具有高概率的整数分解量子算法

付向群,鲍皖苏,周 淳,钟普查
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文基于量子 Fourier 变换给出了一个新的整数分解量子算法,通过利用多次量子 Fourier 变换和变量代换,使得 r 变成相位因子(r 是从模 N 整数环中所选元素的阶),进而可使非零的非目标态的几率幅变为零,算法成功的概率大于 3/4,高于 Shor 整数分解量子算法,且不再依赖于 r 的大小(Shor 算法成功的概率依赖于 r 的大小),同时还将新算法的资源消耗情况与 Shor 算法进行了对比.

关键词: 量子算法; 整数分解; 公钥密码; 量子 Fourier 变换
中图分类号: TN301.6 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0035-05

Quantum Algorithm for Prime Factorization with High Probability

FU Xiang-qun, BAO Wan-su, ZHOU Chun, ZHONG Pu-cha
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: In this paper, based on the quantum Fourier transform, we give a new quantum algorithm for prime factorization. The algorithm turns r to be phase factor under repeated application of Fourier transform and variate transform, where r is the order of a selective element in the ring of integers modulo N. Furthermore the amplitude of the non-target states except zero state is modified to be 0. Our algorithm's success probability, which is more than 3/4 and higher than Shor's algorithm, doesn't depend on the size of r other than Shor's algorithm. Meanwhile, we present a comparison of the required resource between the new algorithm and Shor's algorithm.

Key words: quantum algorithm; prime factorization; public key crypto; quantum Fourier transform

1 引言

众所周知,量子计算机具有强大的并行计算能力,以 n 比特输入为例,量子计算机可以通过一步运算完成对 2^n 个输入的计算,

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,0^n\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,f(x)\rangle$$

但是在输出运算结果时,每个结果都是等概率地输出.量子计算算法的作用就是使得想要的结果能以很高的概率输出.因此按照量子计算机的基本原理,针对需要解决的实际问题,设计符合量子计算机运算机理的量子计算算法是量子计算机解决问题的关键.

在 20 世纪 90 年代,出现了两个著名的量子计算算法:1994 年,P W Shor[1] 提出了一个在多项式时间内求解整数分解问题和有限域上离散对数问题的量子计算算法,它在密码学上的重要意义是:利用该算法可以有效破译,即在多项式时间内成功破译 RSA 公钥密码体制、ECC 公钥密码体制和 Diffie-Hellman 密钥分配协议;1996 年,L K Grover[2] 提出了一个针对未加整理的数据库的量子搜索算法,它在密码学上的重要意义是:利用该算法对密码进行密钥穷尽攻击,计算复杂度可以得到开平方根的降低.上述两个量子算法的相继提出对现代密码的安全性带来了巨大冲击,特别是对公钥密码的安全性产生了巨大影响.因为目前实用的公钥密码体制的安全性基础大多是基于大整数分解问题或离散对数求解问题的难解性,而且一些数字签名、秘密共享[3,4] 的安全性也是基于这些问题的难解性.目前,解决大整数分解问题的最优算法是数域筛法[5],但其计算复杂性是亚指数时间,即

$$O(e^{(1.923+o(1))(\ln N)^{1/3}(\ln\ln N)^{2/3}}),$$

尽管后来一些学者对整数分解问题进行了研究[6],但算法并不具有普适性.

量子计算下可以有效地求解两个素数乘积的整数分解问题的核心是 Shor 整数求阶量子算法的提出,该算法是一个概率算法,算法运行一次成功的概率是 $4\varphi(r)/\pi^2 r$(φ 是欧拉函数,r 是 Z_N 中所选元素的阶).

收稿日期:2009-05-04;修回日期:2009-12-22

长期以来,如何进一步提高整数求阶量子算法的成功概率一直是整数分解问题量子算法研究的难点. D McAnally[7]在 2002 年提出一种新的整数求阶算法,该算法执行两次 Shor 整数求阶量子算法得到 Z_N 中所选元素阶的概率大于 60%,执行四次 Shor 整数求阶量子算法,得到所选元素阶的概率大于 90%,但是该算法本质上仍依赖于 Shor 整数求阶量子算法的成功率.本文给出了一个新的整数分解量子算法,利用量子 Fourier 变换能够将一些输入状态之间的关系变成相位因子这一性质,通过利用多次量子 Fourier 变换和变量代换,使得$|0\rangle$态之外的非目标态(对整数分解不起作用的量子态)的几率幅变为零,算法成功的概率高于 Shor 整数分解量子算法,且不再依赖于 Z_N 中所选元素阶 r 的大小,同时还将新算法的性能与 Shor 算法进行了对比.

