一种新的攻击RSA的量子算法

王亚辉 颜松远
(武汉大学计算机学院 武汉 430072)

摘 要 整数分解是数论中一个非常古老的难解性问题,而对于当今世界上最有名且广泛使用的RSA公钥密码体制,其安全性是基于整数分解的难解性的。迄今为止,最有希望破解RSA的方法就是Shor的量子算法。利用RSA不动点性质,基于量子Fourier变换和变量代换,提出了一种新的攻击RSA的量子算法。该算法不需要分解n,而是从RSA密文C中直接恢复其明文M。该算法与Shor算法相比,需要的量子位更少,且成功概率大于1/2。最后将新算法的资源消耗情况与Shor算法的进行了对比。

关键词 量子Fourier变换,RSA密码,量子算法,信息安全
中图法分类号 TP301.6 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.004

New Quantum Algorithm for Breaking RSA

WANG Ya-hui YAN Song-yuan
(Computer School, Wuhan University, Wuhan 430072, China)

Abstract It is well known that the security of the most famous and widely used public-key cryptosystem RSA relies on the computational intractability of the integer factorization problem. In this paper, by a combined use of the fixed-point property of RSA, multiple Fourier transforms and variable substitution, a new quantum algorithm for directly recovering the RSA plaintext M from the ciphertext C was presented, without explicitly factoring the modulus n. Compared to Shor's quantum algorithm, the new algorithm requires fewer quantum bits. The probability of success of the new algorithm is bigger than 1/2. Moreover, a comparison of the required resources between our algorithm and Shor's was presented.

Keywords Quantum Fourier transform, RSA cryptography, Quantum algorithm, Information security

1 引言

整数分解在经典计算中是一个难解性问题,目前广泛使用的RSA公钥密码算法[1]正是基于它的难解性设计的。众所周知,破译RSA最简单、最直接的办法就是分解RSA模数n(一般来讲,n是一个具有至少1024个二进制位的大合数)。

目前整数分解快速算法的基本思想是找到正整数对(α,β)使得$\alpha\neq\pm\beta \pmod n$且$\alpha^2\equiv\beta^2 \pmod n$成立,一旦找到整数对$(\alpha,\beta)$,那么通过计算$\gcd(\alpha\pm\beta,n)$,就能以大于1/2的概率得到$n$的因子。在经典领域最快的整数分解算法是数域筛法(NFS)[2,3],但其复杂性是亚指数的,即$O(\exp(c(\log n)^{1/3}(\log\log n)^{2/3}))$。然而,Shor于1994年提出了一种整数分解的量子多项式复杂性算法[4],给量子计算的研究注入了新的活力,引发了近几年来量子计算和量子计算机研究的热潮。文献[5]讨论说明了如何把一些现代密码体制归结为隐子群上的问题,从而用量子算法进行分析。

2001年,美国IBM公司纽约实验室与斯坦福大学固体和光学实验室合作,利用核磁共振技术实验实现了Shor算法对15的分解[6],但该实验不能显示其量子属性,也无法扩展到更多的比特,其进一步的应用受到限制。2004年,中国科学技术大学合肥微尺度国家实验室杜江峰教授领导的课题组首次提出了基于绝热量子计算的质因子分解算法,并成功地在实验中实现了21的分解[7]。2012年,合肥微尺度国家实验室Nanyang Xu等人通过绝热理论并结合二进制乘法表,构造了Hamiltonian H_p,利用核磁共振量子处理器(NMR)实现了143的分解[8]。2013年,M. R. Geller等人发现,对于具有某些特殊性质的Fermat数,并不需要通常所需的那么多的量子位,比如分解51和85仅需要8个qubits[9]。但是这些特殊的情况很难推广到一般的情形。

Shor算法的主要思想在于把因子分解问题转化为求函数的周期问题。新算法则是根据RSA不动点的性质,利用量子计算技巧将不动点攻击问题转化为了求函数周期问题。

本文首先介绍一些与RSA密码分析有关的基础知识和基于量子整数分解的Shor算法,然后讨论并介绍不基于整数分解的直接破译RSA的量子计算新算法,最后将对新算法和Shor算法进行分析比较,并给出进一步实现该算法的研究方向。

