基于方程求解与相位估计攻击 RSA 的量子算法

王亚辉[1),2)] 张焕国[1),2)] 吴万青[3)] 韩海清[1),2)]

[1)](武汉大学计算机学院 武汉 430072)

[2)](空天信息安全与可信计算教育部重点实验室 武汉 430072)

[3)](河北大学计算机科学与技术学院 河北 保定 071002)

摘 要 量子计算的发展对现有的公钥密码体制提出了严峻的挑战,利用 Shor 算法就可攻击公钥密码 RSA, ELGamal 等.因此,研究量子计算环境下的密码破译有重大意义.经典的因子分解算法是通过求解同余方程 $\alpha^2 \equiv \beta^2 \pmod{n}$ 实现的.据查证,目前还没有求解此方程的量子算法,故我们试图从量子计算的角度提出解决此同余方程的量子算法.该算法是对经典求解同余方程 $\alpha^2 \equiv \beta^2 \pmod{n}$ 的量子化实现.相比于 Shor 算法,算法 1 所需量子位少,具有亚指数时间复杂度,且成功概率接近于 1.为了降低时间复杂度,我们从非因子分解角度出发,基于量子 Fourier 逆变换和相位估计,给出了算法.同 Shor 算法相比,算法 2 不需要分解 n,而从 RSA 密文 C 直接恢复出明文 M,具有多项式时间复杂度,且成功概率高于 Shor 算法攻击 RSA 的成功概率,同时不必要满足密文的阶为偶数.

关键词 信息安全;密码学;RSA 密码体制;量子计算

中图法分类号 P301 **DOI 号** 10.11897/SP.J.1016.2017.02688

Quantum Algorithms for Breaking RSA Based on Phase Estimation and Equation Solving

WANG Ya-Hui[1),2)] ZHANG Huan-Guo[1),2)] WU Wan-Qing[3)] HAN Hai-Qing[1),2)]

[1)](*Computer School, Wuhan University, Wuhan* 430072)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan* 430072)

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

Abstract The development of quantum computation presents a serious challenge to the existing public-key cryptosystems, and the public-key cryptosystems, RSA, ELGamal, etc. are broken by using Shor's algorithm. Therefore, it is of great significance to study the cryptanalysis in the quantum computing environment. It is well-known that the RSA public-key cryptography depends essentially only on the computational intractability of the Integer Factorization Problem (IFP), so obviously, the most direct method to attack RSA is to solve the IFP. If IFP can be solved in polynomial-time, then RSA and many other cryptographic systems can be broken. However, the currently existing fastest integer factorization algorithm up to date is the Number Field Sieve, which runs in sub-exponential time. Surprisingly, the world was astonished when Shor announced in 1994 that he found a quantum integer factorization algorithm which can solve IFP and break RSA both in polynomial-time. Since then, various improved and compiled versions of Shor's algorithm using different technics have been proposed and studied, in short, there are two important research directions in quantum integer factorization: (1) Build a (practical)

收稿日期:2016-06-27;在线出版日期:2017-04-28.本课题得到国家自然科学基金重点项目(61332019)、国家"九七三"重点基础研究发展规划项目基金(2014CB340601)、国家自然科学基金(61303212,61202386)、国家自然科学基金重大项目(91018008)资助.**王亚辉**,女,1988 年生,博士研究生,主要研究方向为量子计算、密码学. E-mail:wangyh_ecc@whu.edu.cn. **张焕国**,男,1945 年生,博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为信息安全、密码学、可信计算. **吴万青**,男,1981 年生,博士,讲师,主要研究方向为信息安全、量子密码. **韩海清**,男,1979 年生,博士,博士后,主要研究方向为密码学、量子计算.

quantum computer or even other types of physical computers to implement the full version or compiled version of Shor's algorithm. (2) Improve, modify and simply Shor's original algorithm or even invent new quantum factoring algorithms to be run on quantum computers with fewer quantum bits. Therefore, there are two aspects that need to be improved. One is that how to present a quantum algorithm for breaking RSA with fewer qubits. The classical factorization algorithm is realized by solving the congruent equation $\alpha^2 \equiv \beta^2 (\mathrm{mod}\, n)$. However, to the best knowledge of the authors, there is no quantum algorithm for solving this equation till now. So we are trying to give quantum Algorithm 1 to solve this equation from the perspective of quantum computation, which is the implementation of quantization of the classical quantum algorithm for solving the congruent equation. Compared to Shor's algorithm, Algorithm 1 requires fewer quantum bits, with sub-exponential time complexity. Moreover, the success probability is close to 1. Another is that how to design the compiled version of Shor's algorithm. In order to induce the time complexity, from the point of view of non-factorization, based on the quantum inverse Fourier transform and phase estimation, a polynomial-time quantum Algorithm 2 for directly recovering the RSA plaintext M from the ciphertext C without explicitly factoring the modulus n is presented, and hence, breaks the famous RSA public-key cryptosystem. Compared to Shor's algorithm, Algorithm 2 directly recovers the RSA plaintext M from the ciphertext C, without factoring the modulus n; the order of the ciphertext C satisfying $C^r \equiv 1 (\mathrm{mod}\, n)$ does not need to be even; and the success probability of Algorithm 2 is higher than Shor's.

Keywords　information security; cryptology; RSA cryptography; quantum computing

1　引　言

量子计算的发展对现有的公钥密码体制提出了严峻挑战，利用 Shor 算法就可攻击公钥密码 RSA，ELGamal 等. 因此，研究量子计算环境下的密码破译就有重大意义[1]. RSA[2]是目前信息安全领域应用广泛的公钥密码体制，其研制者 Rivest，Shamir 和 Adleman 获得了 2002 年图灵奖. RSA 的加密和解密过程如下：

$$\begin{cases} C \equiv M^e (\mathrm{mod}\, n) \\ M \equiv C^d (\mathrm{mod}\, n) \end{cases}$$

满足

$$ed \equiv 1 (\mathrm{mod}\ \phi(n)) \qquad (1)$$

其中 M 是明文，C 是密文，e 是加密指数，d 是解密指数，$n=pq$ 是模数，且 p,q 是素数，ϕ 是欧拉函数.

众所周知，RSA 密码体制的安全性是基于整数分解问题的困难性[3]. 之所以 RSA 密码体制难以破译，就是因为它所依赖的数论问题不能快速解决. 目前最快的经典整数分解算法是数域筛法[4-5]，其复杂性是 $O(\exp(c(\log n)^{1/3})(\log\log n)^{2/3})$，其中 $c \approx 1.92$. 因此这仍是一个亚指数复杂性算法，仅适合于分解 200 个十进制位左右的整数. 迄今为止，利用数域筛法分解的最大的数是 RSA-768(768 个二进制位，232 个十进制位).

显然，破译 RSA 最直接的方法就是解决整数分解问题. 因此，全世界的密码分析者的目光都集中在如何快速解决整数分解问题. 1994 年，美国出现了轰动世界的重大科学发现，美国电话电报公司的研究员 Shor 提出了一个快速的量子算法[6-7]，它可以在多项式时间内解决整数分解问题，可攻破 RSA. Shor 算法的主要思想是把整数分解问题转化为求元素 $a \in Z_n^*$ 模 n 的阶问题，通过计算 $\gcd(a^{r/2} \pm 1, n)$ 就能以 $4\phi(r)/\pi^2 r$ 的概率得到 n 的因子. Shor 算法的提出给量子计算的研究注入了新的活力，引发了近二十多年来人们对量子计算和量子计算机研究的热潮[8-15].