2 预备知识

为讨论方便,我们约定整数环 $Z_N=\{0,1,\cdots,N-1\}$, Z_N^* 为整数环 Z_N 中除去零元素的集合,$\omega_n=e^{2\pi i/n}$是 n 次单位根.

求两个整数的最大公因子算法是公元前三世纪由 Euclidean 发现的,Euclidean 算法[8]主要是利用带余除法的相关性质求两个数的最大公因子.如果两个整数都可以表示为至多 L 比特的比特串,那么算法的计算复杂性是 $O(L^3)$.

在经典计算机上求解整数的一个因子问题事实上等价于整数求阶问题[9].

定义 1[10](a 模 N 的阶) 在整数环 Z_N 中,对于任意一个 $a\in Z_N^*$,如果 r 是最小的非零整数使得 $a^r=1 \bmod N$ 成立,那么 r 称为 a 模 N 的阶.

定义 2[10] 对于一个整数 N,x 是一个整数满足 $0<x\leqslant N$ 和 $x\mid N$,如果 x 是 1 或 N,那么 x 称为 N 的一个平凡因子,否则称为非平凡因子.

引理 1[9] 对于一个整数 $N=p_1^{t_1}\cdots p_m^{t_m}$,如果 Z_N^* 中的一个元素 x 模 N 的阶 r 是偶数且 $x^{r/2}\neq -1 \bmod N$,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[9] 设 $N=p_1^{t_1}\cdots p_m^{t_m}$ 是正奇合数的素因子分解,从 Z_N^* 中随机选取整数 x,x 模 N 的阶为 r,则

$$p(r \text{ 为偶数且 } x^{r/2}\neq -1 \bmod N)\geqslant 1-\frac{1}{2^m}$$

由引理 1 和引理 2 容易得到推论 1 成立.

推论 1 对于一个整数 $N=pq$,从 Z_N^* 中随机选取一个与 N 互素的整数 x,x 模 N 的阶为 r,那么利用整数 x 可以对 N 进行整数分解的概率为 $p\geqslant 3/4$.

定义 3(量子 Fourier 变换)[9] 如果在一组标准正交基$|0\rangle,|1\rangle,\cdots,|N-1\rangle$上的一个线性算子在基态上的作用 U_F 为

$$U_F:|j\rangle\mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{jk}\ |k\rangle$$

那么对任意的状态的作用可以表示为

$$U_F:\sum_{j=0}^{N-1}x_j|j\rangle\ \mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}x_j\omega_N^{jk}\ |k\rangle$$

称 U_F 为量子 Fourier 变换.其中,"$\mapsto$"表示为该变换是可逆变换.

3 Shor 整数分解量子算法

1994 年,Shor 在其原始论文[1]中首次提出了整数求阶量子算法,并注意到整数因子分解问题可归约为整数求阶问题,其整数求阶量子算法[1]具体步骤如下:

Step1 给定一个整数 N,$L=\lceil\log N\rceil$,选择两个整数 m、α,其中 N 是两个素数的乘积,$N^2\leqslant 2^m\leqslant 2N^2$,$1<\alpha<N-1$;

Step2 给定两个 m 维量子寄存器,其初态均为$|0^m\rangle$,对第一个寄存器做在标准正交基$|0\rangle,|1\rangle,\cdots,|2^m-1\rangle$上的量子 Fourier 变换 U_F,产生一个状态叠合

$$|0^m,0^m\rangle\mapsto\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,0^m\rangle;$$

Step3 做量子黑盒变换,完成 $\alpha^x \bmod N$ 的并行计算问题

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,0^m\rangle\mapsto\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,\alpha^x \bmod N\rangle;$$

