基于近似最大公因多项式问题的公钥密码方案*

于志敏，古春生，景征骏
（江苏技术师范学院 计算机工程学院，江苏 常州 213001）

摘　要：研究了有限域 F_2 上有随机噪声的一组多项式的近似最大公因式问题，提出了基于近似最大公因多项式问题的公钥密码方案。证明了方案的正确性并归约证明了方案的安全性等价于求解近似最大公因式问题，同时讨论了对于该方案可能的攻击方式。通过与现有公钥系统比较，该方案的安全性和可靠性较高，运算速度较快。

关键词：近似最大公因多项式；公钥密码方案；随机噪声；有限域；安全性
中图分类号：TP393.07　　**文献标志码**：A　　**文章编号**：1001-3695(2012)07-2690-03
doi:10.3969/j.issn.1001-3695.2012.07.079

Public key cryptosystem based on approximate greatest common polynomial divisor

YU Zhi-min, GU Chun-sheng, JING Zheng-jun
(*School of Computer Engineering, Jiangsu Teachers University of Technology, Changzhou Jiangsu* 213001, *China*)

Abstract: This paper considered the approximate greatest common polynomial divisor problem for a set of polynomials with random noise over finite field F_2 and presented a new public key cryptosystem based on the approximate greatest common polynomial divisor over finite field. It proved the correctness of this public key scheme, and reduced the security of this public key scheme to solving approximate greatest common polynomial divisor problem. Then discussed some possible attack for this cryptosystem. Compared with the existing public key systems, this cryptosystem has the faster calculating speed, higher security and reliability.

Key words: approximate greatest common polynomial divisor; public key cryptosystem; random noise; finite fields; security

1976 年 Diffie 和 Hellman 提出公钥加密思想以来，研究人员构造了多种公钥方案，目前使用的公钥方案主要是基于数论中问题的计算难度构造的 RSA、ELGamal、椭圆曲线方案等。但是，研究人员已经设计出有效量子算法计算因式分解问题和离散对数问题[1]、椭圆曲线离散对数问题[2]，也就是说当前基于数论中问题的计算难度构造的公钥方案在量子计算机上已经被破解。人们相信基于格问题的计算难度的公钥方案能够抵抗量子计算机的攻击，设计的密码方案主要有：基于多项式环上的 NTRU[3]，基于格问题计算难度的公钥方案[4~6]。但是研究表明目前设计构造的公钥方案所基于的格问题计算难度都不是 NP 难的[7,8]。对于这些非 NP 的格计算问题，如果设计出有效求解算法，那么基于这类问题难度的公钥方案也就不安全了。因此，研究新的计算问题并基于其计算难度构造新的有效公钥方案就显得尤为重要。本文就是在这方面的一个尝试，主要研究有限域上近似最大公因式问题，并基于该问题的计算难度设计了一个新的公钥方案。

众所周知，在有限域 $F_2[x]$ 上一个度为 n 的多项式 $f(x)$ 存在概率多项式时间 $O(n^2)$ 的因式分解算法[9]，对于一组多项式求其最大公因式也存在确定性多项式时间算法，如欧几里得辗转相除法。但是对于有限域 $F_2[x]$ 上存在噪声的一组多项式 $f_i(x)=q_i(x)p(x)+n_i(x)(i=0,1,\cdots,\tau)$ 求解其近似最大公因多项式 $p(x)$ 问题，据笔者所知，目前还未在相关文献中论述。

本文研究了有限域 $F_2[x]$ 上一组多项式的近似最大公因多项式问题，并设计构造了基于该问题计算难度的公钥方案。本文方案中只有有限域 $F_2[x]$ 上模 2 加法运算，计算速度快并且易于实现，其计算时间仅为 $O(n^2)$。

1　基于近似多项式 GCD 的公钥方案

1.1　公钥方案

公钥方案由密钥生成算法 KeyGen(n)、加密算法 Encrypt(pk,m) 和解密算法 Decrypt($sk,c(x)$) 构成，其中 n 为安全参数。

a) 公钥生成算法 KeyGen(n)。在 $F_2[x]$ 上随机选取多项式 $p(x)$、$k(x)$，满足 $p(x)$ 的常数项为 1，$k(x)$ 的常数项为 0，$\deg(p(x))=10n$，$\deg(k(x))=\log n$。随机选取 $q_0(x)$，$q_1(x),\cdots,q_\tau(x),r_0(x),r_1(x),\cdots,r_\tau(x)\in F_2[x]$ 满足 $\deg(q_i(x))=10n$，$\deg(r_i(x))=n$ 且 $\tau=n$。$\deg(f(x))$ 表示多项式 $f(x)$ 的度。令 $a_i(x)=q_i(x)p(x)+k(x)r_i(x)$，则公钥 $pk=\langle a_0(x),a_1(x),\cdots,a_\tau(x),k(x)\rangle$，私钥 $sk=\langle p(x),k(x)\rangle$。

b) 加密算法 Encrypt(pk,m)。随机选取整数集 $S\subset\{0,$

收稿日期：2011-12-20；**修回日期**：2012-02-09　　**基金项目**：国家自然科学基金资助项目(70671096)；江苏省常州市“831 工程”科研基金资助项目(KYZ08043)

作者简介：于志敏(1973-)，男，吉林梅河口人，讲师，硕士，主要研究方向为网络与信息安全(619686056@qq.com)；古春生(1971-)，男，安徽繁昌人，副教授，博士，主要研究方向为网络与信息安全；景征骏(1978-)，男，江苏丹阳人，讲师，博士研究生，主要研究方向为网络与信息安全.