经典的因子分解算法大都是通过求解同余方程 $\alpha^2 \equiv \beta^2 (\mathrm{mod}\, n)$ 实现的，也即找到正整数对 (α,β) 使得 $\alpha^2 \equiv \beta^2 (\mathrm{mod}\, n)$ 且 $\alpha \neq \pm\beta (\mathrm{mod}\, n)$ 成立. 一旦找到正整数对 (α,β)，就可以通过计算 $\gcd(\alpha \pm \beta, n) = (p,q)$ 得到模数 n 的因子 p,q. 进一步可以得到公钥密码体制 RSA 的密钥 $d \equiv 1/e (\mathrm{mod}((p-1)(q-1))$，从而攻破 RSA 公钥密码. 据查证，目前还没有对此

方程求解的量子算法，故我们试图从量子计算的角度做一个尝试. 基于 Grover 搜索[16-17]，本文给出了同余方程 $\alpha^2 \equiv \beta^2 \pmod{n}$ 的量子求解算法. 这是本文的一个创新点. 虽然该算法的计算复杂性是亚指数的，但这是第一个求解同余方程 $\alpha^2 \equiv \beta^2 \pmod{n}$ 的量子算法. 算法所需要的量子位数比 Shor 算法所需要的量子位数少，且算法的成功概率接近 1.

众所周知，如果整数分解问题得以解决，那么我们就可攻破 RSA；然而，攻破 RSA 却不一定要通过解决整数分解问题. 因此我们可以考虑从非因子分解角度出发，通过计算密文 C 的阶，达到恢复明文 M 的目的. 即不用通过分解模数 n 也能攻破 RSA. 基于量子 Fourier 逆变换和相位估计，提出另一个攻击 RSA 的量子算法. 该算法避开了 Shor 算法的元素的阶必须为偶数和因子是 n 的非平凡因子这两个要求，不需要分解 n 而从 RSA 密文 C 直接恢复出明文 M. 算法的成功概率大于 Shor 算法攻击 RSA 的成功概率.

本文第 2 节介绍 Shor 算法攻击 RSA 的国内外研究现状；第 3 节介绍与 RSA 密码分析有关的基础知识以及 Shor 算法对 RSA 的攻击；第 4 节分析经典的分解算法，并提出基于方程求解攻击 RSA 的量子算法；第 5 节基于相位估计提出了一个攻击 RSA 的量子算法，并进行算法分析，该算法不通过分解模数 n；第 6 节是总结与下一步工作.

2 相关工作

Shor 算法对 RSA 的攻击体现在 Shor 算法对 RSA 的安全基础的大数 n 的分解，关于 Shor 算法对 n 的分解的研究一直是国内外专家学者的研究热点. 研究者们利用各种不同的技巧，提出了 Shor 算法的不同编译版本(complied version). 比如，2001 年，文献[18]利用核磁共振技术演示了 Shor 算法对整数 15 的分解实验，但该实验不能很好的显示其量子属性，也无法扩展到更多的量子比特，从而分解更大的数，限制了进一步的研究. 2007 年，文献[19]在研究 Shor 算法的量子比特间残余耦合所产生的影响时，通过编写 Quantware 库并调用该库，用 30 个量子比特实现了 $n=943$ 的分解. 该方法虽然理解容易，但是 Quantware 库的限制性却很多. 同年，文献[20]在国际上首次利用光量子计算机实现了 Shor 量子分解算法，并在该量子计算机上成功操控了 4 个光子量子比特构造一个简单的线性光网络实现 $n=15$ 的分解. 2008 年，文献[21]首次提出了基于绝热量子计算的因子分解算法. 相比于 Shor 算法，该算法利用的量子位少，并成功地在 NMR 量子处理器上实现了 21 的分解. 2012 年，文献[22]在文献[21]的基础上提出了一个改进的绝热量子算法，并利用核磁共振量子处理器实现了对 143 的分解. 并且这是目前为止分解的最大的数. 同年，文献[23]利用约瑟夫森电荷量子比特实现了 Shor 算法. 并且最后利用 3 量子比特成功完成了对 $n=15$ 分解的物理实现. 但它对物理属性要求很高，也就是说它需要在特定的物理条件下才能实现. 2013 年，文献[24]基于费马数的特性，利用 8 量子比特分解 51 和 85，并给出了量子电路图. 同年，文献[25]提出了一个量子分解新观点，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，则第二个寄存器只需要 2 个量子位，从而大大减少量子位.

总之，目前通过量子计算实现整数分解有两个主要的研究方向：

(1) 建立实用的量子计算机或者其他类型的物理计算机，包括最快的 D-Wave 2 量子计算机[18-20,22].

(2) 研发 Shor 算法的改进版本. 一方面是提出研发一些易于实现的所谓的“编译”版本. 另一方面从减少量子位角度出发提出改进算法[21,23-25].

3 量子算法知识背景介绍

3.1 基础知识

这节介绍与 RSA 密码分析有关的基础知识.

定义 1(RSA 问题)[3]. 给定 $e \equiv 1/d \pmod{(p-1)(q-1)}$，$n=pq$，$C \equiv M^e \pmod{n}$. 求出 M 或者 d.

定理 1. 设 C 是 RSA 的密文，记 r 为 $C \in Z_n^*$ 模 n 的阶，则

$$M \equiv C^{1/e \pmod{r}} \pmod{n}.$$

证明. 因为 r 是 $C \in Z_n^*$ 模 n 的阶，所以 $r \mid \phi(n)$ 又由 $\gcd(e, \phi(n))=1$ 所以 e 与 r 互素，那么存在 e 模 r 的乘法逆 d'. 即 $ed' \equiv 1 \pmod{r}$. 那么 $(M^e)^{d'} \pmod{n}$ 是密文 C 对应的明文，即 $M \equiv C^{d'} \pmod{n}$ 因此有 $M \equiv C^{1/e \pmod{r}} \pmod{n}$ 成立. 证毕.

引理 1[17]. 设 $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ 是一个正奇合数的素因子分解. 如果 Z_n^* 中的一个元素 x 模 n 的阶 r 是偶数且 $x^{r/2} \neq -1 \pmod{n}$，那么 $\gcd(x^{r/2}+1, n)$ 或者 $\gcd(x^{r/2}-1, n)$ 是 n 的一个非平凡因子.

引理 2[17]. 设 $n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ 是一个正奇合数的素因子分解. 令 x 是在 $1\leq x\leq n-1$ 内均匀随机选出的整数，且 x 与 n 互质，令 r 是 x 模 n 的阶，则

$$P(r\text{ 是偶数，且 }x^{r/2}\neq -1(\bmod n))\geq 1-\frac{1}{2^m}.$$

推论 1. 设 $n=pq$，x 是从 $[0,n-1]$ 中随机选取的与 n 互质的整数，x 模 n 的阶为 r，那么利用 x 对 n 进行整数分解的概率为 $p\geq 3/4$.

证明. 由引理 2 知，此时 $m=2$，则

$$P(r\text{ 是偶数，且 }x^{r/2}\neq -1\ (\bmod n))\geq 1-\frac{1}{2^2}=3/4.$$

再由引理 1 可知：通过计算 $\gcd(x^{r/2}\pm 1,n)$ 可得到的 n 的非平凡因子，即为 p,q.

因此利用 x 对 n 进行整数分解的概率为 $p\geq 3/4$. 证毕.

定义 2. 量子 Fourier 变换（记为 QFT）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

$$\mathrm{QFT}:|j\rangle\rightarrow\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}e^{2\pi ijk/q}|k\rangle,$$

那么对任意量子态的变换可写作

$$\sum_{j=0}^{q-1}x_j|j\rangle\rightarrow\sum_{k=0}^{q-1}\sum_{j=0}^{q-1}x_je^{2\pi ijk/q}|k\rangle.$$

同样的，我们定义量子傅里叶逆变换（记为 QFT^{-1}）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

$$\mathrm{QFT}^{-1}:|k\rangle\rightarrow\frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}e^{-2\pi ikj/q}|j\rangle.$$

文献[17]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.

3.2 Shor 算法对 RSA 的攻击

1994 年，Shor 提出了量子整数分解算法[5-6]，其核心在于把因子分解问题转化成寻找函数的周期问题，从而利用量子 Fourier 变换求解周期问题. Shor 算法攻击 RSA 的基本步骤大致如下：

1. 给定整数 n，选择 a 和 q，其中 n 是两个素数的乘积，$a\in Z_n^*$ 且 $n^2\leq q=2^k<2n^2$.