Step4 对第一寄存器再做在标准正交基$|0\rangle,|1\rangle,\cdots,|2^m-1\rangle$上的量子 Fourier 变换

$$\begin{aligned}&\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,\alpha^x \bmod N\rangle\\ &\mapsto\frac{1}{2^m}\sum_{x=0}^{2^m-1}\sum_{c=0}^{2^m-1}\omega_{2^m}^{xc}|c,\alpha^x \bmod N\rangle\\ &\overset{x=kr+t}{=}\frac{1}{2^m}\sum_{c=0}^{2^m-1}\sum_{t=0}^{r-1}\sum_{k=0}^{\lfloor(2^m-t-1)/r\rfloor}\omega_{2^m}^{(kr+t)c}|c,\alpha^t \bmod N\rangle\end{aligned}$$

其中,t 称为偏移量;

Step5 观察得到具体状态$|c,x^t\rangle$,得到 c,利用连分数方法计算出 r.然后判断 r 是否为 α 的周期.如果是,则算法结束.否则,返回 Step1,直到找到正确的 r 为止.

Shor 通过证明算法运行一次成功的概率为 $4\varphi(r)/\pi^2 r$,因此 Shor 整数求阶量子算法的成功率依赖于 Z_N 中所选元素 α 模 N 的阶的大小.

基于 Shor 整数求阶量子算法,可以对整数 $N=pq$ 进行分解,具体如下:

选择一个整数 $\alpha\in Z_N$,利用 Shor 整数求阶量子算

法求出 α 模 N 的阶 r.如果 r 是奇数,算法需重新选择 α;如果 r 是偶数,计算 $(\alpha^{r/2}+1) \bmod N$,记为 d,当 $d \neq -1$ 时,计算并输出 $\gcd(\alpha^{r/2}+1, N)$,则 $\gcd(\alpha^{r/2}+1, N)$ 是 N 的一个因子,否则需重新选择 α 并计算 α 模 N 的阶.

4　新的整数分解量子算法

量子计算机之所以能快速计算出整数的阶,是因为在 Shor 整数求阶量子算法中运用了量子 Fourier 变换,通过量子 Fourier 变换可将偏移量 t 变成一个相位因子,使得输入量子态的几率幅发生改变,即目标态被观察到的概率变大,而非目标态被观察到的概率变小.以下我们正是基于这一思想,给出一个新的整数分解量子算法,通过多次运行量子 Fourier 变换使得输入态之间存在的关系转化为相位因子.

由于对任意 $\alpha \in Z_N^*$,如果 $\gcd(\alpha, N) \neq 1$,则由 Euclidean 算法可求出 N 的一个因子为 $\gcd(\alpha, N)$,因此,以下我们不妨只讨论 $\gcd(\alpha, N) = 1$ 时整数 $N = pq$ 的分解情况.

新整数分解量子算法:

Step1　$N = pq$,任意给定一个数 $\alpha \in Z_N^*$ 和三个 $L = \lceil \log N \rceil$ 维量子寄存器,其中 α 与 N 互素,量子寄存器的初态都为 $|0^L\rangle$.

Step2　对前两个寄存器分别做在标准正交基 $|0\rangle, |1\rangle, \cdots, |N-1\rangle$ 上的量子 Fourier 变换,产生叠加态:

$$|0^L\rangle|0^L\rangle|0^L\rangle \mapsto \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}|x\rangle|y\rangle|0^L\rangle$$

Step3　完成函数 $f(x, y) = \alpha^x$ 的并行计算并将其加到第三个寄存器中:

$$\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}|x\rangle|y\rangle|0^L\rangle \mapsto \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}|x\rangle|y\rangle|\alpha^x\rangle$$

再对第三个寄存器进行观测可以得到一个元素 α^t,其中 $0 \leqslant t \leqslant N-1$,记 α 的阶为 r,由于 $\alpha^x = \alpha^{x+ry} = \alpha^t \bmod N$,故前两个寄存器的叠加态为 $\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|t - ry\rangle|y\rangle|\alpha^t\rangle$.

