•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700629

基于e次根攻击RSA的量子算法

王亚辉[1,2], 张焕国[2*], 王后珍[2]

(1.信阳师范学院 计算机与信息技术学院, 河南 信阳 464000; 2.武汉大学 计算机学院, 湖北 武汉 430072)

摘　要:量子算法的出现给现有的公钥密码体制带来了严峻挑战, 其中, 最具威胁的是Shor算法。Shor算法能够在多项式时间内求解整数分解问题和离散对数问题, 使得当前应用广泛的RSA、ElGamal和ECC等公钥密码体制在量子计算环境下不再安全, 因此研究量子计算环境下的密码破译就有重大意义。解决整数分解问题是Shor算法攻击RSA的核心思想, 但攻破RSA并非一定要从解决整数分解问题入手。作者试图从非整数分解角度出发, 设计攻破RSA密码体制的量子算法。针对RSA公钥密码体制的特点, 通过量子傅里叶变换求出RSA密文C模n的e次根进而得到RSA的明文M。即不通过整数分解问题攻破了RSA。与以往密码分析者通过分解模数n试图恢复私钥的做法不同, 直接从恢复明文消息入手, 给出一个对抗RSA密码体制的唯密文攻击算法。研究表明, 本文算法的成功概率高于利用Shor算法攻击RSA的成功概率。同时本文算法具有如下性质,即不通过解决整数分解问题实现攻破RSA, 且避开了密文C模n的阶为偶数这一限制。

关键词:信息安全; 密码学; RSA密码; 量子计算

中图分类号:TP301　　**文献标志码**:A　　**文章编号**:2096-3246(2018)02-0163-07

Quantum Algorithm for Attacking RSA Based on the e^{th} Root

WANG Yahui[1,2], *ZHANG Huanguo*[2*], *WANG Houzhen*[2]

(1.School of Computer and Info. Technol., Xinyang Normal Univ.,Xinyang 464000,China; 2.Compute School,Wuhan Univ.,Wuhan 430072,China)

Abstract: The emergence of some quantum algorithms has brought a serious threat to modern cryptography,among which Shor's algorithm is the most important threatening algorithm for cryptanalysis currently.Shor's algorithm can solve the integer factorization problem (IFP) and discrete logarithm problem (DLP) in polynomial-time,which makes the current widely used RSA,ElGamal and ECC public key cryptosystem unsafe any more under the quantum computing environment.Therefore,it is necessary to research the cryptanalysis in the quantum computing environment.Solving the IFP is the core idea of Shor's algorithm for attacking RSA,but breaking RSA does not have to be solved by solving the IFP.A quantum algorithm is designed to attack the RSA cryptosystem starting from the angle of non-factorization.Focusing on the characteristics of RSA public key cryptosystem,using the quantum Fourier transform,the RSA plaintext M can be got by calculating the e^{th} root modulus n.That is,without solving the IFP,RSA is broken.Different from the previous practices that cryptanalysts try to recover the private-key,a ciphertext-only attack algorithm for RSA,directly from recovering the plaintext M to start, is presented.Results show that the probability of success of the new algorithm is higher than that of Shor's algorithm attacking RSA.At the same time,the new algorithm does not recover the RSA plaintext from the ciphertext without factoring the modulus n,and avoids the restriction that the order of ciphertext C modules n is even.

Key words: information security;cryptology;RSA cryptography;quantum computing

量子计算是综合利用量子力学原理和计算机科学相关知识进行计算的新的计算模式。它利用量子系统的叠加性、纠缠性和相干性等实现量子的并行计算。量子算法的出现给现有的公钥密码体制带来

收稿日期:2017 – 08 – 05

基金项目:国家自然科学基金重点资助项目(61332019); 国家重点基础研究发展规划资助项目(2014CB340601); 国家自然科学基金资助项目(61402339; 61202386); 国家自然科学基金重大项目资助(91018008);国家密码发展基金资助项目(MMJJ201701304)

作者简介:王亚辉(1988—), 女, 博士生. 研究方向: 密码学; 量子计算. E-mail: wangyh_ecc@whu.edu.cn

* 通信联系人 E-mail: liss@whu.edu.cn

网络出版时间:2018 – 03 – 21 17 : 27 : 32　　**网络出版地址**: http://kns.cnki.net/kcms/detail/51.1773.TB.20180321.1727.007.html

了严峻的挑战。公钥密码体制的安全性分析无论是在理论上还是实际应用中都具有重大意义，特别是广泛使用的RSA、ElGamal和ECC等公钥密码体制的安全性更值得深入研究[1]。

