan-Qing, born in 1981, Ph. D. candidate. His research interests include information security and quantum cryptography.

WU Shuo-Mei, born in 1977, lecturer. Her research interest is computer cryptography.

LIU Jin-Hui, born in 1989, Ph. D. candidate. Her research interests include information security, cryptography.

WANG Hou-Zhen, born in 1981, lecturer. His research interests include information security, cryptography.

JIA Jian-Wei, born in 1988, Ph. D. candidate. His research interests include information security, cryptography.

Background

This work is supported by the National Natural Science Foundation of China of China (Nos. 61303212, 61202386), the State Key Program of National Natural Science of China (No. 61332019), and the National Basic Research Program (973 Program) of China (No. 2014CB340600).

The project is a quantum computation complexity review. It has theoretical significance for designing post quantum computation public key cryptosystems. Many researchers have been taking the deep work about quantum complexity, and these results are scattered in many papers. In this paper we make a summary of the quantum computation complexity theory. Various quantum Turing machine models and the relationship between them are introduced, and the quantum circuit model and the quantum Turing machine are compared with each other. Quantum computing complexity is discussed in detail, including quantum algorithm complexity, the complexity of the problem and the quantum circuit complexity. Especially this paper proposes a new quantum computation data complexity. Finally, some important issues worth studying in the future and the design and analysis of cryptosystems under quantum computation environment are outlooked.