密码体制的量子算法分析*)

吕 欣[1] 冯登国[1,2]

(中国科学院研究生院信息安全国家重点实验室 北京100039)[1]

(中国科学院软件所信息安全国家重点实验室 北京100080)[2]

摘 要 很多快速量子算法都可以归结为隐子群问题的讨论,本文回顾了隐子群问题量子算法的基本思想,分析了群上量子算法的优越性。分析了可以归结为隐子群问题的公钥密码体制,描述了求解椭圆曲线上离散对数问题的量子算法,讨论了隐子群问题量子算法的局限性。

关键词 量子计算,量子密码,隐子群,量子傅里叶变换

Quantum Analysis of Modern Cryptosystems

LU Xin[1] FENG Deng-Guo[1,2]

(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Bejing 100039)[1]

(State Key Laboratory of Information Security, Institute of Software of Chinese Academy of Sciences, Bejing 100080)[2]

Abstract Many fast quantum algorithms, which cannot be solved efficiently by classical probabilistic algorithms, can be reduced to the discussion of hidden subgroup problems. The quantum algorithms of hidden subgroup problems are reviewed and the advantages of quantum algorithm over group are analyzed in the paper. This paper surveys the modern cryptosystems that can be broken by quantum hidden subgroup algorithms in polynomial time. Limits of the hidden subgroup problems quantum algorithms are also discussed.

Keywords Quantum computation, Cryptanalysis, Hidden subgroup, Quantum fourier transform

1 介绍

量子计算是量子力学与计算机科学相交叉的学科。近年来,在量子信息论、量子纠错、量子保密通信等方面都有很大的突破。量子信息学的研究对现代密码学有两方面的影响。一是快速量子算法对一些密码体制带来威胁。另一方面是量子密钥分配的研究给探索无计算假设的密码体制带来了新思路。本文主要讨论前一个方面的内容。

对量子计算的研究开始于20世纪80年代初。著名物理学家 Feynman 在1982年提出了普适量子模拟器的概念,并指出未来的量子计算机有可能会在某些方面优越于传统计算机。同时指出了用经典计算模型不能有效地模拟量子模型[1]。并预言量子计算可能会优越于现有的计算理论。Deutsch 描述了一个可以模拟任何有限的、可以实现的物理系统的量子计算模型—量子图灵机模型[2]和量子线路模型[3]。Andrew Yao 证明了 Deutsch 的量子图灵机与量子线路多项式计算的等价性[4],使研究人员可以用线路来描述量子算法。受 Simon[5]启发,Peter Shor 在1994年,给出了大整数分解和离散对数问题的多项式时间的量子算法[6],使部分经典计算的难题可以在量子计算机上以用多项式时间算法解决。因为这一算法对基于 RSA 的密码体制构成威胁,使得量子计算机引起人们空前关注。另一个著名的量子算法是 Glover 的量子搜索算法[7]。量子搜索算法并没有在指数上加速 NP 完全问题的求解,但其应用的广泛性同样很有意义。

现代密码体制是基于单向函数的存在性。单向函数是指满足下面条件的函数 $f:\{0,1\}^n\to\{0,1\}^m$:

1) 函数求解是容易的,即存在确定性多项式算法,输入 x,求 $f(x)$是容易实现的。

2) 求逆是困难的,即对于任何概率性多项式算法,求解 $f^{-1}(y)=x$ 是困难的。

许多公钥密码体制都是建立在单向函数存在性的基础之上的。例如:基于大整数分解的 RSA 公钥算法。而单向函数的选择范围在(NP-P)范围内(这里假设 $P\neq NP$)。