现代公钥密码体制是基于计算数论中困难问题设计的，而整数分解问题是计算数论中重要的困难问题之一。如今广泛用于电子银行，网络等领域的RSA公钥密码体制的安全性正是基于整数分解问题的难解性[2]设计的。之所以RSA密码体制难以破译，就是因为它所依赖的整数分解问题不能快速解决。目前，对密码学最具威胁的两类量子算法是Shor算法和Grover搜索算法。Shor算法[3−4]能够在多项式时间内求解整数分解问题和离散对数问题，这使得当前应用广泛的RSA、ElGamal和ECC等公钥密码体制在量子计算环境下不再安全；Grover搜索算法[5]是一种通用的量子搜索算法，为一大类搜索问题的解决提供了平方根加速，相当于将密钥长度减半，从而威胁到现有的密码体制。此后，量子算法的研究得到了快速发展[6−14]。

Shor算法的提出表明，在量子计算环境下，整数分解问题可以在多项式时间内得以解决，这就意味着基于整数分解问题设计的RSA公钥密码体制的安全性面临威胁。Shor算法对RSA的攻击是从求解整数分解问题角度出发，而关于整数分解问题的研究也一直是学者们的研究热点。研究者们在Shor算法的基础上，一方面，从减少量子位角度出发对算法进行优化；另一方面，从量子计算机实现角度出发实现对小整数的分解实验。Yang等[15]在国际上首次利用光量子计算机实现了Shor算法分解算法，并在该量子计算机上成功操纵了4个光子量子比特构造了一个简单的线性光网络来实现整数15的分解，然而仅仅只能实现诸如整数15这样的小整数分解。Bigrourd等[16]提出了Shor算法的一个改进版本，且利用时域泰伯效应验证了整数19 403的分解。Gilowski等[17]利用冷原子提出了高斯和方法的量子化版本，且利用此方法验证了整数263 193的分解。Peng等[18]提出了第一个绝热量子计算的整数分解算法，并利用该算法在NMR量子处理器上实现了21的分解。该方法使用的量子比特数不到Shor算法分解整数15时使用的量子比特数的一半，而且分解时间更短，但是分解仅仅是对一类具有特定规律的整数有效。Xu等[19]利用核磁共振量子处理器，仅仅需要4量子位实现了分解整数56 153。Smolin等[20]提出了一个量子整数分解新观点，通过寻找阶为2的元素a实现对n的分解。因为元素的阶为2，则第2个寄存器只需要2个量子位，从而大大减少量子位。Cao等[21]给出了Shor算法的一个改进算法，利用多量子寄存器实现因子分解，该方法所需要的量子位数多。Liu等[22]给出了Shor算法的改进算法，通过计算2的阶，进而利用数论的相关性质得到模数n的因子。各方面的资源消耗与Shor算法相当。Geller等[23]利用费马数的特性，利用8量子比特实现对整数51和85的分解，并给出了量子实现电路图，虽然分解整数所用的量子位少，却是针对一些特殊的整数费马数的，不具有普适性。王亚辉等[24]从非整数分解角度出发，基于方程求解与相位估计提出攻击RSA的量子算法。

通过对Shor算法进一步研究和分析，发现以下两点有待优化：一是，Shor算法分解效率不高；二是，Shor算法要求元素a模n的阶r必须为偶数，且输出必须是n的非平凡因子。正是由于Shor算法攻击RSA还有进一步可以优化的空间，作者放弃Shor算法基于求解整数分解问题的理论内核，从非整数分解角度出发，针对RSA公钥密码的特点，基于密文函数$C^x \pmod n$的周期性，利用量子傅里叶变换可以求得RSA密文C模n的e次根进而得到RSA的明文，即攻破RSA。本文算法不仅避开了Shor算法的元素的阶必须为偶数和因子是模数n的非平凡因子这两个要求，且算法的成功概率高于Shor算法攻击RSA的成功概率。

1 背景知识介绍

1.1 计算数论基础

1977年，Rivest、Shamir和Adleman提出了第一个实用的公钥密码体制，也就是著名的RSA公钥密码体制。由于Rivest、Shamir 和Adleman在公钥密码体制方面的理论和实际应用中作出的贡献，尤其是RSA密码体制的发明，计算机学会（ACM）于2000年授予他们图灵奖，也就是计算科学领域的诺贝尔奖。RSA公钥密码体制定义如下：

