文章编号：1000-5013(2015)06-0640-05 **doi**：10.11830/ISSN.1000-5013.2015.06.0640

对 Shor 算法破解 RSA 的探讨

涂玲英[1,2]，胡一凡[1,2]，张洪涛[1,2]，代永涛[1,2]，熊红梅[1,2]

（1. 湖北工业大学 纳米电子技术与微系统实验室，湖北 武汉 430068；
2. 湖北工业大学 电气与电子工程学院，湖北 武汉 430068）

摘要： 针对 Shor 算法具有随机性，会导致破解 RSA 公钥密码体制成功率不高的问题，对 Shor 算法原理、RSA 公钥密码体制特点和大量计算结果进行分析，提出量子函数式 $f(x)=a^x \bmod n$ 对 a 值的随机选取是有规律的. 结合数论知识和蒙特卡洛法证明，结果表明：随机数 a 取完全平方数，所求周期 r 很可能不满足 Shor 算法要求；a 取非完全平方数可以提高 Shor 算法破解 RSA 的成功率.

关键词： Shor 算法；非完全平方数；RSA 算法；公钥密码体制；蒙特卡洛法

中图分类号： TP 301.6 **文献标志码**： A

迄今为止，RSA 算法被认为是世界上最成熟完善的公钥密码体制. 它能够抵抗已知的绝大多数密码攻击，已被 ISO 推荐为公钥数据加密标准. 目前，世界上还没有任何可靠的方法破解 RSA. 随着 Shor 算法的提出和量子计算机的不断发展，RSA 的安全性也受到威胁. Shor 算法利用量子计算的并行性，可以快速分解出大数的质因子，它的提出在理论上破解了目前被公认为最安全的 RSA 公钥密码. Shor 算法的基本原理是运用量子傅里叶变换，将大整数因子分解转化为求某一个函数的周期[1]. 但是在求函数周期过程中，现有的 Shor 算法随机性大，效率不高[2]. 鉴于此，本文通过对 Shor 算法和 RSA 算法原理的分析，并结合前人的研究成果，提出了一种可以提高 Shor 算法破解 RSA 成功率的方法.

1 RSA 公钥密码

RSA 使用公开的公钥进行加密通信，密文只能被拥有与之匹配的私钥的人解开. RSA 算法的理论基础[3]是可逆模指数运算，它的安全性基于数论中大整数分解的复杂性. 数论中，大整数分解的问题可概述为：已知整数 $n=p \cdot q$，其中，p 和 q 是 2 个素数，求出 p 和 q 的值.

在 RSA 公钥密码体制中，用户拥有 2 个密钥：公钥 PK$=\{e,n\}$和私钥 SK$=\{d,n\}$. 公钥用于加密，私钥用于解密. 用户可将公钥 PK 公开，而私钥中的 d 必须严格保密. RSA 公钥密码中相关参数的计算如下. 1) 选取 2 个保密的素数 p 和 q（p 和 q 为 100 位以上的十进制数）. 2) 计算 $n=p \cdot q$ 的值. 其中，n 是 RSA 算法的模数. 3) 计算 $\phi(n)=(p-1)(q-1)$的值，$\phi(n)$是 n 的欧拉函数值. 4) 随机选取 1 个整数 e，使其满足 $1<e<\phi(n)$，且 $\gcd(\phi(n),e)=1$. 5 计算私钥 SK 中的 d 值，满足 $d \times e \equiv 1 \bmod \phi(n)$，$d$ 是 e 在模 $\phi(n)$下的乘法逆元. 因为 $\gcd(\phi(n),e)=1$，由模运算可知，它的乘法逆元一定存在. 6) 将 PK$=\{e,n\}$作为公钥公布，SK$=\{d,n\}$作为私钥保留. 此时，p，q 不再需要，可以销毁.

设 m 为需要加密的明文，c 为加密后的密文. 加密时，先将明文比特串进行分组，让每个明文分组的十进制数 m_i 小于 n，记 c_i 为对应的 m_i 加密后的密文，则加密算法为

$$c_i = m_i^e \bmod n. \tag{1}$$

式(1)中：$0 \leqslant m_i < n$，$0 \leqslant c_i < n$.

收稿日期： 2015-05-24

通信作者： 涂玲英(1963-)，女，副教授，主要从事量子通信与量子计算、视频监控系统的研究. E-mail：947392311@qq.com.