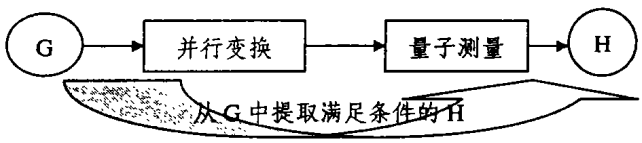

图1 量子算法的基本模型

研究表明[8,9],Deutsch 算法,Simon 算法,以及 Shor 的大整数分解和离散对数算法都可以归结为对隐子群问题的讨论。本文讨论的主要目的在于如何把一些现代密码体制归结为隐子群上问题,用量子算法进行分析。量子算法的优势在于能够同时对不同的态进行并行操作。而量子算法在群结构上的优势在于能够对群上具有不同性质的集合(陪集)进行并行处理,并能够通过做某种数学变换(常用到的是离散傅里叶变换),来巧妙地标记出所要找的集合 H。而 H 通常与 G 之间保持着很好的数学关系(见图1)。而并行变换通常是由某些并行码(如 Hadmard 变换)或傅里叶变换来实现。

2 量子傅里叶变换

傅里叶变换在经典信息处理中扮演着重要的角色,同样量子傅里叶变换也是很多快速量子算法的基础。

*)基金项目:本文得到国家重点基础研究发展规划973项目(G1999035802)和国家自然科学基金项目(60273027)的资助。吕 欣 博士研究生,研究方向为信息安全,量子密码与量子计算。冯登国 研究员,博士生导师,研究方向为网络信息安全与密码学。

定义1 给定一组正交基$|0\rangle,|1\rangle,\cdots,|2^n\rangle$，$N=2^n$。离散量子傅里叶变换定义为：

$$QDF(|x\rangle)\rightarrow\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\exp(2\pi ixy/N)|y\rangle \quad (1)$$

量子傅里叶反变换定义为：

$$QDF^{-1}(\sum_{y=0}^{N-1}\exp(2\pi iy\sigma)|y\rangle\rightarrow|\sigma\rangle \quad (2)$$

可以看出，用量子傅里叶反变换可以方便地估计相位$|\sigma\rangle$。当然这是以量子态可以测量的量子力学基本假设为依据的[7]。可以验证量子傅里叶变换为酉变换。

3 隐子群上的量子算法

3.1 函数求周期

基于文[9]的思想，一个函数$f(x)$是周期函数，如果满足：对于$\forall x$，存在最小的整数r，使得$f(x)=f(x+r)$，r称作$f(x)$的周期。求函数周期的问题是量子算法中最为重要的算法之一。设有酉变换U_f满足：$|x\rangle U_f|f(y)\rangle=|x\rangle|f(x+y)\rangle$

根据量子理论，设存在酉变换U和本征向量$|\xi\rangle$，如果存在复数u，使得$U|\xi\rangle=u|\xi\rangle$，$u$就称作$U$对于本征向量$|\xi\rangle$下的本征值。定义量子态：

$$|\xi_k\rangle=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp[-\frac{2\pi iks}{r}]|f(s)\rangle \quad (3)$$

容易验证$|\xi_k\rangle$是酉变换U_f的本征向量，$\exp[\frac{2\pi iks}{r}]$是对应的本征值，容易验证$U_f|\xi_k\rangle=\exp[\frac{2\pi ikx}{r}]|\xi_k\rangle$。

同时注意到：观察(3)式，当k等于零时，幅值有r个相同的解，求和后为1。当k等于零时，幅值有r个不同的解均匀分布在单位圆上，求和后相互抵消，结果为0。所以有$\sum_{k=1}^{r-1}|\xi_k\rangle=f(0)$，由于对$|\xi_k\rangle$不容易制备，因此可用$f(0)$来替代。

函数求周期算法步骤如下：

1) 初始化两个寄存器为：$|0\rangle|f(0)\rangle=\sum_{k=1}^{r-1}|0\rangle|\xi_k\rangle$

2) 对第一个寄存器执行QFT得：$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|\xi_k\rangle$

3) 执行第二个寄存器执行酉变换U_f得：$\frac{1}{\sqrt{N}}\sum_{k=0}^{r-1}(\sum_{x=0}^{N-1}\exp(2\pi ikx/r)|x\rangle)|\xi_k\rangle$

4) 对上式第一个寄存器执行量子傅里叶反变换，通过量子测量得到$\frac{k}{r}$的近似值。再通过数论中连分数的知识就可以求出r的值。有关连分数的概念请参阅文[8]。