2 基础知识

首先介绍一些与RSA密码分析有关的基础知识,更多信

到稿日期:2015-06-10 返修日期:2015-07-20
王亚辉(1988-),女,博士生,主要研究方向为密码学与信息安全,E-mail:wangyh_ecc@whu.edu.cn;颜松远(1954-),男,博士,教授,主要研究方向为计算数论、密码学和信息安全,E-mail:songyuanyan@whu.edu.cn(通信作者)。

息请参考文献[10-13]。

定义 1[13] 对于任意的 $a\in Z_n^*$，如果 r 是最小的使得 $a^r\equiv 1(\bmod n)$ 的正整数，则 r 称为 a 模 n 的阶，记为：order (a,n)。

定义 2[13] 在 RSA 密码体制[10]中，加密和解密过程如下：

$$C\equiv M^e(\bmod n),M\equiv C^d(\bmod n)$$

其中，

(1)(M,C)分别是明文和密文；

(2)$n=pq$ 是模数，其中 p 和 q 是不同的素数；

(3)$ed\equiv 1(\bmod \phi(n))$，其中$(e,d)$分别是加密指数和解密指数，$(e,n)$是公钥，$(d,p,q)$是私钥。

定义 3 RSA 问题定义如下：

给出 $e\equiv 1/d(\bmod (p-1)(q-1)),n=pq,C\equiv M^e(\bmod n)$。找到 M 或者 d。

定义 4[12] 给定 e,n。设 $0\leqslant x\leqslant n$，如果

$$x^{e^k}\equiv x(\bmod n),k\in Z^+$$

则 x 称为 RSA 的不动点，且 k 为不动点的阶。

定理 1[12] 设 C 是 RSA 的不动点，且阶为 k。

$$C^{e^k}\equiv C(\bmod n),k\in Z^+$$

则

$$C^{e^{k-1}}\equiv M(\bmod n),k\in Z^+$$

其中，M 是明文，C 是密文，e 是加密指数。

证明：因为 RSA 的密文：$C\equiv M^e(\bmod n)$是对消息空间$\{0,1,2,n-1\}$的预处理，因此不动点一定存在，即满足

$$C^{e^k}\equiv C(\bmod n)$$

的密文 C 存在。因为

$$\begin{aligned}&C^{e^k}\equiv C(\bmod n)\\&\Rightarrow C^{e^k}\equiv M^e(\bmod n)\\&\Rightarrow C^{e^{k-1}e}\equiv M^e(\bmod n)\\&\Rightarrow (C^{e^{k-1}})^e\equiv M^e(\bmod n)\\&\Rightarrow C^{e^{k-1}}\equiv M(\bmod n)\end{aligned}$$

推论 1 如果找到函数 $f(x)\equiv C^{e^x}(\bmod n)$的周期 r，则由定理 1 可知：RSA 可被攻破，也即 $M\equiv C^{e^{r-1}}(\bmod n)$。

引理 1[11] 设 $n=p_1^{a_1}\cdots p_m^{a_m}$ 是一个正奇合数的素因子分解，令 x 是在 $1\leqslant x\leqslant n-1$ 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

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

推论 2 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 $p\geqslant 3/4$。

定义 5[11] 量子 Fourier 变换定义为：在一组标准正交基 $|0\rangle,|1\rangle\cdots,|N-1\rangle$上的一个线性算子，在基态上的作用为

$$|j\rangle\mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{2\pi ijk/N}|k\rangle$$

那么对任意量子态的变换可写作

$$\sum_{j=0}^{N-1}x_j|j\rangle\mapsto\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}x_j e^{2\pi ijk/N}|k\rangle$$