基金项目： 湖北省武汉市科技局“十城千辆新动力汽车计划”项目(2013011801010600)

解密时，先对密文 c 进行比特串分组，则解密算法为

$$m_i = c_i^d \bmod n. \tag{2}$$

因此，RSA 公钥密码体制中，最关键的是公钥 PK 中的 e 值和私钥 SK 中的 d 值.

2　Shor 算法

2.1　原理描述

Shor 算法的原理是依据数论中的相关定理，将大数因子分解转化为求 1 个函数的周期. 主要过程[4]有如下 3 个步骤. 1) 已知整数 n 的值，随机选取正整数 a，$a\in Z_n^*$，$Z_n^*=\{a\in Z\mid a<n,\ \gcd(a,n)=1\}$. 2) 定义函数 $f(x)=a^x \bmod n$，能发现 $f(x)$ 是 1 个周期函数，记周期为 r，则

$$a^x \bmod n = a^{x+r} \bmod n. \tag{3}$$

故

$$a^r = 1 \bmod n. \tag{4}$$

3) 求 A 和 B，表达式为

$$(a^{r/2})^2 - 1 = 0 \bmod n, \tag{5}$$

$$(a^{r/2}+1)(a^{r/2}-1) = 0 \bmod n. \tag{6}$$

令

$$A = \gcd(a^{r/2}+1, n), \quad B = \gcd(a^{r/2}-1, n), \tag{7}$$

得出

$$n = A \times B. \tag{8}$$

式(7)中：为保证 A，B 为整数，周期 r 应为非零偶数[5-6].

2.2　周期 r 的求取

由 A 和 B 的表达式可知：只要求出函数 $f(x)$ 的周期 r，大整数 n 的因子分解问题就得到了解决. Shor 算法中，周期 r 的信息是通过量子傅里叶变换获得的[7-8].

首先，对 2 个量子寄存器 $R1$ 和 $R2$ 进行初始化，再对 $R1$ 依次作 H 变换和幺正变换，得到的结果分别存放到 $R1$ 和 $R2$ 中. $R1$ 和 $R2$ 中的状态为纠缠态，即

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

$$U_f:\mid \Psi_1\rangle \rightarrow \mid \Psi_2\rangle = \frac{1}{q}\sum_{x=0}^{q-1} \mid x\rangle \mid f(x)\rangle = \frac{1}{q}\sum_{x=0}^{q-1} \mid x\rangle \mid a^x \bmod N\rangle. \tag{10}$$

然后，对 $|R2\rangle$ 进行测量. 假设 $f(x)$ 的周期为 r. 当 $|R2\rangle$ 坍缩时，$|R1\rangle$ 也对应地坍缩为

$$\mid R1\rangle = \frac{1}{\sqrt{A+1}}\sum_{j=0}^{A} \mid 1+jr\rangle. \tag{11}$$

式(11)中：A 为小于 $(q-1)/r$ 的最大整数.

最后，对 $|R1\rangle$ 作量子傅里叶变换，并对其进行测量，求出函数 $f(x)$ 的周期 r，表达式为

$$\widetilde{f}(c) = \frac{\sqrt{r}}{q}\sum_{j=0}^{q/(r-1)} \exp(2\pi(1+jr)c/q) - (\frac{\sqrt{r}}{q}\exp(2\pi jrc/q))c. \tag{12}$$

量子傅里叶变换会使需要的结果增强，并使不需要的结果为 0，这种现象称为量子干涉[9]. 所以，当 $c=kq/r$，则

$$\mid R1\rangle_{\mathrm{QFT}} = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp(2\pi/k) \mid kq/r\rangle. \tag{13}$$

$|R1\rangle$ 经量子傅里叶变换后，周期从 r 变为 q/r. 由于 $c=kq/r$，c 和 q 是已知的，如果 k 与 r 互质，就能求出 r[10]. 最大的非零偶数 r，就是需要求的 $f(x)$ 的周期.

3　Shor 算法在破解 RSA 中的应用

RSA 的安全性取决于大整数 n 的分解，Shor 算法的功能是分解大整数 n，所以 Shor 算法在理论上破解了 RSA 公钥密码[11-12]. 破解过程具体如下 6 个步骤.

步骤 1　通过量子傅里叶变换，求出函数 $f(x)$ 的周期 r，并保证 r 为非零偶数.

步骤 2 将 r 带入式子(7),(8)中,结合待分解的大整数 n,求出 A 和 B 的值.

步骤 3 RSA 中已销毁的 p,q 值分别是 A,B.