定义1（RSA公钥密码体制[2]） RSA公钥密码体制可以定义为：

$$\mathrm{RSA}=\{\mathcal{M},C,\mathcal{K},M,C,e,d,n,E,D\}。$$

其中：

1）$\mathcal{M}$是明文集合，称为明文空间；C是密文集合，称为密文空间；$\mathcal{K}$是密钥集合，称为密钥空间。M是一段特殊明文；C是一段特殊密文；$n=pq$是模数，p和q是不同的大素数，n通常至少有100位数。

2）$\{(e,n),(d,n)\in\mathcal{K}\}$，$e$是公钥，$d$是私钥且满足$ed\equiv 1 \pmod{\varphi(n)}$，其中，$\varphi(n)=(p-1)(q-1)$是欧拉函数。

3）E是加密函数$E:M\mapsto C$，即

$$C\equiv M^e \pmod n。$$

4)D是解密函数$D: C \mapsto M$即

$$M \equiv C^d \pmod n。$$

RSA公钥密码体制是典型的基于整数分解问题的密码体制。且有结论: RSA的破译难度不超过整数分解。Shor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密码体制。

定理1(线性丢番图方程的解[2]) 设$\frac{a}{b}$的有限连分数渐进分数如下:

$$\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \cdots, \frac{P_n}{Q_n}\right] = \frac{a}{b} \tag{1}$$

则方程$ax-by=d$的整数解为:

$$\begin{cases} x = (-1)^{n-1} Q_{n-1}, \\ y = (-1)^{n-1} P_{n-1} \end{cases} \tag{2}$$

其中, $d=\gcd(a,b)$。

定理2[2] 乘法的逆元$1/b \pmod n$存在当且仅当$\gcd(b,n)=1$。

定理3(欧拉定理[2]) 设a和n都是正整数, 且$\gcd(a,n)=1$。则

$$a^{\varphi(n)} \equiv 1 \pmod n \tag{3}$$

1.2 量子计算基础

计算机要处理数据, 必须把数据表示成计算机能够识别的形式。经典信息处理的最基本单元是比特(bit, 即二进制0或1)。所有计算都建立在比特的基础上, 与之对应, 量子信息与量子计算也是建立在类似比特概念的量子比特上。一个量子比特是一个可以在二维希尔伯特空间(Hilbert space)中描述的两态量子体系。在此希尔伯特空间中, 通常人们选择一对正交归一化的态

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}、|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

代表经典比特的0和1。一个量子比特的任意状态都可以表示为这个两个基本状态的线性组合。称$|\rangle$为狄拉克(Dirac)记号, 它在量子力学中表示状态。经典比特和量子比特的区别之处在于, 量子比特的状态除了$|0\rangle$和$|1\rangle$外, 还可以是状态的线性组合, 通常称为叠加态, 即

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{4}$$

其中, α、β为复数, 称为量子态的概率幅, 可以用来检测一个量子比特是处于$|0\rangle$态还是$|1\rangle$态。即检测量子态$|\Psi\rangle$得到$|0\rangle$的概率为$|\alpha|^2$, 得到$|1\rangle$的概率为$|\beta|^2$, 且满足归一化条件:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{5}$$

类似于经典计算机线路用连线和逻辑门构成, 量子计算机线路也可用连线和基本量子门组成的量子线路构造。这些量子逻辑门实质上是幺正操作, 基于线性性质, 几何上可用矩阵表示。常见的单量子比特门如Hadamard门为:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}。$$

其作用在n量子比特$|0\rangle^{\otimes n}$上时, 可产生均匀叠加态, 即

$$H|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle \tag{6}$$

Hadamard门变换是量子算法中常用的重要量子门。

定义2(量子Fourier变换(QFT)[25]) 量子Fourier变换定义为: 在一组标准正交基$|0\rangle, |1\rangle, \cdots, |q-1\rangle$上的一个线性算子, 在基态上的作用为:

$$\mathrm{QFT}: |j\rangle \to \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \mathrm{e}^{2\pi \mathrm{i} jk/q} |k\rangle \tag{7}$$

那么, 对任意量子态的变换可写作:

$$\sum_{j=0}^{q-1} x_j |j\rangle \to \sum_{k=0}^{q-1} \sum_{j=0}^{q-1} x_j \mathrm{e}^{2\pi \mathrm{i} jk/q} |k\rangle \tag{8}$$

Nielson等[25]给出了量子Fourier变换是可逆变换的证明, 并且给出了其量子实现电路。

2 基于e次根攻击RSA的量子算法

RSA公钥密码体制的安全性取决于整数分解问题的困难性, 因此解决整数分解问题是攻击RSA最直接的方式。然而攻破RSA却不一定要通过解决整数分解问题实现。从非整数分解角度出发, 针对RSA公钥密码体制的特点, 利用量子傅里叶变换可以求得RSA密文C模n的e次根进而得到RSA的明文M, 即攻破RSA。算法1具体步骤如下:

算法1 基于e次根攻击RSA的量子算法

输入: RSA的公钥(e,n), 密文C;

输出: RSA的明文M。

1)选择q, 其中$q=2^k$且满足$n^2 \le q = 2^k < 2n^2$。

2)给定两个量子寄存器, 分别记为寄存器1, 寄存器2。且初始化为零态$|\Psi_0\rangle = |0\rangle|0\rangle$。其中寄存器1需要$2\lceil \mathrm{lb}\, n \rceil$量子位, 寄存器2需要需要$\lceil \mathrm{lb}\, n \rceil$量子位。

3)对寄存器1执行Hadamard门变换, 得到叠加态为:

$$H: |\Psi_0\rangle \to |\Psi_1\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle|0\rangle \tag{9}$$

4)对$|\Psi_1\rangle$进行U_f变换。由于希尔伯特空间是线性的, 则得到寄存器1和寄存器2的纠缠态$|\Psi_2\rangle$, 有:

$$U_f\colon |\Psi_1\rangle \to |\Psi_2\rangle = U_f\left(\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}U_f|x\rangle|0\rangle = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|f(x)\rangle = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|C^x \pmod n\rangle。$$

即

$$U_f:\sum_{x=0}^{q-1}|x\rangle|0\rangle \to \sum_{x=0}^{q-1}|x\rangle|f(x)\rangle \tag{10}$$

其中，$f(x)=C^x \pmod n$。由此可以看出，对处于叠加态的$|x\rangle$进行U_f变换，可以产生每个x对应的函数值$f(x)$，也即量子的并行性能力在此得以体现。

5）观测寄存器2。不妨假设观测到态$|k\rangle$，事实上，$k\equiv C^t \pmod n$。同时，寄存器1也相应地坍缩，此时寄存器1和寄存器2的态$|\Psi_3\rangle$为：

$$|\Psi_3\rangle = \frac{1}{\sqrt{A}}\sum_{x:C^x\equiv C^t}|x\rangle|k\rangle \tag{11}$$

其中，A是所有满足同余式$C^x\equiv C^t \pmod n$的x的个数。

6）对寄存器1执行量子傅里叶变换（QFT），得到

$$\mathrm{QFT}:|\Psi_3\rangle\to|\Psi_4\rangle=\mathrm{QFT}|\Psi_3\rangle=\frac{1}{\sqrt{A}}\mathrm{QFT}\sum_{x:C^x\equiv C^t}|x\rangle|k\rangle=\frac{1}{\sqrt{A}}\sum_{c=0}^{q-1}\frac{1}{\sqrt{q}}\sum_{x:C^x\equiv C^t}\mathrm{e}^{\frac{2\pi\mathrm{i}xc}{q}}|c\rangle|k\rangle=\frac{1}{\sqrt{Aq}}\sum_{c=0}^{q-1}\sum_{x:C^x\equiv C^t}\mathrm{e}^{\frac{2\pi\mathrm{i}xc}{q}}|c\rangle|k\rangle。$$

其中，$0\le x<q$且满足$C^x\equiv C^t \pmod n$。假设密文C模n的阶为r。即上面的求和式中的所有x满足$x\equiv t \pmod r$，不妨记为$x=t+jr$。由此可以看出寄存器1是以r为周期的态的叠加。此时寄存器的态$|\Psi_4\rangle$为：

$$|\Psi_4\rangle = \frac{1}{\sqrt{Aq}}\sum_{c=0}^{q-1}\sum_{j=0}^{A-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}}|c\rangle|k\rangle \tag{12}$$

进而可知A是不超过$\frac{q-t}{r}$的最大正整数，且$t\le r<n$。又$q\approx O(n^2)$，因此$A\approx q/r$。为了简化计算，假设q是r的整数倍，因此$A=q/r$。则此时寄存器1中的概率幅$A'(c)$记为：

$$A'(c)=\frac{1}{\sqrt{Aq}}\sum_{j=0}^{A-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}}=\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}}。$$

注意到概率幅$A'(c)$是关于c的周期函数，且周期为$\frac{q}{r}$。事实上，

$$A'\left(c+\frac{q}{r}\right)=\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)\left(c+\frac{q}{r}\right)}{q}}=\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}}=A'(c)。$$