2. 给定两个量子寄存器，且初始化为零态

$$|\Psi_0\rangle=|0\rangle|0\rangle.$$

3. 对第一个量子寄存器执行 Hadamard 变换，得到叠加态

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

4. 对第二个量子寄存器做模幂运算 U_f，得到

$$U_f:|\Psi_1\rangle\rightarrow|\Psi_2\rangle=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|a^x(\bmod n)\rangle,$$

其中 $U_f:|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$，$f(x)=a^x\bmod n$.

5. 对第二个量子寄存器进行观测. 假设观测到 $m\equiv a^l(\bmod n)$，此时第一个寄存器中的态也相应的坍缩到所有满足 $a^x\equiv m(\bmod n)$ 的 x. 此时第一个寄存器中的态为

$$|\Psi_3\rangle=\frac{1}{\sqrt{n_l+1}}(|l\rangle+|l+r\rangle+\cdots+|l+n_lr\rangle),$$

其中 n_l 是满足 $l+nr\leq 2^t-1$ 成立的最大正整数.

6. 对第一个量子寄存器执行量子 Fourier 变换

$$\begin{aligned}&\mathrm{QFT}:|\Psi_3\rangle\rightarrow|\Psi_4\rangle\\&=\mathrm{QFT}\Big(\frac{1}{\sqrt{n_l+1}}(|l\rangle+|l+r\rangle+\cdots+|l+n_lr\rangle)\Big)\\&=\mathrm{QFT}\Big(\frac{1}{\sqrt{n_l+1}}\sum_{j=0}^{n_l}|l+jr\rangle\Big)\\&=\frac{1}{\sqrt{n_l+1}}\mathrm{QFT}\Big(\sum_{j=0}^{n_l}|l+jr\rangle\Big)\\&=\frac{1}{\sqrt{n_l+1}}\frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\Big(\sum_{j=0}^{n_l}e^{\frac{2\pi i(l+jr)c}{q}}\Big)|c\rangle.\end{aligned}$$

7. 利用连分数算法计算出 r，然后判断 r 是否为元素 a 的阶. 如果是，则算法结束，否则返回第 1 步，直到找到正确的阶 r.

8. 如果 r 是奇数，重新选择 a. 如果 r 是偶数，则计算 $\gcd(a^{r/2}\pm 1,n)=(p,q)$. 如果 $p,q\neq 1$，则 p,q 就是 n 的因子，否则重新选择 a 进行计算.

9. 计算 $M\equiv C^{1/e(\bmod (p-1)(q-1))}(\bmod n)$，即为 RSA 的明文，从而攻破 RSA.

Shor 量子分解算法总共所需量子位为 $3\lceil\log n\rceil$.

Shor 通过证明得出运行一次算法的成功概率为 $4\phi(r)/\pi^2r$，其中 ϕ 是欧拉函数，r 是 a 模 n 的阶，$a\in Z_n^*$. 从而可以看出 Shor 算法的成功概率是依赖于元素 a 模 n 的阶 r.

定理 2. Shor 算法攻击 RSA 的成功概率为

$$3\phi(r)/\pi^2r\leq p_{\mathrm{Shor}}<4\phi(r)/\pi^2r.$$

证明. 由上述知识可知：Shor 算法运行一次得到元素 x 模 n 的阶的成功概率为 $4\phi(r)/\pi^2r$. 又由推论 1 知：利用元素 x 模 n 的阶进行整数分解的概率为 $p\geq 3/4$. 因此 Shor 算法攻击 RSA 的成功概率为 $3\varphi(r)/\pi^2r\leq p_{\mathrm{Shor}}<4\phi(r)/\pi^2r$. 证毕.

4 基于方程求解攻击 RSA 的量子算法

众所周知，目前还没有经典的多项式因子分解算法，而经典领域进行整数分解的基本思想是求出同余方程 $\alpha^2\equiv\beta^2(\bmod n)$ 的解 (α,β)，然后通过计算

$\gcd(\alpha\pm\beta,n)=(p,q)$得到 n 的因子.本节通过分析经典的分解算法,给出了对应的求解同余方程 $\alpha^2\equiv\beta^2(\bmod n)$的量子求解算法.

4.1 经典算法步骤

目前整数分解算法的基本思想:找到正整数(α,β)使得 $\alpha\neq\pm\beta(\bmod n)$且 $\alpha^2\equiv\beta^2(\bmod n)$成立.一旦找到整数$(\alpha,\beta)$,那么通过计算 $\gcd(\alpha\pm\beta,n)=(p,q)$得到 n 的因子 p,q.

经典的找到(α,β)最终求得 n 的因子的算法步骤如下:

1. 构建同余关系.构建如下的因子基 FB

$$\mathrm{FB}=\{p_1,p_2,\cdots,p_t\},$$

它由所有不超过 y 的所有素数构成.选择一个任意整数序列$\{\alpha_i\}_{i=1}^r$,使得所有的 α_i 满足

$$\alpha_i^2\equiv\beta_i(\bmod n)=\prod_{j=1}^{t}p_j^{v_j},$$

其中 v_j 是 p_j 的指数.在这步的最后,$\{\alpha_i\}_{i=1}^r$的子序列$\{\alpha_i'\}_{i=1}^k$,$k<r$ 和$\{\beta_i\}_{i=1}^r$的子序列$\{\beta_i'\}_{i=1}^k$,$k<r$.这样就得到同余关系

$$\alpha_i'^2=\beta_i'=\prod_{j=1}^{t}p_j^{v_{j,i}},\ i=1,2,\cdots,k \tag{2}$$

对应的指数向量如下:

$$\begin{cases}\boldsymbol{v}_j,1=(v_1,1,v_2,1,\cdots,v_t,1)\\ \boldsymbol{v}_j,2=(v_1,2,v_2,2,\cdots,v_t,2)\\ \vdots\\ \boldsymbol{v}_j,k=(v_1,k,v_2,k,\cdots,v_t,k)\end{cases} \tag{3}$$

2. 找乘方.由第 1 步的子序列$\{\beta_i'\}_{i=1}^k$,找到一个新的子序列$\{\beta_i''\}_{i=1}^s$,$s<k$.如果$\sum\limits_{\substack{1\leq j\leq t\\1\leq i\leq s}}\boldsymbol{v}_j,i\equiv0(\bmod 2)$成立,那么就可以构成一个乘方 $\beta_1''\beta_2''\cdots\beta_s''=\beta^2$.也就是说,由第 1 步的式(2)和(3),得到

$$\alpha_i'^2=\beta_i'=\prod_{j=1}^{t}p_j^{v_j,i},\ i=1,2,\cdots,s \tag{4}$$

且对应的向量为

$$\begin{cases}\boldsymbol{v}_j,1=(v_1,1,v_2,1,\cdots,v_t,1)\\ \boldsymbol{v}_j,2=(v_1,2,v_2,2,\cdots,v_t,2)\\ \vdots\\ \boldsymbol{v}_j,s=(v_1,s,v_2,s,\cdots,v_t,s)\end{cases} \tag{5}$$

使得

$$\alpha^2=\Big(\prod_{1\leq i\leq s}\alpha_i''\Big)^2=\prod_{1\leq i\leq s}\beta_i''=\prod_{1\leq j\leq t}p_j^{\sum\limits_{1\leq i\leq s}v_j,i}=\prod_{1\leq j\leq t}p_j{}^{2\left(\frac{1}{2}\sum\limits_{1\leq i\leq s}v_j,i\right)}.$$

当$\sum\limits_{\substack{1\leq j\leq t\\1\leq i\leq s}}\boldsymbol{v}_j,i\equiv0(\bmod 2)$成立时

$$\alpha^2=\Big(\prod_{1\leq j\leq t}p_j^{\left(\frac{1}{2}\sum\limits_{1\leq i\leq s}v_j,i\right)}\Big)^2=\beta^2$$

因此,$\alpha=\prod\limits_{1\leq i\leq s}\alpha_i''$,$\beta=\sqrt{\prod\limits_{1\leq i\leq s}\beta_i''}$.