其中，“$\mapsto$”表示变换可逆。

注 1 文献[11]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 Shor 量子分解算法

Shor 于 1994 年提出了量子整数分解算法[4,14]，其核心在于把因子分解问题转化成了寻找函数的周期问题，从而使用量子 Fourier 变换求解周期问题。Shor 算法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 $n^2\leqslant q=2^k\leqslant 2n^2$。

2. 给定两个量子寄存器，且初始化为零态，即$|0^k\rangle|0^k\rangle$，对第一个量子寄存器执行 Hadamard 变换，得到叠加态：

$$|0^k\rangle|0^k\rangle\mapsto\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|0\rangle$$

3. 做量子黑盒计算：

$$\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|0\rangle\mapsto\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|a^x(\bmod n)\rangle$$

4. 对第一个量子寄存器执行量子 Fourier 变换：

$$\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|a^x(\bmod n)\rangle\mapsto\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}\sum_{c=0}^{q-1}e^{\frac{2\pi icx}{q}}|c\rangle|a^x(\bmod n)\rangle$$

5. 对第二个量子寄存器进行观测，假设观测到 a^t，此时两个量子寄存器的态为：

$$\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}\sum_{c=0}^{q-1}e^{\frac{2\pi icx}{q}}|c\rangle|a^x(\bmod n)\rangle\mapsto\frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\sum_{k=0}^{\lfloor(q-t-1)/r\rfloor}e^{\frac{2\pi i(kr+t)c}{q}}|c\rangle|a^t(\bmod n)\rangle$$

6. 对第一个寄存器进行观测，假设观测到$|c\rangle$，利用连分数法计算出 r，然后判断是否为元素 a 的阶 r，如果是，则算法结束；否则返回第 1 步，直到找到正确的阶 r。

注 2 Shor 量子分解算法总共所需量子位为 $3\lceil\log n\rceil$。

注 3 Shor 通过证明得出运行一次算法的成功概率为 $4\phi(r)/\pi^2 r$，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 算法的成功概率依赖于元素 a 模 n 的阶 r。

基于 Shor 量子求阶算法，可以对整数 n 进行分解，从而攻破 RSA，具体如下：

利用 Shor 算法求出元素 a 模 n 的阶 r，如果 r 是奇数，重新选择 a；如果 r 是偶数，则计算 $d=\gcd(a^{r/2}\pm 1,n)$，如果 $d\neq 1$，则 d 就是 n 的因子，否则重新选择 a 进行计算。

定理 2 利用 Shor 算法攻击 RSA 的成功概率 $3\phi(r)/\pi^2 r\leqslant p<4\phi(r)/\pi^2 r$。

证明：由推论 2 和注 2 可知。

4 新的攻击 RSA 的量子算法

Shor 算法是通过求元素的阶，进而分解模数 n 从而攻破 RSA 的。而这一节提出的新算法则是利用 RSA 不动点的性质，基于量子 Fourier 变换和变量代换，不分解 n 而直接攻破 RSA。具体算法如下。

算法 1 新的攻击 RSA 的量子算法

输入：C,e,n

输出：r

1. 找 $q=2^k$，其中 $k=3\lceil\log_e n\rceil$。

2. 给定 3 个 k 维量子寄存器，其初态为$|\psi_0\rangle=|0^k,0^k,0^k\rangle$。

3. 对前两个量子寄存器进行量子 Fourier 变换，产生叠加态

$$\mathrm{QFT}:|\psi_0\rangle\rightarrow|\psi_1\rangle=\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle|y\rangle|0\rangle$$

4. 做量子黑盒变换

$$U_f:|\psi_1\rangle\rightarrow|\psi_2\rangle=\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle|y\rangle|C^x(\bmod n)\rangle$$