其中，利用到$\mathrm{e}^{2\pi\mathrm{i}}=1$。

由此可以看出，量子傅里叶变换（QFT）使得寄存器1的周期从r变为$\frac{q}{r}$，t已经不存在寄存器1的测量结果中如图1所示。

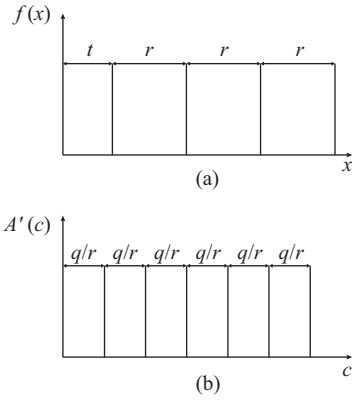

图 1 函数$f(x)$和概率幅$A'(c)$

Fig.1 Function $f(x)$ and probability amplitude $A'(c)$

7）测量寄存器1。不妨假设观测到态$|c\rangle$。因为c和q都是已知的，故利用$\frac{c}{q}$的连分数展开就可得到阶r。

8）因为在RSA密码体制中$ed\equiv 1 \pmod{\varphi(n)}$，由定理2可知$\gcd(e,\varphi(n))=1$。而$r|\varphi(n)$，故可得$\gcd(e,r)=1$。构造线性丢番图方程：

$$e\mu-\varphi(n)\nu=1 \tag{13}$$

则由定理1可得到方程的解μ、ν。

9）计算$M\equiv C^\mu \pmod n$，即为RSA的明文M。这是因为：

$$M^e=(C^\mu)^e=C^{e\mu}=C^{1+\varphi(n)\nu}=C\cdot\left(C^{\varphi(n)}\right)^\nu\equiv C \pmod n。$$

其中，$C^{\varphi(n)}\equiv 1 \pmod n$是由定理3得知。

也即在已知C、e、n的情况下，得到了加密函数$M^e\equiv C \pmod n$的明文M。

算法1基于密文函数$C^x \pmod n$的周期性，利用量子傅里叶变换求得RSA密文C模n的阶r，而截获密文C在实际攻击中也是最容易实现的。与以往密码分析者通过分解模数n试图恢复私钥d的做法不同，作者直接从恢复明文消息入手，给出一个攻击RSA密码体制的唯密文攻击算法。

3 量子算法分析

3.1 量子算法的物理操作可行性

算法1的第3）步执行的H变换和第6）步执行的量

子傅里叶变换(QFT)都可以在多项式规模的量子门电路中得以实现。第4)步执行的酉变换U_f中函数$f(x)$的设计主要由模幂运算可逆电路实现, 可以通过对其经典电路进行改进的可逆计算技术实现[26]。

3.2 量子算法的成功概率分析

引理1　设$a>1$, 则函数$f(x)=\dfrac{\sin ax}{\sin x}$在区间$(0,\dfrac{\pi}{2a}\Big]$内单调递减。

证明: 因为

$$f(x)=\frac{\sin ax}{\sin x} \tag{14}$$

所以

$$f'(x)=\frac{\cos ax\cos x(a\tan x-\tan ax)}{\sin^2 x} \tag{15}$$

令$g(x)=a\tan x-\tan ax$, 则

$$g'(x)=a\left(\sec^2 x-\sec^2 ax\right) \tag{16}$$

而在区间$(0,\dfrac{\pi}{2a}\Big]$内$g'(x)\le 0$, 而$g(0)=0$。因此在区间$(0,\dfrac{\pi}{2a}\Big]$内$g(x)\le 0$。又由在区间$(0,\dfrac{\pi}{2a}\Big]$内$\cos ax\cos x\ge 0$, 因此$g(x)\le 0$, 即函数$f(x)$在区间$(0,\dfrac{\pi}{2a}\Big]$内单调递减。

由算法第6)步可知, 观测到态$|c\rangle$的概率为:

$$\mathrm{Prob}(c)=|A'(c)|^2=\left|\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}}\right|^2=\frac{r}{q^2}\left|\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}jrc}{q}}\right|^2=\frac{r}{q^2}\left|\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}j\{rc\}_q}{q}}\right|^2。$$

其中, $\{rc\}_q$表示$rc(\mathrm{mod}\ q)$的余数。

又注意到

$$A'(c)=\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(t+jr)c}{q}} \tag{17}$$

因此, 可得:

$$A'(c)=\begin{cases}\dfrac{1}{\sqrt{r}}\mathrm{e}^{\frac{2\pi\mathrm{i}tc}{q}}, & \text{如果}c\text{是}A\text{的倍数;}\\ 0, & \text{其他。}\end{cases}$$