Step4　对前两个寄存器分别做在标准正交基 $|0\rangle, |1\rangle, \cdots, |N-1\rangle$ 上的量子 Fourier 变换,可以得到

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|t - ry\rangle|y\rangle|\alpha^t\rangle \mapsto \frac{1}{N\sqrt{N}}\sum_{y=0}^{N-1}\sum_{t'=0}^{N-1}\sum_{y'=0}^{N-1}\omega_N^{(t-ry)t'}\omega_N^{yy'}|t'\rangle|y'\rangle|\alpha^t\rangle$$

Step5　对前两个寄存器进行观测,得到 t', y'.

Step6　如果 $t' = 0$,返回 Step1,重新选择 α;如果 $t' \neq 0$,则执行下一步.

Step7　计算 $d = \gcd(t', N)$;

如果 $d \neq 1$,输出 d,算法结束;

如果 $d = 1$,那么计算 $r = (t')^{-1}y' \bmod N$,当 r 是偶数且 $\alpha^{r/2} \neq -1 \bmod N$ 时,输出 $\gcd(\alpha^{r/2}+1, N)$,算法结束;否则,返回 Step1,重新选择 α.

以下分析算法的正确性,并计算算法成功的概率.

首先,分析经过第四步的变换之后,量子叠加态之间存在的内在关系.

由于

$$\sum_{y=0}^{N-1}\omega_N^{tt'}\omega_N^{y(y'-rt')} = \begin{cases} N\omega_N^{tt'}, & y' = rt' \bmod N \\ 0, & y' \neq rt' \bmod N \end{cases}$$

因此

$$\frac{1}{N\sqrt{N}}\sum_{y=0}^{N-1}\sum_{t'=0}^{N-1}\sum_{y'=0}^{N-1}\omega_N^{(t-ry)t'}\omega_N^{yy'}|t'\rangle|y'\rangle|\alpha^t\rangle = \frac{1}{\sqrt{N}}\sum_{t'=0}^{N-1}\sum_{y' = rt' \bmod N}\omega_N^{tt'}|t'\rangle|y'\rangle|\alpha^t\rangle.$$

从而,前两个寄存器中不满足 $y' = rt' \bmod N$ 的量子态 $|t'\rangle|y'\rangle$ 的几率幅变成 0,经过第四步之后,前两个寄存器保留下的量子态 $|t'\rangle|y'\rangle$ 均满足 $y' = rt' \bmod N$.

其次,讨论第(7)步是如何对整数进行分解的:

①如果 $d \neq 1$,那么 $d \mid N$,又由于 N 是两个素数的乘积且 $t' \leqslant N$,因此可以对 N 进行整数分解;

②如果 $d = 1$,那么 t' 存在一个逆元 $u \in Z_N^*$ 使得 $ut' = 1 \bmod N$,由于 $y' = rt' \bmod N$,故 $uy' = urt' \bmod N$ 即 $r = uy' \bmod N$.此时,当 r 是偶数且 $\alpha^{r/2} \neq -1 \bmod N$ 时,由引理 1 可知,整数 N 可以成功被分解;否则需要重新选择 α 并求其模 N 的阶.

最后,由算法执行过程不难推出,保留下的量子态每个被观察到的的概率是

$$p_{t', y'} = \frac{1}{N}|\omega_N^{tt'}|^2 = \frac{1}{N},$$

因此,所保留下的量子态的概率之和仍为 1.

5　新算法与 Shor 算法的性能对比分析

新算法的核心是量子 Fourier 变换的多次运用.文献[9]指出量子 Fourier 变换是一个酉变换,满足量子算法所要求的可逆条件,在第三步内所使用的并行计算同样也是一个可逆计算.就算法的本身所使用的变换而言,该算法是正确的,在量子计算机可以得到有效的实现.下面分别从算法成功率与资源消耗情况两个方面,将新算法与 Shor 算法进行对比.

算法成功率对比:

在 Shor 整数分解量子算法中,由推论 1 可知,得到 r 之后能成功分解整数 N 的概率大于 3/4,再根据第 3 节的求解过程可知,运行 Shor 整数求阶量子算法一次能够对整数 $N = pq$ 进行分解的成功概率 p 满足

$$3\varphi(r)/\pi^2 r < p < 4\varphi(r)/\pi^2 r,$$

同样 Shor 算法的成功率也依赖于 r 的大小.

在新算法中,由第 4 节对算法的分析过程可得定理 1.