然后对第三个寄存器进行观测，假设此时观测到 C^t，其中 $0\leqslant t\leqslant r-1$，由量子坍缩原理及 $C^x=C^{x+yr}\equiv C^t \bmod n$ 可知，前两个寄存器坍缩后的量子叠加态为：

$$|\psi_3\rangle=\frac{1}{\sqrt{q}}\sum_{y=0}^{q-1}|t-yr\rangle|y\rangle$$

5. 对前两个量子寄存器分别进行量子 Fourier 变换，得到：

$$\begin{aligned}QFT:|\psi_3\rangle\rightarrow|\psi_4\rangle&=\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}\sum_{\mu=0}^{q-1}\sum_{\nu=0}^{q-1}e^{\frac{2\pi i(t-yr)\mu}{q}}e^{\frac{2\pi iy\nu}{q}}|\mu,\nu\rangle\\&=\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}\sum_{\mu=0}^{q-1}\sum_{\nu=0}^{q-1}w_q^{t\mu+y(\nu-r\mu)}|\mu,\nu\rangle\\&=\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}\sum_{\nu\equiv r\mu \bmod d}w_q^{y(\nu-r\mu)}w_q^{t\mu}|\mu,\nu\rangle\\&=\frac{1}{\sqrt{q}}\sum_{\mu=0}^{q-1}w_q^{t\mu}|\mu,\nu\rangle\end{aligned}$$

其中，$w_q=e^{\frac{2\pi i}{q}}$。

6. 对前两个寄存器进行观测，不妨假设观测到$(\mu,\mu r)$。计算 $d=\gcd(\mu,n)$，如果 $d\neq 1$，则输出 d；否则执行第 7 步。

7. 有两种方法可得到结果。

方法 1　由第 6 步知，对前两个寄存器进行观测，可得到$(\mu,\mu r)$，且 μ 和 μr 满足 $\gcd(\mu,n)=1$ 且 $\nu\equiv r\mu \bmod q$，当 $\gcd(\mu,q)=1$ 时，算法输出 $r\equiv\mu^{-1}(\mu r)(\bmod q)$；否则算法输出失败。

方法 2　由第 6 步知，对前两个寄存器进行观测，可得到$(\mu,\mu r)$，此时再次运行算法并进行观测得到不同的 $(\mu',\mu' r)$。因 $\gcd(\mu,\mu')=1$，故存在 λ 和 λ'，使得

$\lambda\mu+\lambda'\mu'=1$

在上式两边同时乘以 r，得到

$\lambda\mu r+\lambda'\mu' r\equiv r(\bmod n)$

从而 r 即为所求。

进一步，计算 $M\equiv C^{e^{r-1}}(\bmod n)$ 即为 RSA 的明文，从而攻破 RSA。

下面对算法 1 作正确性分析。

算法 1 的核心是量子 Fourier 变换的使用，文献[6]指出量子 Fourier 变换是一个酉变换，满足量子计算算法所要求的可逆条件，算法 1 中第 4 步所使用的并行计算同样也是一个可逆计算，因此就算法 1 本身所使用的变换而言，该算法是正确的，在量子计算机上可以得到有效的实现。

再者，注意到

$$\sum_{y=0}^{q-1}w_q^{t\mu+y(\nu-r\mu)}:=\begin{cases}qw_q^{t\mu}, & \nu\equiv r\mu \bmod q\\0, & \nu\not\equiv r\mu \bmod q\end{cases}$$

因此

$$\begin{aligned}&\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}\sum_{\mu=0}^{q-1}\sum_{\nu=0}^{q-1}w_q^{t\mu+y(\nu-r\mu)}|\mu,\nu\rangle\\&=\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}\sum_{\nu\equiv r\mu \bmod q}w_q^{y(\nu-r\mu)}w_q^{t\mu}|\mu,\nu\rangle\end{aligned}$$

由此可知前两个寄存器中不满足 $\nu\equiv r\mu \bmod q$ 的量子态 $|\mu\rangle|\nu\rangle$ 的几率幅为 0，正如第 5 步中呈现的，前两个寄存器保留下的量子态 $|\mu\rangle|\nu\rangle$ 均满足 $\nu\equiv r\mu \bmod q$。