3. 计算 $\gcd(\alpha\pm\beta,n)=(p,q)$.

如上所述,经典的因子分解算法大都是通过求解同余方程 $\alpha^2\equiv\beta^2(\bmod n)$实现的.还没有对此方程求解的量子算法,故我们试图从这个角度做一个尝试,提出解决此同余方程的量子算法,这是本文的一个创新点.具体算法见第 4.2 节.

4.2 量子算法设计

4.2.1 算法设计

这节从量子计算的角度考虑如何实现同余方程 $\alpha^2\equiv\beta^2(\bmod n)$的量子求解方法.

算法 1. 基于方程求解攻击 RSA 的量子算法.

输入:RSA 模数 n

输出:一组满足同余方程 $\alpha^2\equiv\beta^2(\bmod n)$的正整数 α,β

过程 1. 找到一组正整数(α,β)使其满足同余方程 $\alpha^2\equiv\beta^2(\bmod n)$.

1. 找到 $q=2^t$,其中 $t=\lfloor\log n\rfloor$.

2. 对两个寄存器进行初始化:$|\Psi_0\rangle=|0\rangle|0\rangle$.

3. 对第一个寄存器执行 H 门变换,得到

$$H:|\Psi_0\rangle\rightarrow|\Psi_1\rangle=\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha\rangle|0\rangle.$$

4. 对第二个寄存器进行模幂运算 U_f,得到

$$U_f:|\Psi_1\rangle\rightarrow|\Psi_2\rangle=\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha\rangle|f(\alpha)\rangle=\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha\rangle|\alpha^2(\bmod n)\rangle,$$

其中 $U_f:|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$,$f(x)=x^2(\bmod n)$.

5. 重复步骤 5.1~5.5 $O(\sqrt{q})$次.

5.1 在第二个寄存器上执行条件相移变换 U_O,使得相同的态获得 -1 的相位移动,即

$$U_O:|\Psi_2\rangle\rightarrow|\Psi_3\rangle=\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q}(-1)^{\delta_{\alpha^2\bmod n,\beta^2\bmod n}}|\alpha\rangle|\alpha^2(\bmod n)\rangle,$$

其中假设同余方程 $\alpha^2\equiv\beta^2(\bmod n)$的解对有 m 对,也即$\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),\cdots,(\alpha_m,\beta_m)\}$.为了方便书写,我们记为$\{\alpha_1',\alpha_2',\cdots,\alpha_{2m}'\}$.$U_O$表示算子 $U_O=I-2\sum\limits_{i=1}^{2m}|\alpha_i'\rangle\langle\alpha_i'|$.在此定义 δ 函数如下:

$$\delta_{\alpha^2\bmod n,\beta^2\bmod n}=\begin{cases}1, & \text{当 }\alpha^2\bmod n=\beta^2\bmod n\\ 0, & \text{当 }\alpha^2\bmod n\neq\beta^2\bmod n\end{cases}.$$

5.2 在第二个寄存器上执行 U 变换,得到

$$U:|\Psi_3\rangle\rightarrow|\Psi_4\rangle=\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}(-1)^{\delta_{\alpha^2\bmod n,\beta^2\bmod n}}|\alpha\rangle|0\rangle,$$

其中 $U:|\alpha\rangle|b\rangle\rightarrow|\alpha\rangle|b\oplus\alpha^2(\bmod n)\rangle$.

5.3 对第一个寄存器执行 H 门变换.

5.4 在第一个寄存器上执行条件相移,使$|0\rangle^{\otimes t}$之外的每个计算基态获得 -1 的相位移动.

5.5 对第一个寄存器执行 H 门变换.

6. 测量第一个寄存器.假设我们观测到态$|\alpha\rangle$,事实上由量子力学可知,满足 $\alpha^2\equiv\beta^2(\bmod n)$的态$|\alpha\rangle$,$|\beta\rangle$能够以相

同的，较高的概率被观测到. 但是当$|\alpha\rangle$被测量到时，$|\beta\rangle$相应的坍缩，在这种情况下，我们需要进行过程 2.

过程 2.　找到同余方程$\beta^2\equiv a(\mathrm{mod}n)$的一个解$\beta$，其中$a=\alpha^2$是由过程 1 得到的.

1. 找到$q=2^{t'}$，其中$t'=\left\lceil\log\frac{n}{2}\right\rceil$.

2. 对两个寄存器进行初始化：$|\Psi_0\rangle=|0\rangle|0\rangle$.

3. 对第一个寄存器执行 H 门变换，得到

$$H:|\Psi_0\rangle\rightarrow|\Psi_1\rangle=\frac{1}{\sqrt{q}}\sum_{\beta=0}^{q-1}|\beta\rangle|0\rangle.$$

4. 对第二个寄存器进行模幂运算U_f，得到

$$U_f:|\Psi_1\rangle\rightarrow|\Psi_2\rangle=\frac{1}{\sqrt{q}}\sum_{\beta=0}^{q-1}|\beta\rangle|f(\beta)\rangle=\frac{1}{\sqrt{q}}\sum_{\beta=0}^{q-1}|\beta\rangle|\beta^2(\mathrm{mod}n)\rangle,$$

其中$U_f:|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$，$f(x)=x^2(\mathrm{mod}n)$.

5. 重复步骤 5.1～5.5 $O(\sqrt{q})$次.

5.1 第二个寄存器上执行条件相移变换$U_{O'}$，使得态$|a\rangle$获得-1的相位移动，即

$$U_{O'}:|\Psi_2\rangle\rightarrow|\Psi_3\rangle=\frac{1}{\sqrt{q}}\sum_{\beta=0}^{q-1}(-1)^{\delta_{a,\beta^2\mathrm{mod}n}}|\beta\rangle|\beta^2(\mathrm{mod}n)\rangle.$$

其中假设同余方程$\beta^2\equiv a(\mathrm{mod}n)$的解有$m'$个，不妨设为$\{\beta_1,\beta_2,\cdots,\beta_{m'}\}$. $U_{O'}$表示算子$U_{O'}=I-2\sum_{i=1}^{m'}|\beta_i\rangle\langle\beta_i|$. 在此定义$\delta$函数如下：

$$\delta_{a,\beta^2\mathrm{mod}n}=\begin{cases}1, & \text{当 }\beta^2\mathrm{mod}n\equiv a\\ 0, & \text{当 }\beta^2\mathrm{mod}n\neq a\end{cases}.$$

5.2 在第二个寄存器上执行U变换，得到

$$U:|\Psi_3\rangle\rightarrow|\Psi_4\rangle=\frac{1}{\sqrt{q}}\sum_{\beta=0}^{q-1}(-1)^{\delta_{a,\beta^2\mathrm{mod}n}}|\beta\rangle|0\rangle,$$

其中$U:|\beta\rangle|b\rangle\rightarrow|\beta\rangle|b\oplus\beta^2(\mathrm{mod}n)\rangle$.

5.3 对第一个寄存器执行 H 门变换.

5.4 在第一个寄存器上执行条件相移使$|0\rangle^{\otimes t'}$之外的每个计算基态获得-1的相位移动.

5.5 对第一个寄存器执行 H 门变换.

6. 测量第一个寄存器. 假设我们观测到态$|\beta\rangle$，如果β满足同余方程$\beta^2\equiv a(\mathrm{mod}n)$，则$\beta$是同余方程$\beta^2\equiv a(\mathrm{mod}n)$的一个解. 事实上，我们以很高的概率观测到满足$\beta^2\equiv a(\mathrm{mod}n)$的$\beta$.

因此，由过程 1 得到的α和过程 2 得到的β，我们就构成$\alpha^2\equiv\beta^2(\mathrm{mod}n)$的解$(\alpha,\beta)$.