也即通过第6)步的量子傅里叶变换(QFT)使得所需要的结果增强, 并使不需要的结果变为0。从而由上式的$A(c)$可知, 通过第7)步观测到的态$|c\rangle$满足$rc(\mathrm{mod}\ q)=0$。如果c满足

$$-r/2\le rc(\mathrm{mod}\ q)\le r/2 \tag{18}$$

则$\mathrm{Prob}(c)$能以较高的概率分布在一个半圆上。

记$\delta_c=2\pi\{rc\}_q/q$, 则$\mathrm{Prob}(c)$是以$\mathrm{e}^{\mathrm{i}\delta_c}$为等比的等比数列, 则

$$\mathrm{Prob}(c)=\frac{r}{q^2}\left|\sum_{j=0}^{q/r-1}\mathrm{e}^{\frac{2\pi\mathrm{i}j\{rc\}_q}{q}}\right|^2=\frac{r}{q^2}\left|\frac{1-\mathrm{e}^{\frac{2\pi\mathrm{i}\{rc\}_q}{q}\cdot\frac{q}{r}}}{1-\mathrm{e}^{\frac{2\pi\mathrm{i}\{rc\}_q}{q}}}\right|^2=\frac{r}{q^2}\left|\frac{1-\mathrm{e}^{\mathrm{i}\delta_c\cdot\frac{q}{r}}}{1-\mathrm{e}^{\mathrm{i}\delta_c}}\right|^2=\frac{r}{q^2}\frac{\sin^2\frac{\delta_c q}{2r}}{\sin^2\frac{\delta_c}{2}}。$$

又因为$\left|\{rc\}_q\right|\le\dfrac{r}{2}$, 所以$|\delta_c|\le\dfrac{\pi r}{q}$。而由引理1知, 函数$f(x)=\dfrac{\sin ax}{\sin x}$在区间$(0,\dfrac{\pi}{2a}\Big]$内单调递减。在$\mathrm{Prob}(c)$中, $a=\dfrac{q}{r}$, $x=\dfrac{\delta_c}{2}$, 则有:

$$\mathrm{Prob}(c)=\frac{r}{q^2}\frac{\sin^2\frac{\delta_c q}{2r}}{\sin^2\frac{\delta_c}{2}}\ge\frac{r}{q^2}\frac{\sin^2\frac{q}{2r}\cdot\frac{\pi r}{q}}{\sin^2\frac{1}{2}\cdot\frac{\pi r}{q}}\ge\frac{4}{\pi^2 r}。$$

其中, 不等式$4x^2/\pi^2\le\sin^2 x\le x^2$, $|x|\le\pi/2$。显然$\pi r/2q<\pi/2$。

下面从观测到的c值得到r的信息。由于

$$-r/2\le rc(\mathrm{mod}\ q)\le r/2,$$

而上式又等价于

$$-r/2\le rc-dq\le r/2,$$

两边同时除以rq, 得到

$$\left|\frac{c}{q}-\frac{d}{r}\right|\le\frac{1}{2q} \tag{19}$$

已知c、q, 又因为$r\le n, q\ge n^2$, 所以恰好有一个满足上式的分式$\dfrac{d}{r}$, 其中分母最多为n。而该分式可以通过$\dfrac{c}{q}$的连分数展开求得。因此, 如果$\gcd(d,r)=1$, 就得到r的值。由于与r互素的d有$\varphi(r)$个。因此有:

$$\mathrm{Prob}\left(\text{与}r\text{互素的}d\right)\ge\frac{4\varphi(r)}{\pi^2 r}。$$

也即利用算法1攻破RSA的成功概率$\ge\dfrac{4\varphi(r)}{\pi^2 r}$。

因为利用Shor算法攻破RSA的成功概率为:

$$\frac{3\varphi(r)}{\pi^2 r}\le P_{\mathrm{Shor}}<\frac{4\varphi(r)}{\pi^2 r},$$

因此, 利用算法1攻破RSA的成功概率大于利用Shor算法攻击RSA的成功概率。

3.3 量子算法的时间复杂度分析

算法1由经典计算部分和量子计算部分两部分组成, 经典计算部分中算法1的第7)步执行的连分数展开和第8)步使用的线性丢番图方程求解都可以在多项式时间内完成。下面主要分析量子计算部分的时间消耗。算法1主要由第4)步的酉变换和第6)步的量子傅里叶变换(QFT)组成。而第4)步执行的酉变换需要$O\left((\mathrm{lb}\ n)^3\right)$的量子门实现。第6步执行的量子傅里叶变换(QFT)同样需要$O\left((\mathrm{lb}\ n)^2\right)$的量子门来实现。