为了进一步说明算法的正确性，下面给出一个实例。

例 1　设 $n=33,e=7,C=14$。

1. 计算 $k=3\lceil\log_7 33\rceil=6$，则 $q=2^6=64$。

2. $|\psi_0\rangle=|0^6,0^6,0^6\rangle$。

3. $$QFT:|\psi_0\rangle\rightarrow|\psi_1\rangle=\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle|y\rangle|0\rangle$$

$$=\frac{1}{64}\sum_{x=0}^{63}\sum_{y=0}^{63}|x\rangle|y\rangle|0\rangle$$

4. $$U_f:|\psi_1\rangle\rightarrow|\psi_2\rangle=\frac{1}{64}\sum_{x=0}^{63}\sum_{y=0}^{63}|x\rangle|y\rangle|14^{7x}(\bmod 33)\rangle$$

此时第三个寄存器：

$[14,20,26,5,14,20,26,5,\cdots,14,20,26,5,14]$

假设此时观测第三个寄存器的结果为 5，则剩下的叠加态为：

$$|\psi_3\rangle=\frac{1}{64}(|3\rangle|0\rangle+|63\rangle|1\rangle+|59\rangle|2\rangle+\cdots+|3\rangle|16\rangle+\cdots+|7\rangle|63\rangle)$$

5. 对前两个量子寄存器进行 Fourier 变换，得到叠加态

$$QFT:|\psi_3\rangle\rightarrow|\psi_4\rangle=\frac{1}{64\sqrt{64}}\sum_{\mu=0}^{63}\sum_{\nu=0}^{63}(w_{64}^{3\mu}+w_{64}^{63\mu+\nu}+w_{64}^{59\mu+2\nu}+w_{64}^{55\mu+3\nu}+\cdots+w_{64}^{3\mu+16\nu}+\cdots+w_{64}^{7\mu+63\nu})|\mu\rangle|\nu\rangle$$

故量子态 $|\mu\rangle|\nu\rangle$ 的几率幅为

$$A=\frac{1}{64\sqrt{64}}(w_{64}^{3\mu}+w_{64}^{63\mu+\nu}+w_{64}^{59\mu+2\nu}+\cdots+w_{64}^{3\mu+16\nu}+\cdots+w_{64}^{7\mu+63\nu})$$

由 $63\mu+\nu\equiv 59\mu+2\nu\equiv 55\mu+3\nu\equiv\cdots\equiv 3\mu+16\nu\equiv\cdots\equiv 7\mu+63\nu\equiv 3\mu \bmod 64$，即 $v\equiv 4\mu \bmod 64$，$A=\frac{1}{\sqrt{64}}w_{64}^{3\mu}$ 可见，当 $|\mu\rangle|\nu\rangle=|0\rangle|0\rangle,|1\rangle|4\rangle,\cdots,|17\rangle|4\rangle,\cdots,|23\rangle|28\rangle,\cdots|63\rangle|60\rangle$ 时，$A\neq 0$；当 $|\mu\rangle|\nu\rangle\neq|0\rangle|0\rangle,|1\rangle|4\rangle,\cdots,|17\rangle|4\rangle,\cdots,|23\rangle|28\rangle,\cdots,|63\rangle|60\rangle$ 时，$A=0$。因此，$|0\rangle|0\rangle,|1\rangle|4\rangle,\cdots,|17\rangle|4\rangle,\cdots,|23\rangle|28\rangle,\cdots,|63\rangle|60\rangle$ 以较高的概率读出，其他的态以接近于 0 的概率读出。

6. 对前两个寄存器进行观测，不妨假设观测到$(17,4)$。计算 $d=\gcd(17,33)=1$，故执行第 7 步。

7. 有两种方法可得到结果。

方法 1　由第 6 步知，对前两个寄存器进行观测，可得到 $|17\rangle|4\rangle$，因为 $\gcd(17,64)=1$，所以算法输出 $r\equiv 17^{-1}(4)(\bmod 64)\equiv 4$，即为所求。