定理 1 新的整数分解量子算法运行一次成功的概率满足

$$\frac{4N-\varphi(N)-4}{4N}\leqslant p<\frac{N-1}{N}.$$

证明:由算法执行步骤可知,算法在两种情况下可对整数 N 进行分解. 当 $\gcd(t',N)\neq 1$ 时,通过求 $\gcd(t',N)$对 N 进行分解;当 $\gcd(t',N)=1$ 时,通过求出 Z_N 中元素 α 的阶对 N 进行分解.

由于在集合$\{0,1,\cdots,N-1\}$中与 N 互素的元素的个数是 $\varphi(N)$,因此新的整数分解量子算法的第 6 步中观察到 $|t'\rangle$不为$|0\rangle$且 $\gcd(t',N)\neq 1$ 的概率为 $\frac{N-\varphi(N)-1}{N}$,此时,能对 N 进行整数分解的概率 $p_1=\frac{N-\varphi(N)-1}{N}$;

观察到$|t'\rangle$满足 $\gcd(t',N)=1$ 的概率为 $\varphi(N)/N$,易知 t'在模 N 下存在一个逆元,亦即可以求出随机数 α 的阶 r,由引理 2,此时能对 N 进行整数分解的概率 p_2 满足

$$\frac{3\varphi(N)}{4N}\leqslant p_2<\frac{\varphi(N)}{N}.$$

综上所述,运行新算法一次能够对两个素数乘积的整数进行整数分解的概率 p 满足

$$\frac{4N-\varphi(N)-4}{4N}\leqslant p=p_1+p_2<\frac{N-1}{N}.$$

证毕.

因为 $N=pq$,所以 $\frac{4N-\varphi(N)-4}{4N}=\frac{4pq-(p-1)(q-1)-4}{4pq}>\frac{3}{4}$,因此,新算法运行一次具有较高的成功概率. 同时,由于 $\varphi(r)<r$,$\frac{4\varphi(r)}{\pi^2 r}<\frac{4}{\pi^2}<\frac{3}{4}$,所以 Shor 算法运行一次成功的概率小于$\frac{3}{4}$,因而有定理 2.

定理 2 如果整数 $N=pq$,p,q 是两个素数,那么利用新算法对 N 进行整数分解的成功概率高于 Shor 整数分解量子算法.

新的整数分解量子算法的成功概率之所以大于 Shor整数分解量子算法,关键在于利用了多次量子 Fourier 变换和变量代换,使$|0\rangle$态之外的非目标态的几率幅变成 0,那么再进行观测时,就能以很大的概率得到对整数分解有用的量子态,而且成功率不再依赖于 Z_N 中所选元素的阶 r 的大小.

算法资源消耗情况对比:

在新的整数分解量子算法中,前五步是在量子计算机上执行的,后两步是在经典计算机上执行的. 由于后两步均可在经典计算机上以多项式时间得到实现,在资源消耗上可以忽略,因此新算法的资源消耗主要在前五步上. 前五步中使用的基本部件主要有模幂运算和量子 Fourier 变换,它们所需的量子逻辑门数文献[9]、[11]、[12]做了比较详细的分析,基于这些研究结果,我们可以给出新算法的资源消耗分析.

新的整数分解量子算法初始化$|0\rangle$态是 L 量子比特的,执行 1 个 Hadmard 变换需要 $O(L)$规模的量子逻辑门[9],实现 1 个量子 Fourier 变换需要 $O(L^2)$规模的量子逻辑门,因此,新算法中 4 个量子 Fourier 变换仍然需要 $O(L^2)$规模的量子逻辑门. 对于模幂运算,由于加法运算和进位运算需要 $3L$ 个量子逻辑门,每个模乘运算需要 L 个长为 L 的加法运算,利用二进制表示法计算模幂运算需要 $2L$ 步模乘运算,所以模幂运算所需要的量子逻辑门数的规模为 $O(L^3)$[11],新算法中只需要 1 次模幂运算,亦即只需要 $O(L^3)$规模的量子逻辑门,因此实现整个新算法的量子线路所需要量子逻辑门的规模为 $O(L^3)$.