4.2.2　算法分析

定理 3.　设$n=pq$，p,q是两个素数. 如果整数对α,β满足同余方程

$$\alpha^2\equiv\beta^2(\mathrm{mod}n)\text{且}\alpha\neq\pm\beta(\mathrm{mod}n).$$

则n可以通过计算$\gcd(\alpha\pm\beta,n)=(p,q)$得到因子$p,q$.

证明.　因为$\alpha^2\equiv\beta^2(\mathrm{mod}n)$，

$\Rightarrow(\alpha+\beta)(\alpha-\beta)\equiv0(\mathrm{mod}n)$，

$\Rightarrow n|(\alpha+\beta)(\alpha-\beta)$，

又因为$\alpha\neq\pm\beta(\mathrm{mod}n)$，

因此计算$\gcd(\alpha\pm\beta,n)=(p,q)$，

也即$n=pq,1<p,q<n$.　证毕.

因此通过算法 1，我们可以得到 RSA 模数n的素因子p,q. 进一步，可以计算 RSA 密码体制的密钥$d\equiv1/e(\mathrm{mod}(p-1)(q-1))$，从而攻破 RSA 公钥密码.

定理 4.　算法 1 通过求解$\alpha^2\equiv\beta^2(\mathrm{mod}n)$的解$(\alpha,\beta)$得到$n$的因子，算法的时间复杂度为$O(\sqrt{n})$.

证明.　算法的主要计算在于模指数的运算，其计算复杂性为$O(c(\log n)^2\log\log n\log\log\log n)$，迭代次数为$O(\sqrt{q})$. 因此，相对于经典算法，新算法是二次加速算法.　证毕.

定理 5.　算法 1 的成功概率接近于 1.

证明.　算法 1 的成功概率依赖于迭代次数. 文献[17]已经证明所需要的迭代次数的上界为

$$R\leq\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil,$$

其中N是搜索空间的总数，M是搜索问题的解的个数. 因此算法迭代$O(\sqrt{q})$次，就能以 100%的成功概率得到同余方程$\alpha^2\equiv\beta^2(\mathrm{mod}n)$的解$(\alpha,\beta)$.　证毕.

定理 6.　算法 1 所需量子位为$\lfloor\log n\rfloor+\left\lceil\log\frac{n}{2}\right\rceil$，少于 Shor 算法攻击 RSA 所需的量子位数.

证明.　由 3.2 节知，Shor 量子分解算法总共需量子位为$3\lceil\log n\rceil$. 显然有

$$\lfloor\log n\rfloor+\left\lceil\log\frac{n}{2}\right\rceil<3\lceil\log n\rceil$$

也即算法 1 所需量子位少于 Shor 算法攻击 RSA 所需要的量子位数.　证毕.

综上所述，量子算法 1 是对经典同余方程$\alpha^2\equiv\beta^2(\mathrm{mod}n)$的量子化实现. 一旦求出解$(\alpha,\beta)$，可以通过计算$\gcd(\alpha\pm\beta,n)=(p,q)$，得到模数$n$的因子$p,q$. 进一步，可以计算公钥密码 RSA 的密钥$d\equiv1/e(\mathrm{mod}(p-1)(q-1))$，从而攻破 RSA 公钥密码. 相比于 Shor 算法，算法 1 所需量子位少，具有亚指数时间复杂度，且成功概率接近于 1.

5　基于相位估计攻击 RSA 的量子算法

如果整数分解问题得以解决，那么我们就可攻

破 RSA;攻破 RSA 却不一定要通过解决整数分解问题.我们通过对比发现:算法 1 仍然具有亚指数时间复杂度,为了降低时间复杂度,我们从非因子分解角度出发,提出另外一个新的量子算法.具体内容如下.

5.1 算法设计

在第 3.2 节介绍的 Shor 算法里,攻击 RSA 主要是通过求元素的阶,而元素的阶主要是在第二个寄存器中进行模幂运算,再对其进行观测,利用量子傅里叶变换,观测第一个寄存器态的周期性来完成的.本节利用量子态的叠加原理,不用观测第二个量子寄存器,提出了一个基于相位估计求密文阶的量子算法.具体算法步骤如下.

算法 2. 基于相位估计攻击 RSA 的量子算法

输入:C,e,n

输出:M

基于相位估计找到密文 C 模 n 的阶,计算 $M\equiv C^{1/e(\bmod r)}(\bmod n)$,恢复 RSA 明文 M.

1. 计算 $q=2^t$,其中 $t=\lceil\log n\rceil$.

2. 给定 2 个 t 维量子寄存器,其初态为

$$|\Psi_0\rangle=|0^t\rangle|1^t\rangle.$$

3. 对第一个量子寄存器进行 Hadamard 门变换,产生叠加态

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

4. 对第二个量子寄存器进行酉变换 U_C^x,得到

$$\begin{aligned}U_C^x:&|\Psi_1\rangle\rightarrow|\Psi_2\rangle\\&=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle U_C^x|1\rangle \qquad (6)\\&=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|C^x(\bmod n)\rangle\\&=\frac{1}{\sqrt{qr}}\sum_{x=0}^{q-1}\sum_{k=0}^{r-1}|x\rangle e^{\frac{2\pi ikx}{r}}|\boldsymbol{\Phi}_k\rangle \qquad (7)\end{aligned}$$

其中 r 为 $C\in Z_n^*$ 模 n 的阶,同时也是函数 $f(x)=C^x(\bmod n)$ 的周期.

5. 对第一个量子寄存器进行量子 Fourier 逆变换,得到

$$\begin{aligned}&\mathrm{QFT}^{-1}:|\Psi_2\rangle\rightarrow|\Psi_3\rangle\\&=\frac{1}{q}\sum_{x=0,c=0}^{q-1}\sum_{k=0}^{r-1}\frac{1}{\sqrt{r}}e^{\frac{-2\pi icx}{q}}e^{\frac{2\pi ikx}{r}}|c\rangle|\boldsymbol{\Phi}_k\rangle\\&=\frac{1}{q\sqrt{r}}\sum_{k=0}^{r-1}\sum_{x=0,c=0}^{q-1}e^{2\pi i\left(\frac{k}{r}-\frac{c}{q}\right)x}|c\rangle|\boldsymbol{\Phi}_k\rangle.\end{aligned}$$

设 $\frac{k}{r}=\varphi_k$,化简得

$$|\Psi_3\rangle=\frac{1}{q\sqrt{r}}\sum_{k=0}^{r-1}\sum_{x=0,c=0}^{q-1}e^{2\pi i(\varphi_k-\frac{c}{q})x}|c\rangle|\boldsymbol{\Phi}_k\rangle \qquad (8)$$

6. 对第一个寄存器进行观测.假设观测到态 $|c_1\rangle$,利用连分数算法可得到满足 $\left|\frac{k_1}{r_1}-\frac{c_1}{q}\right|\leq\frac{1}{2q}$ 的 r_1.如果没有找到满足此式的 r_1,则输出“失败”.

7. 重复步骤 1~5,对第一个寄存器进行观测.假设观测到态 $|c_2\rangle$,利用连分数算法可得到满足 $\left|\frac{k_2}{r_2}-\frac{c_2}{q}\right|\leq\frac{1}{2q}$ 的 r_2.如果没有找到满足此式的 r_2,则输出“失败”.

8. 计算 $r=\mathrm{LCM}(r_1,r_2)$,其中 $\mathrm{LCM}(r_1,r_2)$ 表示 r_1 和 r_2 的最小公倍数,也即得到密文的阶 r.

9. 计算 $M\equiv C^{1/e(\bmod r)}(\bmod n)$,即攻破 RSA.

算法 2 攻击 RSA,没有通过分解 n,也没有利用陷门$\{d,p,q,\varphi(n)\}$的任何信息.仅仅是通过密文 C 就把明文 M 恢复出来,而获得密文在现实攻击中也是最容易满足的条件.因此该攻击属于唯密文攻击.它改变了以往密码分析者试图恢复私钥的做法,直接从恢复消息入手,给出一个对抗 RSA 密码体制的唯密文攻击.