方法 2　由第 6 步知，对前两个寄存器进行观测，可得到 $|17\rangle|4\rangle$；再次运行算法 1，并进行测量，不妨假设这次观测到不同的态 $|23\rangle|28\rangle$，因为 $\gcd(17,23)=1$，所以存在 $\lambda=3,\lambda'=-4$，使得 $23\lambda+17\lambda'=1$，两边同时乘以 r，即 $28\lambda+\lambda'\equiv 4 \bmod 64$，从而也即 $r=4$，即为所求。

进一步，计算 $M\equiv 14^{7^{4-1}}(\bmod 33)=5$，即为 RSA 的明文，从而攻破 RSA。

定理 3　算法 1 是多项式算法，其计算复杂性为 $O(c(\log n)^{2+\epsilon})$，当 $n\rightarrow\infty$。

证明：算法 1 的主要计算在于量子 Fourier 变换，其计算复杂性为 $O(c(\log n)^2\log\log n\log\log\log n)$。而 gcd 计算也需要多项式时间 $O((\log n)^2)$。因此，算法 1 是多项式算法，且其计算复杂性为：$O(c(\log n)^2\log\log n\log\log\log n)=O(c(\log n)^{2+\epsilon})$，当 $n\rightarrow\infty$。

定理 4　实现算法 1 所需量子位为 $6\lceil\log_2 n\rceil$，当 $e>8$ 时，$3\lceil\log_2 n\rceil>\lceil\log n\rceil$，也即当 $e>8$ 时，实现算法 1 所需量子位少于 Shor 量子分解算法。

证明：设函数 $f(x)\equiv C^x(\bmod n)$ 的周期为 r_1，函数 $g(x)\equiv C^x(\bmod n)$ 的周期为 r_2，则 $er_1=kr_2+1,k\leqslant\left\lceil\frac{n}{r}\right\rceil$，故

取$q=2^k$，$k=3\lceil \log_e n \rceil$，可保证一次算出的函数值足够多，使得能够确定第三个寄存器中函数的周期。因此实现算法1总共需要量子位$6\lceil \log_e n \rceil$，显然，当$e>8$时，$3\lceil \log_e n \rceil > \lceil \log n \rceil$。即$6\lceil \log_e n \rceil > 3\lceil \log n \rceil$（因为Shor算法所需量子位为$3\lceil \log n \rceil$），从而当$e>8$时，实现算法1共需量子位少于Shor量子分解算法所需量子位。

定理5 算法1执行一次的成功概率为：$p=p_1+p_2=\frac{n-\phi(n)-1}{n}+\frac{1}{2}$。

证明：如果$d\neq 1$，且$d\neq 0$，则$d|n$，可得到n的一个因子，因为n是两个素数的乘积，考虑到有$\phi(n)$个数与n互素，因此观测到μ的概率为$\frac{n-\phi(n)-1}{n}$，此时n能被分解的概率为$p_1=\frac{n-\phi(n)-1}{n}$。

如果$d=1$，则经过第5步的Fourier变换后，前两个寄存器的叠加态中的每个态$|\mu\rangle|\nu\rangle$被观测到的概率p'为

$$|\frac{1}{q\sqrt{q}}\sum_{y=0}^{q-1}w_q^{(t-yr)\mu}w_q^{y\nu}|^2:=\begin{cases}\frac{1}{q}, & \nu\equiv r\mu \bmod q\\ 0, & \nu\not\equiv r\mu \bmod q\end{cases}$$

而在第7步观测到的μ、ν有q种可能取值，但$\gcd(\mu,q)=1$只有$\phi(q)$种可能取值，因此第6步能够正确输出$r\equiv\mu^{-1}(\mu r)(\bmod q)$的概率为