Shor 整数分解量子算法初始化$|0\rangle$态是 m 量子比特的,算法中需要 2 次量子 Fourier 变换和 1 次模幂运算,实现 2 次量子 Fourier 变换需要 $O(m^2)$规模的量子逻辑门,实现 1 次模幂运算所需要的量子逻辑门数规模为 $O(m^3)$,因此,实现 Shor 整数分解量子算法的量子线路所需量子逻辑门规模也是 $O(m^3)$[9]. 由于 $L=\lceil\log N\rceil$、$N^2\leqslant 2^m\leqslant 2N^2$,即 $2L\leqslant m\leqslant 2L+1$,因此,在算法实现上新的整数分解量子算法所需的量子逻辑门数与 Shor 整数分解量子算法是同等规模的.

6 结束语

本文提出了一个新整数分解量子算法,该算法利用多次量子 Fourier 变换和变量代换使得除$|0\rangle$态之外的非目标态的几率幅变成零,从而提高算法的成功概率. 与 Shor 整数分解量子算法相比,算法具有更高的成功概率,而且不再依赖于 Z_N 中所选元素阶 r 的大小;算法的计算复杂性仍是多项式时间的;算法运行所需的量子逻辑门数的规模为 $O(L^3)$. 与经典计算一样,量子整数分解算法中模幂运算也是最耗时的,因此如何优化算法,提高量子模幂运算的运行效率有待进一步研究.

参考文献:

[1] P W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484 – 1509. (preliminary version in FOCS 1994)

[2] L K Grover. A fast quantum mechanics algorithm for database search[A]. Proceedings of 28th ACM Symposium on Theory of Computation[C]. New York: ACM Press, 1996. 212 – 219.

[3] 张健红,伍前红,邹建成,王育民.一种高效的群签名[J].电子学报,2005,33(6):1113 – 1115.
Zhang Jian-hong, Wu Qian-hong, Zou Jian-cheng, Wang Yu-min. An efficient group signature scheme[J]. Acta Electronica Sinica, 2005, 33(6): 1113 – 1115. (in Chinese)

[4] 许春香,肖国镇.门限多重秘密共享方案[J].电子学报,2004,32(10):1688 – 1689.
Xu Chun-Xiang, Xiao Guo-zhen. A threshold multiple secret sharing scheme[J]. Acta Electronica Sinica, 2004, 32(10): 1688 – 1689. (in Chinese)

[5] J P Buhler, H W Lenstra, C Pomerance. The development of the number field sieve[J]. Lecture Notes in Mathematics (Springer), 1993, 1554: 50 – 94.

[6] 董庆宽,傅晓彤.对大整数 n = pq 分解的一个有效的搜索算法[J].电子学报,2001,29(10):1436 – 1438.
Dong Qing-kuan, Fu Xiao-tong. An effective searching algorithm for factoring large integer n = pq[J]. Acta Electronica Sinica, 2001, 29(10): 1436 – 1438. (in Chinese)

[7] D McAnally. A Refinement of Shor's Algorithm[DB]. Arxiv: quant-ph/0112055 v4, 2002.

[8] 潘承洞,潘承彪.初等数论(第二版)[M].北京:北京大学出版社,2003. 16 – 21.
Pan Cheng-dong, Pan Cheng-biao. Elementary Number Theory (the second edition)[M]. Beijing: Beijing University Press. 2003. 16 – 21.

[9] M A Nielsen, I L Chuang. Quantum Computation and Quantum Information[M]. Cambridge: Cambridge University, 2000. 198 – 223.

[10] A J Menezes, P C V Oorschot, S A Vanstone. Handbook of Applied Cryptography[M]. Canda: CRC Press LLC, 1997. 283 – 312.

[11] C Zalka. Fast versions of Shor's quantum factoring algorithm [DB]. Quant-ph/9806084v1, 1998.

[12] C Zalka. Shor's algorithm with fewer (pure) qubits[DB]. Quant-ph/0601097v1, 2006.

作者简介:

付向群　男,1985 年生于江西进贤,解放军信息工程大学电子技术学院,博士生,研究方向为量子密码.

E-mail: fuxiangqun@126.com

鲍皖苏　男,1966 年生于安徽天长,解放军信息工程大学电子技术学院,教授,博士生导师,主要研究方向为序列密码、公钥密码、量子密码.　E-mail: 2004bws@sina.com