从密码学来看,只要是能从密文中系统地恢复出明文,就是密码破译.算法 2 针对 RSA 的任意密文都可以恢复出明文,因此是对 RSA 的密码破译.不过算法 2 考虑点在于:从非因子分解角度出发破译公钥密码 RSA.即从 RSA 本身破译的传统数学方法出发,是可以不通过因子分解.而传统的方法,都是从因子分解入手的.比如,经典的 Shor 算法就是求解因子分解问题的.

5.2 正确性分析

算法 2 的第 3 步利用 Hadamard 门变换,由文献[17]可知,Hadamard 门变换是一个酉变换.第 4 步所使用的 U_C^x 构造如下:

对于给定的与 n 互素的正整数 C,C 为 RSA 的密文,存在酉变换

$$U_C|y\rangle=|Cy(\bmod n)\rangle$$

且酉变换 U_C 能够被有效执行[17],则 U_C^x 表示酉变换 U_C 的 x 次方,也即

$$U_C^x|y\rangle=|C^xy(\bmod n)\rangle.$$

考虑如下态:

$$|\boldsymbol{\Phi}_k\rangle=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi iks}{r}}|C^s(\bmod n)\rangle \qquad (9)$$

其中,k 表示满足条件 $0\leq k\leq r-1$ 的整数.将酉变换 U_C 作用于量子态 $|\boldsymbol{\Phi}_k\rangle$,得到

$$\begin{aligned}U_C|\boldsymbol{\Phi}_k\rangle&=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi iks}{r}}U_C|C^s(\bmod n)\rangle\\&=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi iks}{r}}|C^{s+1}(\bmod n)\rangle\end{aligned}$$

$$=e^{\frac{2\pi ik}{r}}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi ik}{r}(s+1)}|C^{s+1}(\mathrm{mod}\,n)\rangle$$

$$=e^{\frac{2\pi ik}{r}}|\boldsymbol{\Phi}_k\rangle.$$

因此，量子态$|\boldsymbol{\Phi}_k\rangle$是酉变换$U_C$的本征向量，且$e^{\frac{2\pi ik}{r}}$是对应的本征值. 将酉变换$U_C^x$作用于量子态$|\boldsymbol{\Phi}_k\rangle$，得到

$$U_C^x|\boldsymbol{\Phi}_k\rangle=e^{\frac{2\pi ikx}{r}}|\boldsymbol{\Phi}_k\rangle \tag{10}$$

注意到：r为$C\in Z_n^*$模n的阶，如果$k\equiv 0(\mathrm{mod}\,r)$，则$|C^r(\mathrm{mod}\,n)\rangle=|1\rangle$.

对式(9)求和，也即

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\boldsymbol{\Phi}_k\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi iks}{r}}|C^s(\mathrm{mod}\,n)\rangle \tag{11}$$

由式(11)可知，态$|1\rangle$的振幅为

$$\frac{1}{\sqrt{r}}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{\frac{-2\pi ik}{r}0}=\frac{1}{r}\sum_{k=0}^{r-1}1=1.$$

因为态$|1\rangle$的振幅是1，那么其他所有态的振幅都为0. 因此得到

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\boldsymbol{\Phi}_k\rangle=|1\rangle \tag{12}$$

将式(10)和式(12)代入式(6)可得

$$|\Psi_2\rangle=\frac{1}{\sqrt{qr}}\sum_{x=0}^{q-1}\sum_{k=0}^{r-1}|x\rangle e^{\frac{2\pi ikx}{r}}|\boldsymbol{\Phi}_k\rangle.$$

该式子与等式(7)一致.

而文献[17]指出了量子 Fourier 逆变换是一个酉变换，算法 2 中所使用的变换满足量子计算算法所要求的可逆条件. 因此就算法所使用的变换而言，该算法是正确的. 且图 1 给出实现算法 2 的量子电路图.

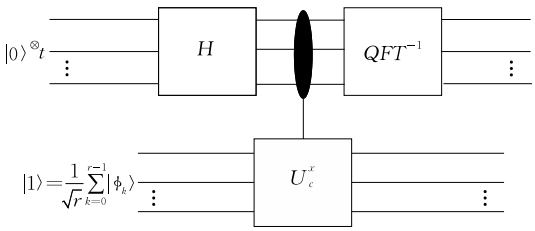


图 1　算法 2 的量子电路图

5.3　成功概率分析

由算法 2 的第 5 步式(8)，如果q是r的整数倍，得到

$$\sum_{x=0}^{q-1}e^{2\pi i(\varphi_k-\frac{c}{q})x}:=\begin{cases}q, & \varphi_k=c/q\\ 0, & \varphi_k\neq c/q\end{cases}.$$

由此可知第一个寄存器中不满足$\varphi_k=c/q$的量子态$|c\rangle$的概率幅为0，在算法 2 第 5 步中第一个寄存器保留下的量子态$|c\rangle$均满足$\varphi_k=c/q$. 由算法 2 的第 5 步的(8)式知：观测到$|c\rangle$的概率为

$$P(c)=\frac{1}{rq^2}\left|\sum_{x=0}^{q-1}e^{2\pi i\left(\varphi_k-\frac{c}{q}\right)x}\right|^2 \tag{13}$$

其中，$\varphi_k=\frac{k}{r}$. 因此所得量子叠加态的每个态$|c\rangle$被观测到的概率为

$$P(c)=\frac{1}{rq^2}\left|\sum_{x=0}^{q-1}e^{2\pi i\left(\varphi_k-\frac{c}{q}\right)x}\right|^2:=\begin{cases}1/r, & \varphi_k=c/q\\ 0, & \varphi_k\neq c/q\end{cases}.$$

而在第 6 步观测到的态$|c\rangle$有r种可能的取值，但是满足$\gcd(c,r)=1$的c只有$\phi(r)$种可能取值，因此第 6 步能正确输出态$|c\rangle$的概率为

$$P=P(c)\times\phi(r)=\frac{\phi(r)}{r}.$$

当q是r的整数倍时，算法 2 的成功概率为$\frac{\phi(r)}{r}$，其中ϕ为欧拉函数.

如果q不是r的整数倍，则由图 2 看到，满足

$$\left|\frac{k}{r}-\frac{c}{q}\right|\leq\frac{1}{2q} \tag{14}$$

的c一定存在于$\{0,1,2,\cdots,q-1\}$中.

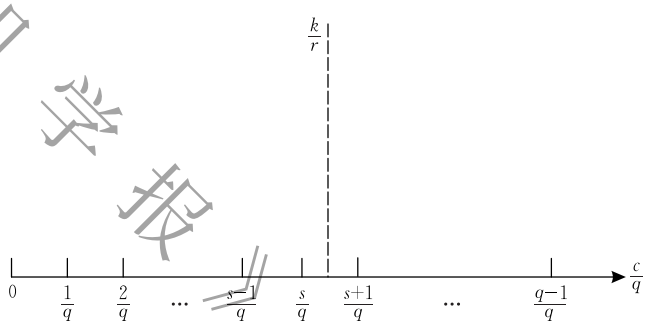


图 2　在q不是r的整数倍的情况下对r的搜索

当满足式(14)时，容易得知相位集中在复平面的上平面或者下平面，此时对x的求和可导致相位的叠加，但如果不满足式(14)，此时对x的求和就导致相位的互相抵消，其大小几乎可以忽略不计. 因此，观测到$|c\rangle$的概率为

$$P(c)=\frac{1}{rq^2}\left|\sum_{x=0}^{q-1}e^{2\pi i(\varphi_k-\frac{c}{q})x}\right|^2$$

$$\approx\begin{cases}1/r, & |k/r-c/q|\leq 1/2q\\ 0, & \text{其他}\end{cases}.$$

从而在q不是r的整数倍的情况下，可以以近似于$\frac{1}{r}$的概率观测到态$|c\rangle$，同样地，这样的态共有$\phi(r)$种可能取值. 因此此种情况下第 6 步能正确输出态$|c\rangle$的概率为

$$P\approx P(c)\times\phi(r)=\frac{\phi(r)}{r}.$$

即在 q 不是 r 的整数倍的情况下,算法 2 的成功概率$\approx\frac{\phi(r)}{r}$.