3.2 群元素求阶

令有阶为N的群G，群上的二元运算已知。$a\in G$，求满足$a^r=1$的最小的r的问题就称为群元素求阶问题。群元素求阶是函数求周期问题的特例。在该算法中定义

$$|\xi_k\rangle=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp[-\frac{2\pi iks}{r}]|a^s\rangle_G \quad (4)$$

为酉算子U_a的本征向量，U_a满足$|x\rangle U_a|y\rangle=|x\rangle|a^xy\rangle$，相应的本征值为$\exp(2\pi ikx)$，同样有：$U|\xi_k\rangle=\exp[\frac{2\pi ikx}{r}]|\xi_k\rangle$

按照函数求周期量子算法的步骤就可以估计出r的值。要注意的是这里的运算x^k是群G上的运算。算法如下：

1) 初始化两个寄存器为$|0\rangle|1\rangle=|0\rangle\sum_{k=0}^{r}|\xi_k\rangle$

2) 对第一个寄存器执行QFT，机器状态变为：$\frac{1}{\sqrt{2^m}}\sum_{k=0}^{r-1}(\sum_{x=0}^{2^m-1}|x\rangle|\xi_k\rangle)$

因为现在不知道r的值，所以用$m>\log_2 r^2$，这里可选择$m=\log_2 N$。

3) 对第二个寄存器执行酉变换得：$\frac{1}{\sqrt{2^m}}(\sum_{x=0}^{2^m-1}\exp(2\pi ikx/r)|x\rangle)|\xi_k\rangle$

4) 对第一个寄存器执行QFT^{-1}得出$\frac{k}{r}$的近似值，在通过连分式计算得出r的值。

3.3 隐子群问题

定义2 G为一个有限群，H是G的子群。$(a_1G,a_2G,\cdots,a_nG)$称为G关于子群H的左陪集，n为群H的阶。X为一个集合，存在映射$f_i:G\rightarrow X$，$f_i(1<i<n)$是常数，并对于$i\neq j$有$f_i\neq f_j$。求这样的一个子群H的问题称之为隐子群问题。

根据群论的观点，陪集实质上是对一个群或说为一个集合的等价划分，把一个大集合划分为具有某种共同特性的小的集合。把对G的研究，转化为对比群G元素个数少得多的陪集的研究。而量子并行处理的特性与群上这种等价划分的结合，使得在经典计算机中的很多难题，在量子计算机上可以在多项式时间内解决。

4 可归结为隐子群问题的密码体制

4.1 大整数分解问题

根据数论知识大因子分解问题可以归结为整数模N群上求元素阶的问题[5,7]。设G是一个Z/Z_N的加群，定义$f:Z\rightarrow G$上的函数，$f(x)=a^x \bmod N$，a是群G元素，并且$\gcd(a,N)=1$，求最小的x使得，$a^x \bmod N=1$。

$X:\{x|a^x \bmod N=1,x\in Z\}$是满足$f(x)=1$所有的解的集合，这里$X=\{r,2r,\cdots,nr\}$是满足条件的解，实际上$X$是群$G$的一个子群。把问题归结为求群的子群的生成集加快了算法的速度。G通过陪集分解可划为如下若干个关于子群X的等价类，分别用$G_1,G_2,\cdots,G_r$表示：

$$G=\{g_0|g_0=ar,a\in Z\}\cup\{g_1|ar+1,a\in Z\}\cup\cdots\cup\{g_{r-1}|ar+(r-1)\}$$

求群元素阶的问题就转化为在$G_1,G_2,\cdots,G_r$中求G_r的生成集的问题。

对于上面问题，$f:Z\rightarrow G$是一个同态映射，$Ker(f)=\{x|a^x \bmod N=e_G\}$，求阶问题归结为求同态映射核的问题。

利用经典计算来分解大整数的现有的最快算法的计算复杂度为$\exp(c(n\log)^{1/2})$[10]，而用上述量子算法可以通过$O(n^3)$步操作实现。

4.1.1 可以归结为整数分解问题的密码体制

4.1.1.1 RSA公钥体制

RSA密码体制是典型的基于大因子分解问题的密码体制。并且有结论：RSA的破译难度不超过大数分解。Peter Shor[6]提出的量子算法的初衷就是为了解决这一应用广泛的公钥体制。这里不再赘述。