第2)步初始化两个寄存器为零态需要$O(\text{lb}\,n)$的量子门来实现。第3)步执行Hadamard门变换需要$O(\text{lb}\,n)$的量子门实现。因此算法1的量子计算部分也可以在多项式时间内完成。综上所述,算法1是多项式时间量子算法。

分析算法1所需要的量子比特数。由步骤2)可知,寄存器1需要2⌈lb n⌉量子比特,寄存器2需要需要⌈lb n⌉量子比特。因此算法1共需要3⌈lb n⌉量子比特。

为了更直观看出算法1的特点以及与前人算法在攻击RSA方面的差异。在表1中,针对各算法在成功概率、时间复杂性、所需要的量子位、理论基础以及攻击类型等方面进行了比较。

表 1 各算法消耗资源对比

Tab.1 Comparision of the consuming in different algorithms

攻击RSA算法	算法成功概率	时间复杂度	所需量子位	理论基础	攻击类型
Shor算法[3–4]	P_{Shor}	$O\left((\text{lb}\,n)^3\right)$	3⌈lb n⌉	整数分解	整数分解攻击
Smolin等算法[20]	P_{Shor}	$O\left((\text{lb}\,n)^3\right)$	3⌈lb n⌉	整数分解	整数分解攻击
Cao等算法[21]	P_{Shor}	$O\left((\text{lb}\,n)^3\right)$	4⌈lb n⌉	整数分解	整数分解攻击
本文算法	$\geq \dfrac{4\varphi(r)}{\pi^2 r}$	$O\left((\text{lb}\,n)^3\right)$	3⌈lb n⌉	非整数分解	e次根攻击

注:$3\varphi(r)/\pi^2 r \leq P_{\text{Shor}} < 4\varphi(r)/\pi^2 r$。

通过表1得出,算法1具有如下性质:1)从非整数分解角度出发,给出一个基于e次根攻击RSA的量子算法;2)避开了Shor算法元素的阶为偶数和输出的因子是模数n的非平凡因子这两条限制;3)具有多项式时间复杂度;4)具有高的成功概率。

4 结 论

由于RSA公钥密码体制的广泛应用,快速攻译RSA已成为现代密码分析的一个重要研究方向。Shor算法能够在多项式时间内攻破RSA,但其算法明确要求元素a模n的阶为偶数,否则返回算法第1)步重新选择a进行计算,并且输出结果有可能是n的非平凡因子。

作者提出的基于e次根攻击RSA的量子算法1,从非整数分解角度出发,利用量子傅里叶变换计算密文C模n的e次根进而恢复出RSA的明文M。与以往密码分析者通过分解模数n试图恢复私钥d的做法不同,本文直接从恢复明文消息入手,给出一个对抗RSA密码体制的唯密文攻击算法。研究表明,本算法的成功概率$\geq 4\varphi(r)/\pi^2 r$,高于利用Shor算法攻击RSA的成功概率,同时避开了Shor算法的两点限制。

本文主要针对基于整数分解问题的RSA密码体制进行量子攻击研究,那么,对于基于离散对数问题和椭圆曲线离散对数问题的密码体制的量子攻击将是下一步的研究方向。

参考文献:

[1] Zhang Huanguo,Han Wenbao,Lai Xuejia,et al.Survey on cyberspace security[J].Scientia Sinica(Informationis),2016,46(2):125–164.[张焕国,韩文报,来学嘉,等.网络空间安全综述[J].中国科学(信息科学),2016,46(2):125–164.]

[2] Yan Songyuan.Quantum computational number theory[M].Berlin:Springer,2015.

[3] Shor P W.Algorithms for quantum computation:Discrete logarithms and factoring[C]//Proceedings of 35th Annual Symposium on Foundations of Computer Science.Washington:IEEE,1994:124–134.

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

[5] Grover L K.Quantum mechanics helps in searching for a needle in a haystack[J].Physical Review Letters,1977,79(23):325–328.

[6] Broadbent A,Fitzsimons J,Kashefi E.Universal blind quantum computation[C]//Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science.Las Vegas:IEEE,2010:517–526.

[7] Li Q,Chan W H,Wu C H,et al.Triple-server blind quantum computation using entanglement swapping[J].Physical Review A,2014,89(4):040302.