由上面的分析可知,密文 C 的阶决定算法 2 的成功概率,特别地,当 r 为素数时,算法 2 的成功概率$\approx(r-1)/r$,也即随着 r 的增大,算法的成功概率接近于 1.

定理 7. 算法 2 的成功概率大于 Shor 算法攻击 RSA 的成功概率.

证明. 由定理 2 知,Shor 算法攻击 RSA 的成功概率为 $3\phi(r)/\pi^2 r\leq p<4\phi(r)/\pi^2 r$. 由上面的分析知道,对于算法 2,如果 q 是 r 的整数倍时,算法 2 的成功概率为$\frac{\phi(r)}{r}$. 如果 q 是 r 的整数倍时,算法 2 的成功概率$\approx\frac{\phi(r)}{r}$. 而$\frac{4\phi(r)}{\pi^2 r}<\frac{\phi(r)}{r}$,也即算法 2 的成功概率大于 Shor 算法攻击 RSA 的成功概率. 证毕.

5.4 复杂性分析

算法 2 的第 2 步初始化零态是 $O(\log n)$量子比特的. 第 3 步执行 Hadamard 变换需要 $O(\log n)$规模的基本量子门[17]. 第 4 步所使用的酉变换 U_C^x需要 $O((\log n)^3)$规模的量子门. 第 5 步中的量子 Fourier 变换需要 $O((\log n)^2)$规模的量子门. 第 6 步和第 7 步所使用的连分数需要的量子门规模为 $O((\log n)^3)$. 因此算法 2 所需要的基本量子门规模为 $O((\log n)^3)$.

5.5 实 例

从已有的参考文献来看,人们利用量子计算机只能分解一些诸如 15,21,143 这些数. 因此在此我们也采用同等规模的例子来说明算法 2 的正确性. 具体见例 1.

例 1. 在 RSA 密码体制中,设 RSA 模数 $n=35$,加密指数 $e=11$,密文 $C=13$, 找到明文 M.

1. 计算 $t=\lceil\log 35\rceil=6$,则 $q=2^6=64$.

2. 给定 2 个 6 维量子寄存器,其初态为

$$|\Psi_0\rangle=|0\rangle|1\rangle.$$

3. 对第一个量子寄存器进行 Hadamard 门变换, 产生叠加态

$$H:|\Psi_0\rangle\rightarrow|\Psi_1\rangle=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|1\rangle=\frac{1}{8}\sum_{x=0}^{63}|x\rangle|1\rangle.$$

4. 将酉变换 U_C^x应用到第二个量子寄存器得

$$\begin{aligned}U_C^x:|\Psi_1\rangle\rightarrow|\Psi_2\rangle&=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|C^x(\bmod n)\rangle\\&=\frac{1}{8}\sum_{x=0}^{63}|x\rangle|13^x(\bmod 35)\rangle\\&=\frac{1}{8}(|0\rangle|1\rangle+|1\rangle|13\rangle+|2\rangle|26\rangle+|3\rangle|27\rangle+\\&\quad|4\rangle|1\rangle+|5\rangle|13\rangle+|6\rangle|26\rangle+|7\rangle|27\rangle+\cdots+\\&\quad|60\rangle|1\rangle+|61\rangle|13\rangle+|62\rangle|26\rangle+|63\rangle|27\rangle).\end{aligned}$$

可见在第二个寄存器中,1,13,26,27 等 4 个态杂乱排列. 选择这些态中的一个进行量子 Fourier 逆变换,则将在第一个量子寄存器中以

$$P(c)=\frac{1}{c}\frac{1}{q^2}\left|\sum_{x=0}^{q-1}e^{2\pi i\left(\phi_k-\frac{c}{q}\right)x}\right|^2$$

的几率观测到$|c\rangle$. 在这里,第二个量子寄存器的 k 取 0,1,2,…,$r-1$. 应用量子 Fourier 逆变换之后,对 $q=64$ 绘出的概率分布如图 3 所示.

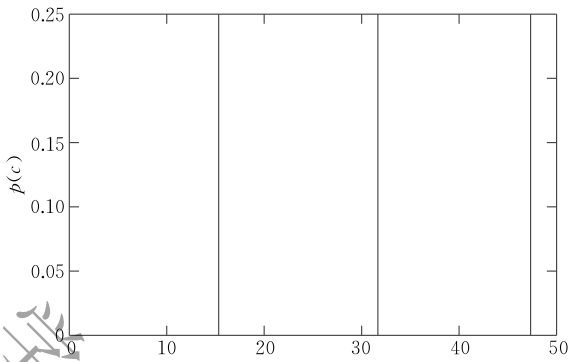


图 3 QFT^{-1}后观察到第一寄存器中态$|c\rangle$的概率,$q=64$

可以看到,对每个 k 的值,使几率接近于 $1/r$ 的 s 值为 $s=16,32,48$ 等.

5. 测量第一个量子寄存器. 假设观测到 $s=16$,利用连分数算法得到 $r_1=4$.

6. 重复步骤 1~4. 测量第一个量子寄存器. 假设观测到 $s=32$,利用连分数算法得到 $r_2=2$.

7. 计算 $r=\mathrm{LCM}(r_1,r_2)=4$,计算

$$\begin{aligned}M&\equiv C^{1/e(\bmod r)}(\bmod n)\\&\equiv 13^{1/11(\bmod 4)}(\bmod 35)\\&\equiv 27.\end{aligned}$$

则输出 $r=4$,且得到明文 $M=27$.

进一步,可验证

$$\begin{aligned}M^e(\bmod n)&=27^{11}(\bmod 35)\\&\equiv 13\\&=C.\end{aligned}$$

即攻破了 RSA.

为了更直观清晰的看出算法 1 和算法 2 的特点以及跟前人在攻击 RSA 方面的不同,在表 1 中,我

们针对各算法在成功概率、时间复杂性、所需要的量子位以及理论基础等方面进行了比较.

表 1　各算法消耗资源对比

攻击RSA算法	成功概率	时间复杂度	量子位	理论基础
文献[6,7]	p_{Shor}	$O((\log n)^{2+\varepsilon})$	$3\lceil\log n\rceil$	因子分解
文献[26]	p_{Shor}	$O((\log n)^{2+\varepsilon})$	$3\lceil\log n\rceil$	因子分解
算法 1	≈ 1	$O(\sqrt{n})$	$\lfloor\log n\rfloor+\left\lceil\log\frac{n}{2}\right\rceil$	因子分解
算法 2	$\frac{\phi(r)}{r}$	$O((\log n)^{2+\varepsilon})$	$3\lceil\log n\rceil$	非因子分解

其中 $3\phi(r)/\pi^2 r\leq p_{\text{Shor}}<4\phi(r)/\pi^2 r$.

通过表 1，我们可以看出：算法 1 具有如下特点：(1) 基于因子分解实现攻击 RSA 的，即算法 1 是对经典同余方程 $\alpha^2\equiv\beta^2(\bmod n)$ 的量子化实现；(2) 相比于 Shor 算法，算法 1 所需量子位少；(3) 具有亚指数时间复杂度；(4) 成功概率接近于 1. 算法 2 具有如下特点：(1) 基于非因子分解实现攻击 RSA 的，从目前查到的文献来看，还没有从非因子分解角度考虑攻击 RSA 的量子算法；(2) 同 Shor 算法所需量子位相同；(3) 具有多项式时间复杂度；(4) 成功概率高于 Shor 算法攻击 RSA 的成功概率.