步骤 4 将 p,q 带入式子 $\phi(n)=(p-1)(q-1)$中,求出 $\phi(n)$.

步骤 5 将 $\phi(n)$和已知的 e 值带入式子 $d\times e\equiv 1 \bmod \phi(n)$中,求出 d 值.

步骤 6 将 d,n 的值带入式(2)中,完成了对 RSA 的破解.

4 对 Shor 算法破解 RSA 的优化

4.1 优化思路

Shor 算法虽然在理论上破解了 RSA,但还是存在一些微小的不足的地方. 应用 Shor 算法破解 RSA,并不是大数 n 满足了条件就一定能成功破解,只是能使破解的成功率尽量接近 1.

Shor 算法能否成功破解 RSA 的关键在于函数 $f(x)$的周期 r,而 r 在很大程度上取决于随机选择的数 a. Shor 算法中,$a\in Z_n^*$,如果对 a 再做一个限定,求得的周期 r 为偶数的概率可能会变大很多. 提出一个提高 Shor 算法破解 RSA 成功率的优化思路:对 a 做个限定,$a\in Z_n^*$,且 a 不能是完全平方数.

例 1 函数 $f(x)=a^x \bmod 33$,选取 $a=4$,求周期 r.

$f(0)=1,\quad f(1)=4,\quad f(2)=16,\quad f(3)=31,\quad f(4)=25,$

$f(5)=1,\quad f(6)=4,\quad f(7)=16,\quad f(8)=31,\quad f(9)=25,\quad \cdots$

此时周期 $r=5$,不是偶数.

为了方便计算 a 取完全平方数时周期 r 的值,用 C 语言编写了一段程序,程序的源代码为

```
#include <stdio.h>
#include <math.h>
int gcd(int x,int y);
void main()  {int a,c,x,n;
printf("Please enter two int numbers:a=?,n=? \n");
scanf("%d,%d",&a,&n);  if(gcd(a,n)! =1 || a>n)
printf("Please enter two correct int numbers b,n\n");
    else { x=1; c=1%n;
    while((int)(pow((double)a,(double)x))%n! =c)
    x++;  printf("函数 f(x)的周期 r 是:%d\n",x);
    }
}
    int gcd(int x,int y) {
    int z;  if(x<y)
    { z=x; x=y; y=z;}
if(x%y = = 0)  return y;
else  return gcd(y, x%y); }
```

在 Visual C^{++} 中运行程序验证例 1 的结果,验算结果如图 1 所示. 由图 1 可知:当 $a=4$ 时,周期 r 为 5,例 1 的结果得到了验证. 此程序方便求取 r,为大量计算 a 取不同的完全平方数时对应的周期 r 提供了便利.

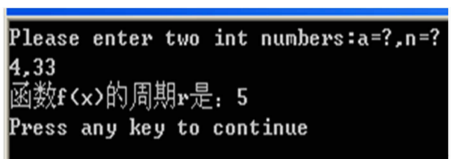

图 1 例 1 的验算结果

Fig. 1 Verification results of example 1

4.2 优化思路的证明

由例 1 可知:a 取完全平方数算得的周期都不是偶数. 通过计算发现,这是 Shor 算法周期求解中的大概率事件. 如果对随机选取的 a 增加限制,不选取完全平方数,破解 RSA 的成功率会相应地提高[5].

证明 已知 $n=pq$,p 和 q 均为素数,$a\in Z_n^*$,其中 $Z_n^*=\{a\in Z\mid a<n,\ \gcd(a,n)=1\}$.

令 $p=2^x+1$，$q=2^y+1$，且 $x\neq y$，则成功破解 RSA 的概率表示为

$$2^{-(x+y)}\left(1+\sum_{j=0}^{\min(x,y)-1}4^j\right)\leqslant\frac{1}{2}.$$

类似地，假设存在数 $f\in Z_p^*$，$g=f^s$，其中，s 是奇数. 则 g 的阶满足 $\mathrm{ord}_p(g)s=0 \bmod(p-1)$，即 $\mathrm{ord}_p(g)s=k(p-1)$，$g$ 模 p 的阶一定为偶.

如果 a 在 Z_p^* 或 Z_q^* 中有偶数阶，则 a 在 Z_n^* 中有偶数阶. 推出至少有一半的 $a\in Z_n^*$ 满足以下 2 个条件：1) $\exists k$ 满足 $\mathrm{ord}_n(a)=2k$；2) $a^k\neq-1 \bmod n$.