4.1.1.2 基于二次剩余的密码体制

概率公钥密码体制是相对于确定性公钥系统的，它是一类基于二次剩余问题的密码体制(如RSA)，其优点在于攻击者不能预先计算出某些明文对应的密文。二次剩余问题定义如下：令$Z_n^*=\{a\in Z_n|\gcd(a,n)=1,n=pq$，存在$x\in Z_n^*$，并且

$(\frac{x}{n})=1$，问 x 是否 mod n 是的二次剩余的问题。$(\frac{x}{n})$代表 x mod n 的 Jacobi 符号。

由数论的知识，知道 n 的分解或 n 本身就为一素数时，二次剩余问题很容易解决。所以说二次剩余问题并不比分解 n 困难。即二次剩余问题可以归结为大因子分解问题。

另外还有其他的密码体制，如 Rabin 密码体制。Rabin 体制是建立在求 $\phi(n)$的困难性之上的。而事实上，求 $\phi(n)$的难度与分解 n 相当。

4.2 离散对数问题

4.2.1 离散对数问题量子算法

已知阶为 N 的群 G，$a\in G$ 是群 G 的一个生成元，并且有 $a^r=1$，对于 $b=a^m$ 已知 a 求 b 在多项式时间内容易求出，已知 b 求 m 的问题称之为群 G 上的离散对数问题，认为是经典难题，记为 $m=\log_a b$。

定义式(4)为 U_a 和 U_b 共有的本征向量，其中 $|x\rangle U_a|y\rangle=|x\rangle|a^x y\rangle$，$|x\rangle U_b|y\rangle=|x\rangle|b^x y\rangle$，相应的本征值分别为 $\exp(2\pi ikx/r)$和 $\exp(2\pi ikmx/r)$。文[9]先利用量子求阶算法，求出 r。而后再执行 U_b 来估计(km/r)的值，这虽然使得计算复杂度降低，但很难保证两次计算中 k 值相同，使得算法很难实现。本文中，把两次测量合并为一次，虽然量子操作较文[9]增多了，但能有效地确定 k 的值，从而可以有效地估计 m，算法如下：

1) 初始化三个寄存器为$|0\rangle|0\rangle|1\rangle$

2) 设 $l=2\log_2 N$，对前两个比特执行 QFT 得：$\sum_{k=0}^{r-1}(\sum_{x=0}^{2^l-1}|x\rangle)(\sum_{y=0}^{2^l-1}|y\rangle)|\xi_k\rangle$

3) 分别对前两个寄存器执行有变换 U_a，U_b 得：

$$\sum_{k=0}^{r-1}(\sum_{x=0}^{2^l-1}\exp(2\pi ikx/r)|x\rangle)(\sum_{y=0}^{2^l-1}\exp(2\pi ikmy)|y\rangle)|\xi_k\rangle$$

4) 分别对前两个寄存器执行 QFT^{-1}得：(k/r)，(km/r)

5) 利用连分式运算计算出 $m \bmod \frac{r}{\gcd(k,c)}$的值

4.2.2 可以归结为离散对数问题的密码体制

4.2.2.1 Z/Z_n 循环群上的离散对数问题

ElGamal 公钥算法是建立在 Z_p(p 为一素数)上离散对数问题的算法。ElGamal 公钥算法$\{P,C,K\}$，$P=Z_p^*$ 是明文空间，$C=Z_p^*\times Z_p^*$ 是密文空间，$a\in Z_p^*$ 是一个本原元。$K=\{(p,a,a,\beta)|\beta\equiv a^a(\bmod p)\}$是密钥空间。公开 p,a,β，保密 a。详细的加解密过程见文[13]。从 ElGamal 体制的密钥构成可以看出，其实质是求 Z/Z_p 这个循环群上的离散对数问题，由 4.2.1的算法可以直接求出私钥 a。