6　总结与下一步工作

整数分解问题是一个古老的难解问题，然而到目前为止，还没有一个有效的整数分解算法. 整数分解在现代密码研究中有着重要的应用. 比如说 RSA 公钥密码体制的安全性正是基于整数分解的难解性，为此其提出者 Rivest，Shamir 和 Adleman 获得了 2002 年图灵奖. 经典的因子分解算法大都是通过求解同余方程 $\alpha^2\equiv\beta^2(\bmod n)$ 实现的. 目前还没有对此方程求解的量子算法，故我们从这个角度做了尝试，基于 Grover 搜索，提出求解 $\alpha^2\equiv\beta^2(\bmod n)$ 的量子算法，这是本文的一个创新点. 虽然该算法的计算复杂性是亚指数的，但这是第一个求解同余方程 $\alpha^2\equiv\beta^2(\bmod n)$ 的量子算法. 算法 1 所需要的量子位数比 Shor 算法所需要的量子位数少，且算法 1 的成功概率接近 1.

众所周知，如果整数分解问题得以解决，那么我们就可攻破 RSA；然而，攻破 RSA 却不一定要通过解决整数分解问题. 因此我们可以考虑从非因子分解角度出发，发现通过计算密文 C 的阶，可以恢复出明文 M. 也就是说不用通过分解模数 n 也能攻破 RSA. 因此基于量子 Fourier 逆变换和相位估计，我们给出了一个不通过因子分解攻击 RSA 的量子算法，即算法 2. 算法 2 具有多项式计算复杂性. 与 Shor 算法相比，算法 2 不需要分解 n 而从 RSA 密文 C 直接恢复出明文 M，且成功概率高于 Shor 算法攻击 RSA 的成功概率. 同时不必要满足密文的阶为偶数.

到目前为止，Shor 算法仅适合快速求解某些周期性的问题(整数分解问题、离散对数问题、椭圆曲线离散对数问题、Pell 方程求解等，都可归约到函数周期的计算问题上来)，而对于那些非周期性问题，Shor 算法是否也能求解，这是个有意义的研究方向，仍是一个需要深入研究的问题.

致　谢　审稿专家对本文提出了宝贵的修改意见，在此对审稿专家表示由衷的感谢！

参　考　文　献

[1] Zhang Huan-Guo, Han Wen-Bao, Lai Xue-Jia, et al. Survey on cyberspace security. Science China Information Sciences, 2016, 46(2): 125-164(in Chinese)
(张焕国，韩文报，来学嘉等. 网络空间安全综述. 中国科学：信息科学，2016，46(2)：125-164)

[2] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126

[3] Yan S Y. Quantum Computational Number Theory. Berlin, Germany: Springer, 2015

[4] Lenstra A K, Lenstra H W Jr eds. The development of the number field sieve. Lecture Notes in Mathematics 1554. Berlin, Germany: Springer, 1993

[5] Cécile P. The multiple number field sieve with conjugation and generalized Joux-Lercier methods//Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Solfla, Bulgaria, 2015: 156-170

[6] 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

[7] 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

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

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

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

[11] Wu W Q, Zhang H G, Wang H Z, Mao S W. Polynomial-time quantum algorithms for finding the linear structures of Boolean function. Quantum Information Process, 2015, 14(4): 1215-1226

[12] Zhang Huan-Guo, Mao Shao-Wu, Wu Wan-Qing, et al. Overview of quantum computation complexity theory. Chinese Journal of Computers, 2016, 39(12): 2403-2428(in Chinese)
(张焕国, 毛少武, 吴万青等. 量子计算复杂性理论综述. 计算机学报, 2016, 39(12): 2403-2428)

[13] Wu Nan, Song Fang-Min, LI Xiang-Dong. Universal quantum computer: Theory, organization and implementation. Chinese Journal of Computers, 2016, 39(12): 2429-2445(in Chinese)
(吴楠, 宋方敏, LI Xiang-Dong. 通用量子计算机: 理论、组成与实现. 计算机学报, 2016, 39(12): 2429-2445)

[14] 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. Computational Intelligence and Neuroscience, 2016, 2016(2): 1-17

[15] Fu Xiang-Qun, Bao Wan-Su, Wang Shuai. Quantum algorithm for discrete logarithm over Z_N. Chinese Journal of Computers, 2014, 37(5): 1058-1062(in Chinese)
(付向群, 鲍皖苏, 王帅. Z_N上离散对数量子计算算法. 计算机学报, 2014, 37(5): 1058-1062)

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

[17] Nielson M A, Chuang I L. Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge, UK: Cambridge University Press, 2010

[18] Vandersypen L M K, Steffen M, Breyta G, et al. Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance. Nature, 2001, 414(6866): 883-887

[19] Ignacio G M, Klausm F, Shepelyansky D L. Effects of imperfections for Shor's factorization algorithm. Physical Review A, 2007, 75(5): 052311

[20] Yang C, Daniel L, Browne E, et al. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. Physical Review Letters, 2007, 99(99): 250504

[21] Peng X H, Liao Z Y, Xu N Y, Qin G, et al. Quantum adiabatic algorithm for factorization and its experimental implementation. Physical Review Letters, 2008, 101(22): 220405

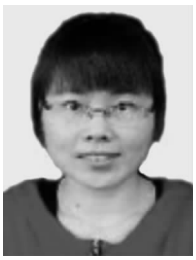
[22] Xu N Y, Zhu J, Lu D W, et al. Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. Physical Review Letters, 2012, 108(13): 130501

[23] Lucero E, Barends R, Chen Y, et al. Computing prime factors with a Josephson phase qubit quantum processor. Nature Physics, 2012, 8(10): 719-723

[24] Geller M R, Zhou Z Y. Factoring 51 and 85 with 8 qubits. Scientific Reports, 2013, 3(3023): 1-5

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

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



WANG Ya-Hui, born in 1988, Ph.D. candidate. Her current research interests include quantum computing and cryptography.

ZHANG Huan-Guo, born in 1945, Ph. D., professor, Ph. D. supervisor. His current research interests include information security, cryptography and trusted computing.

WU Wan-Qing, born in 1981, Ph. D., lecturer. His current research interests include information security and quantum computing.

HAN Hai-Qing, born in 1979, Ph. D. His current research interests include quantum computing and cryptography.

Background

This work is supported by the State Key Program of National Natural Science of China (Grant No. 61332019), the Major State Basic Research Development Program (973 Program) of China (No. 2014CB340601), the National Science Foundation of China (Grant Nos. 61303212, 61202386), and the Major Research Plan of the National Natural Science Foundation of China (Grant No. 91018008).

The development of quantum computation presents a serious challenge to the existing public-key cryptosystems, and the public-key cryptosystems, RSA, ELGamal, etc. are

broken by using Shor's algorithm. Therefore, it is of great significance to study the cryptanalysis in the quantum computing environment. The essential trick to breaking the RSA public-key cryptosystem is a method for factoring modulus n efficiently. Since Shor proposed a quantum integer factorization algorithm which can solve IFP and break RSA both in polynomial-time, various improved and compiled versions of Shor's algorithm using different technics have been proposed and studied. In short, there are two important research directions in quantum integer factorization: (1) with fewer quantum bits. (2) compiled version of Shor's algorithm.

Therefore, there are two aspects that need to be improved. One is that how to present a quantum algorithm for breaking RSA with fewer qubits. Based on Grover search, a quantum algorithm for finding the pair of solutions (α,β) to the square congruence $\alpha^2\equiv\beta^2 \pmod n$ is presented. The algorithm runs in sub-exponential time, but this is the first quantum algorithm for solving the square congruence $\alpha^2\equiv\beta^2 \pmod n$. And compared to Shor's algorithm, the algorithm requires fewer quantum bits. Another is that how to design the compiled version of Shor's algorithm. So based on the quantum inverse Fourier transform and phase estimation, a polynomial-time quantum algorithm for directly recovering the RSA plaintext M from the ciphertext C without explicitly factoring the modulus n is presented, and hence, breaks the famous RSA public-key cryptosystem. The algorithm runs in polynomial-time $O((\log n)^3)$.