[8] Wang Hongfu.Quantum algorithm for obtaining the eigenstates of a physical system[J].Physical Review A,2016,93(5):052334.

[9] Wu Wanqing,Zhang Huanguo,Wang Houzhen,et al.Polynomial-time quantum algorithms for finding the linear structures of boolean function[J].Quantum Information Process,2015,14(4):1215–1226.

[10] Zhang Huanguo,Mao Shaowu,Wu Wanqing,et al.Overview of quantum computation complexity theory[J].Chinese Journal of Computers,2016,39(12):2403–2428.[张焕国,毛少武,吴万青,等.量子计算复杂性理论综述[J].计算机学报,2016,39(12):2403–2428.]

[11] Wu Nan,Song Fangmin,Li Xiangdong.Universal quantum

computer:Theory,organization and implementation[J]. Chinese Journal of Computers,2016,39(12):2429–2445.[吴楠,宋方敏,Xiangdong Li.通用量子计算机:理论、组成与实现[J].计算机学报,2016,39(12):2429–2445.]

[12] He Yefeng.Two-party quantum key agreement protocol based on GHZ states[J].Journal of Sichuan University(Engineering Science Edition),2016,48(6):197–201.[何业锋.基于GHZ态的两方量子密钥协商协议[J].四川大学学报(工程科学版),2016,48(6):197–201.]

[13] Zhu B L,Zhu W Y,Liu Z J,et al.A novel quantum-behaved bat algorithm with mean best position directed for numerical optimization[J].Computational Intelligence and Neuroscience,2016,2016(2):1–17.

[14] Fu Xiangqun,Bao Wansu,Wang Shuai.Quantum algorithm for discrete logarithm over Z_N[J].Chinese Journal of Computers,2014,37(5):1058–1062.[付向群,鲍皖苏,王帅.Z_N上离散对数量子计算算法[J].计算机学报,2014,37(5):1058–1062.]

[15] Yang C,Daniel L,Yang T,et al.Demonstration of a complied version of Shor's quantum factoring algorithm using photonic qubits[J].Physical Review Letters,2007,99(25):250504.

[16] Bigourd D,Chatel B,Schleich W P,et al.Factorization of numbers with the temporal talbot effect:Optical implementation by a sequence of shaped uitrashort pulse[J].Physical Review Letters,2008,100(3):030202.

[17] Gilowski M,Wendrich T,et al.Gauss sum factoring with cold atoms[J].Physical Review Letters,2008,100(3):030201.

[18] Peng X H,Liao Z Y,Xu N Y,et al.Quantum adiabatic algorithm for factorization and its experimental implementation[J].Physical Review Letters,2008,101(2):220405.

[19] Xu N Y,Zhu J,Lu D W,et al.Quantum factorization of 143 on a dipolar coupling nuclear magnetic resonance system[J]. Physical Review Letters, 2012,108(13):130501.

[20] Smolin J A,Smith G,Vargo A.Oversimplifying quantum factoring[J].Nature,2013,499(7457):163–165.

[21] Cao Zhengjun,Cao Zhenfu.On Shor's factoring algorithm with more registers and the problem to certify quantum computers[EB/OL](2014-09-10)[2017-08-05]. https://arxiv.org/abs/1409.7352.

[22] Liu L H,Cao Z J.On computing $\mathrm{ord}_n(2)$ and its application[J]. Information and Computation,2006,204(7):1173–1178.

[23] Geller M R,Zhou Z Y.Factoring 51 and 85 with 8 qubits[J]. Scientific Reports,2013,3:3023.

[24] Wang Yahui,Zhang Huanguo,Wu Wanqing,et al.Quantum algorithms for breaking RSA based on phase estimation and equation solving[J].Chinese Journal of Computers,2017,40(12):2688–2699.[王亚辉,张焕国,吴万青,等.基于方程求解与相位估计攻击RSA的量子算法[J].计算机学报,2017,40(12):2688–2699.]

[25] Nielson M A,Chuang I L.Quantum computation and quantum information[M].10th Anniversary Edition.Cambridge:Cambridge University Press,2010.

[26] Bennett C H.Time/space trade-offs for reversible computaion[J].SIAM Journal on Computing,1989,18(4):766–776.

（编辑　赵　婧）

引用格式:Wang Yahui,Zhang Huanguo,Wang Houzhen.Quantum algorithm for attacking RSA based on the e^{th} boot[J].Advanced Engineering Sciences,2018,50(2):163–169.[王亚辉,张焕国,王后珍.基于*e*次根攻击RSA的量子算法[J].工程科学与技术,2018,50(2):163–169.]