4.2.2.2 椭圆曲线上的离散对数问题

椭圆曲线密码体制基于椭圆曲线上离散对数问题的难解性的。对于 Galois 域 GF(p)($P>3$)上的椭圆曲线 E，是满足下面方程的所有点$(x,y)(x,y\in GF(p))$的集合：

$$y^2=x^3+ax+b$$

并定义 E 上的无穷远点为 O，其中$4a^3+27b^2\neq 0$。

点集合对于下面的加法规则构成一个加群：

(1)$O+O=O$(2)$(x,y)+O=(x,y)$(3)$(x,y)+(x,-y)=0$

已知点 $K\in E$，定义对点 K 自身按上述加法规则加 n 次，其结果为 $G=nK$。在椭圆曲线上求点 $K\in E$ 的 n 次加法操作的运算可以用“重复加倍和加”方法来计算[13]。已知 G、K 求 n 的问题称之为椭圆曲线上的离散对数问题，被认为是经典难题。

类似于 Peter Shor 的离散对数量子算法，给出椭圆曲线上的离散对数算法如下：

对于 $A,B\in E$，设 $B=mA$，$rA=O$，椭圆曲线 E 满足上述定义。

令 $f(x_1,x_2)=x_1B-x_2A$，则有 $f[(x_1+k),x_2+ks]=f(x_1+x_2)$，$(k,km)$称为 $f(x_1,x_2)$的周期。

定义 $\xi_k=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp(-\frac{2\pi iks}{r})|sA\rangle$

为 U_A 和 U_B 共有的本征向量，其中 $|x\rangle U_A|y\rangle=|x\rangle|Axy\rangle$，$|x\rangle U_B|y\rangle=|x\rangle|Bxy\rangle$，相应的本征值分别为 $\exp(2\pi ikx/r)$和 $\exp(2\pi ikmx/r)$。

椭圆曲线上的离散对数问题量子分析算法如下：

1) 建立初始态$|0\rangle|0\rangle|0\rangle=\sum_{k=0}^{r-1}|0\rangle|0\rangle|\xi_k\rangle$

2) 第2)～6)步与4.2.1求离散对数的算法相同。最后可以利用连分式运算计算出 $m \bmod \frac{r}{\gcd(k,r)}$的值。

结论与展望 快速量子算法的研究对基于计算假设的密码体制提出了新的挑战，本文综述了可以归结为隐子群上量子算法的密码体制的分析方法。隐子群问题的核心是量子傅里叶变换，量子傅里叶变换也是迄今为止仅有的以指数速度优越于经典算法的工具。而可以利用傅里叶变换求解的问题也非常有限。是否存在其他在指数上优越于经典算法的量子算法，是今后量子算法研究的一个重要课题。另一方面，由于制备多个量子比特的机器，在技术上有很大的局限性，因此探索用尽量少的量子比特就可以实现量子算法也是今后的一个重点研究内容。

参 考 文 献

1 Feynman R P. Simulating Physics with computers. Appear in Feynman and Computation: Exploring the Limits of Computers. In: Anthony J G Hey ed. 1999

2 Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. In: Proc. of the Royal Society, London, vol. A400, 1985. 97～117

3 Deutsch D. Quantum computational networks. In: Proc. Roy. Soc. Lond. A 425, 1989. 73～90

4 Yao A. Quantum circuit complexity. In: Proc. of the 34th Annual IEEE Symposium on Foundations of Computer Science, 1993. 352～361

5 Simon D. On the power of quantum computation. In: Proc. of the 35th Annual IEEE Symposium on Foundations of Computer Science, 1994. 116～123

6 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

7 Grover L K. A fast quantum mechanical algorithm for database search. In: Proc. of 28th STOC, 1996. 212～219

8 Nielson M A, Chuang I L. Quantum computation and quantum Information, Cambridge university press, 2000

9 Mosca M. The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer. In: Proc. of the 1st NASA Intl. Conf. on Quantum Computing and Quantum Communication, LNCS 1509, Springer-Verlag, 1999. 174～188

10 Jozsa R. Quantum Algorithms and the Fourier Transform: [Technical Report]. arXive: quant-ph/9707033, 1997

11 Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography, C. R. C. Press, 1997

12 夏培肃. 量子计算. 计算机研究与发展, 2001(10): 1153～1171