令 $d=g^u$，v 为 d 的阶，这就等同于 $uv=0 \bmod(p-1)$，v 最小.

已推出属于 Z_n^* 的 a 的阶是偶数，计算 $a\in Z_n^*$ 不满足条件 2)但满足 $(a/n)=-1$ 的元素，等同计算 $a^k=-\bmod p$ 和 $a^k=-1 \bmod q$. 这表示 u 和 v 都不能划分 k. $(a/n)=-1$ 表示 $(a/p)=-1$ 且 $(a/q)=1$，或者 $(a/p)=1$ 且 $(a/q)=-1$.

设 $m\in Z_p^*$，$a=m^t$（t 为奇数），需计算所有满足条件的偶数 t_1. $a=m^{t_1}$ 的阶是 2^is，s 为奇数. 此时，所有 1 到 $p-1$ 之间的奇数都能求出 t_1.

讨论和 q 有关的元素. 已设 $q=2^y+1$，令 $r\in Z_q^*$，$a=r^{t_2}$，计算所有满足条件的偶数 t_2. 当 $x=y$ 时，t_2 没有偶数解；当 $x>y$ 时，r^{t_2} 的阶会划分 r^{t_2}，没有这样的值. 所以，只剩下 $x>y$.

当 $x\neq y$ 时，只需考虑 $x<y$ 的情况，满足条件 1)，2)的所有值满足

$$A(n)=\frac{p-1}{2}2^{(x-1)}=\frac{p-1}{2}\frac{2^y}{2^{(y-x+1)}}\frac{1}{4}(p-1)(q-1)\frac{1}{2^{(y-x)}}=\frac{1}{4}\varphi(n)\frac{1}{2^{(y-x)}}.$$

所以，成功破解 RSA 的概率是

$$p(n)=1-\frac{A(n)}{\varphi(n)}=1-\frac{1}{2^{(y-x+2)}}\geqslant\frac{3}{4},\qquad x<y.$$

在 $x=y$ 的情况下，此时概率为 1，表示 $(a/n)=-1$ 中的 a 总是满足条件 1)和 2).

从证明过程可看出，对 a 经过一定的限定，应用 Shor 算法破解 RSA 的成功率明显得到提高，说明优化思路是可行有效的. 采用蒙特卡洛法作进一步分析.

列举不同的整数 N 值，算出 a 在 2 个条件下，函数 $f(x)$ 的周期 r 为偶数的概率 P，如表 1 所示. Shor 算法能否高效破解 RSA，对应函数式 $f(x)$ 的周期 r 为偶数的概率 P 是重要指标. 功能函数方程为

$$T_1=g(X_1,X_2,\cdots,X_n)=P_1-P_2. \tag{14}$$

式(14)中：P_1 为 $a\in Z_n^*$ 且 a 为非完全平方数条件下，周期 r 为偶数的概率；P_2 为 $a\in Z_n^*$ 条件下，周期 r 为偶数的概率.

用蒙特卡洛法分析提高 Shor 算法破解 RSA 成功率的原理是：假设对大整数 N 进行 M 次随机抽样，求出每组 P_1，P_2，并将其代入功能函数进行计算，得到 M 个 T 值. 若 $T>0$，则破解的成功率得到提升；若 $T\leqslant0$，则破解的成功率未得到提升.

在考虑各参数变异性时，借助 ANSYS 中的概率功能模块，求出当 $a\in Z_n^*$ 且 a 为非完全平方数时，周期 r 为偶数的概率 P_1 和当 $a\in Z_n^*$ 时，周期 r 为偶数的概率 P_2 的概率分布，从而得到功能函数的可靠度和可靠度指标. 采用蒙特卡洛法中的拉丁超立方法，对表 1 中参数值所对应的模型进行 500 次计算分析，得到 a 在 2 种不同条件下，对应 P_1 和 P_2 的部分分布曲线，如图 2 所示.