$$p_2=p'\times\phi(q)=\frac{\phi(q)}{q}=\frac{1}{2}$$

所以$p=p_1+p_2=\frac{n-\phi(n)-1}{n}+\frac{1}{2}$即为算法1的成功概率，其中$\phi$为欧拉函数。

定理6 实现算法1的量子线路所需要量子逻辑门规模为$O(k^3)$。

证明：算法1的初态$|0\rangle$是k量子比特的，执行1个Hadamard变换需要$O(k)$规模的量子逻辑门[6]，实现1个量子Fourier变换需要$O(k^2)$规模的量子逻辑门，因此，算法1中的4个量子Fourier变换依然需要$O(k^2)$规模的量子逻辑门。因为模幂运算所需要的量子逻辑门规模为$O(k^3)$[15]，故算法1的第三个寄存器中的模幂运算所需要的量子逻辑门规模为$O(k^3)$，因此实现整个算法1的量子线路所需要量子逻辑门规模为$O(k^3)$。

结束语 RSA[1]是当今计算机安全领域最有名、应用最为广泛的密码体制，为此其研制者Rivest、Shamir和Adleman获得2002年的图灵奖。为了研究RSA密码的安全性，必须研究各种可能的攻击、破译RSA的方法[12]。本文利用RSA不动点的性质，基于量子Fourier变换和变量代换的技巧，提出了一个新的攻击RSA的量子多项式复杂性算法。该算法不需要分解n，而从RSA密文C中直接恢复其明文M，其成功的概率大于1/2。它所需的量子门规模与Shor算法一样，依然为$O(k^3)$。与Shor算法相比，新算法需要比较少的量子位，这就降低了对通用量子计算机的器件要求，提高了采用通用量子计算机破译公钥密码的可能性。目前所有量子整数分解算法（如文献[8,9,16,17]中介绍的算法）都只能分解一些很小的整数，远远达不到实用的目的，并且不能对现行的RSA体制构成威胁。因此，建造数千个量子位的实用量子计算机（硬件），或者研制量子位需求少但功能强大的量子分解算法（软件），是当前量子计算尤其是量子整数分解的两个主要研究方向。

参考文献

[1] Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems [J]. Communications of the ACM, 1978, 21(6): 120-126

[2] Lenstra A K, Lenstra Jr H W, et al. The Development of the Number Field Sieve [M]. Springer-Verlag, 1993

[3] Kleinjung T, Aoki K, Lenstra A K, et al. Factorization of a 768-Bit RSA modulus [C]// Lecture Notes in Computer Science 6223. Springer, 2010: 333-350

[4] Shor P W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring [C]// Proc of 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1994: 124-134

[5] Lu X, Feng D G. Quantum Analysis of Modern Cryptosystems [J]. Computer Science, 2005, 32(2)(in Chinese)
吕欣，冯登国. 密码体制的量子算法分析[J]. 计算机科学，2005，32(2)

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

[7] Peng X H, Liao Z Y, Xu N Y, et al. A Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation [J]. Physical Review Letters, 2008, 101(22): 4473-4475

[8] 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): 4089-4091

[9] Geller M R, Zhou Z Y. Factoring 51 and 85 with 8 Qubits [J]. Scientific Report, 2013, 3(10): 3023

[10] Cohen H. A Course in Computational Algebraic Number Theory [M]// Graduate Texts in Mathematics 138. New York: Springer, 1993

[11] Nielson M A, Chuang I L. Quantum Computation and Quantum Information [M]. Cambridge: Cambridge University Press, 2000

[12] Yan S Y. Cryptanalytic Attacks on RSA [M]. New York: Springer, 2010

[13] Yan S Y. Computational Number Theory and Modern Public-Key Cryptography [M]. Wiley and Higher Education Press, 2013

[14] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [J]. SIAM Journal on Computing, 1997, 41(2): 1484-1509

[15] Zallka C. Fast Versions of Shor's Quantum Factoring Algorithm [DB]. arXiv: Quant-ph/9806084v1, 1998

[16] Dattani N S, Bryans N. Quantum Factorization of 56153 with only 4 Qubits [DB]. arXiv: 1411. 6758v3[quant-ph], Nov 2014

[17] Smolin J A, Vargo A. Oversimplifying Quantum Factoring [J]. Nature, 2013, 499(7457): 163-165