表 1　a 在不同条件下函数周期为偶数的概率

Tab. 1　Probability that the cycle of function is even when a is under different conditions

N	P	
	$a\in Z_n^*$ 时	$a\in Z_n^*$ 且 $\sqrt{a}\in Z$ 时
21	0.473	0.812
2 701	0.485	0.855
⋮	⋮	⋮

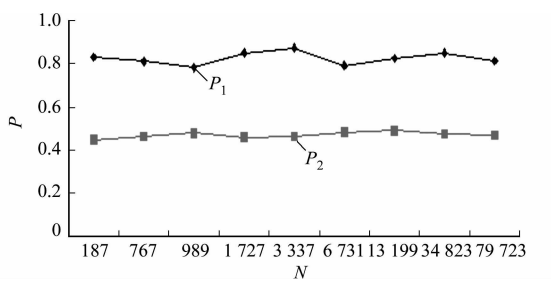

图 2　P_1 和 P_2 的部分曲线分布

Fig. 2　Part of the curve distribution of P_1 and P_2

由图 2 可知：对于任意样本 N 值，P_1 均大于 P_2. 对随机数 a 不做限定时，Shor 算法成功破解 RSA 的概率

P_2 不会超过50%;若限定随机数 a 取非完全平方数,破解的成功率 P_1 不会低于75%,即 $T>0$,说明Shor算法破解RSA的成功率得到提升.

5 结束语

Shor算法尽管已是一种成熟的算法,并在理论上破解了RSA,但由于随机性,它破解RSA的成功率不高.根据RSA和Shor算法的原理,通过大量计算得到的结果显示,$a\in Z_n^*$ 且 a 不取完全平方数时,函数 $f(x)$ 的周期很可能是偶数,那么RSA被破解的成功率会大幅提升.并对这个优化思路进行了证明.受现有技术的制约,文中的优化思路只停留在理论上.

参考文献:

[1] HARDY G H,WRIGHT E M. An introduction to the theory of numbers[M]. 张晓尧,译. 5版. 北京:人民邮电出版社,2009:58-102.

[2] 朱和贵. 探析初等数论基本知识在密码学中的应用[J]. 山东工业技术,2014(21):253.

[3] 李海峰,马海云,徐燕文. 现代密码学原理及应用[M]. 北京:国防工业出版社,2013:110-114.

[4] NAM Y S,BLUMEL R. Sealing laws for Shor's alglorithm with a banded quantum fourier transform[J]. Physica Review A,2013,87(3):032333.

[5] 彭卫丰,孙力. SHOR量子算法的优化及应用研究[J]. 计算机应用与软件,2009,26(5):239-240,246.

[6] NIELSEN M A,CHUANG I L. 量子计算和量子信息(一)[M]. 赵千川,译. 北京:清华大学出版社,2009:199-223.

[7] 王蕴,黄德才,俞攸红. 量子计算及量子算法研究进展[J]. 计算机系统应用,2011,20(6):228-231.

[8] 徐炜,肖智,杨道理. 量子算法在大数据挖掘中的应用前景浅析[C]// 中国信息经济学会学术年会暨博士生论坛论文集. 广东:中国信息经济学会,2013:2-7.

[9] 付向群,鲍皖苏,王帅. ZN上离散对数量子计算算法[J]. 计算机学报,2014,37(5):1058-1062.

[10] GARCIA-MATA I,FRAHM K M,SPEPELYANSKY D L. Effects of imperfections for Shor's factorization algorithm[J]. Physical Review A,2007,75(5):2311.

[11] LUCERO E,BARENDS R,CHEN Y,et al. Computing prime factors with a Josephson phase qubit quantum processor[J]. Nature Physics,2012,8:719-723.

[12] THOMPSON M G,POLITI A,MATTHEWS J C F,et al. Integrated waveguide circuits for optical quantum computing[J]. Circuits, Device and System, IET,2010,5(2):94-102.

Discussion on Cracking RSA With Shor Algorithm

TU Lingying[1,2], HU Yifan[1,2], ZHANG Hongtao[1,2], DAI Yongtao[1,2], XIONG Hongmei[1,2]

(1. Nanoelectronics and Microsystems Technology Laboratory, Hubei University of Technology, Wuhan 430068, China;
2. School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan 430068, China)

Abstract: Since the randomness of Shor algorithm could lead to low success rate in cracking RSA. By analyzing the principle of Shor algorithm, characteristics of RSA public key password system and lots of data, the view that the way for quantum functional in randomly selecting value is regular was putting forward . Verified by number theory and Monte Carlo method, the results showed that if takes a perfect square, the cycle probably can't meet the requirements of Shor algorithm. It comes to a conclusion that take a non-perfect square can improve the success rate of Shor algorithm in cracking RSA.

Keywords: Sahor algorithm; non-perfect squares; RSA algorithm; public key password system; Monte Carlo method

(**责任编辑**: 黄晓楠 **英文审校**: 吴逢铁)