$1,\cdots,\tau\}$ 和度为 n 的多项式 $r(x)\in F_2[x]$。将明文 m 的二进制比特作为多项式 $m(x)$ 的系数,满足 $\deg(m(x))<\log n$,即 $m(x)\leftarrow m$。计算并输出密文 $c(x)\leftarrow m(x)+r(x)k(x)+\sum_{i\in S}a_i(x)$。

c)解密算法 Decrypt(sk, $c(x)$)。计算 $m(x)\leftarrow[[c(x)]_{p(x)}]_{k(x)}$,$m\leftarrow m(x)$。其中,表达式 $[a(x)]_{t(x)}$ 表示模 $t(x)$ 剩余,即 $a(x)\bmod t(x)$。

1.2　公钥方案的正确性证明

定理 1　上述公钥方案是正确的。

证明　假设(pk,sk)是 KeyGen(n)生成的密钥对,$c(x)\leftarrow$ Encrypt(pk, m)。由加密算法可知,$c(x)\leftarrow m(x)+r(x)k(x)+\sum_{i\in S}a_i(x)$,代入 $a_i(x)=q_i(x)p(x)+k(x)r_i(x)$,整理得 $c(x)=p(x)\sum_{i\in S}q_i(x)+k(x)(r(x)+\sum_{i\in S}r_i(x))+m(x)$。

由有限域 F_2 上的多项式计算可知,$\deg(k(x)(r(x)+\sum_{i\in S}r_i(x))+m(x))\leqslant n+\log n<\deg(p(x))$

因此,$[c(x)]_{p(x)}=k(x)(r(x)+\sum_{i\in S}r_i(x))+m(x)$。

又因 $\deg(k(x))>\deg(m(x))$,故 $m(x)\leftarrow[[c(x)]_{p(x)}]_{k(x)}$,$m\leftarrow m(x)$ 成立。

1.3　公钥方案复杂性分析

1.3.1　时间复杂性

a)密钥生成算法。KeyGen(n)中 $p(x)$、$r_i(x)$、$q_i(x)$、$k(x)$ 随机生成系数的运算次数是 $\tau(10n+n)+10n+\log n$。计算 $p(x)q_i(x)$ 所需运算次数为 $100\ n^2$,计算 $k(x)r_i(x)$ 所需运算次数 $n\log n$,$q_i(x)p(x)+k(x)r_i(x)$ 计算 τ 次。则计算 $a_i(x)=q_i(x)p(x)+k(x)r_i(x)(i=0,\cdots,\tau)$ 一共需要 $\tau(100n^2+n\log n)$ 次。由于方案中取 $\tau=n$,可知密钥的生成计算时间复杂性至多为 $O(n^3)$。显然,使用快速 Fourier 变换密钥生成计算时间可以改进到 $O(n^2\log n)$。

b)公钥加密算法。Encrypt(pk,m)是基于 $GF(2)$ 的计算。从定义可知公钥的每个分量 $\deg(a_i(x))=20\ n$,存储的空间约为 $20\ n$ bit。且知道加密时随机选择整数集 $S\subset\{0,1,\cdots,\tau\}$,显然 S 中元素个数 $|S|<n$,可知每次加密至多进行 $O(n^2)$ 次加法计算,使用快速 Fourier 加密计算时间可以改进到 $O(n\log n)$。

c)公钥解密算法。Decrypt(sk,$c(x)$)过程仅需两个模约减运算,计算时间复杂性至多为 $O(n^2)$,使用快速 Fourier 解密计算时间可以改进到 $O(n\log n)$。

1.3.2　空间复杂性

显然,方案中公钥比特数为 $(20n+2)\times O(n)=O(n^2)$,私钥比特数为 $(10n+1)+(n+1)=O(n)$。密文膨胀率为 $(20n+2)/(\log n)=O(n/\log n)$。

2　公钥方案安全性分析

本章首先定义有限域上近似最大公因多项式问题,然后归约证明第 1 章公钥方案的安全性等价于求解近似最大公因多项式问题。

定义 1　设 $p(x),q_i(x),k(x),r_i(x)\in F_2[x],i=0,1,\cdots,\tau$,满足 $\deg(p(x))>\deg(r_i(x))$。给定 $k(x)$ 和 $a_i(x)=q_i(x)p(x)+r_i(x)(i=0,1,\cdots,\tau)$,求解 $p(x)$ 问题称为近似最大公因多项式问题,其中 $r_i(x)$ 为添加的随机噪声多项式。

2.1　安全性归约证明

本小节归约证明上述公钥密码方案的安全性到求解最大近似公因多项式问题。在归约中重新组装了经典的 hard-core-bit 证明过程。给定一个随机选择的公钥,粗略展示了如果入侵者能够以不可忽略的优势预测随机加密后的明文,就能够用于恢复密钥。使用了如下分布:

$$D(p(x))=\left\{\begin{array}{l}\text{给定 } p(x),\text{随机选择 } q(x),R(x),\\ \text{满足 } \deg(q(x))=10n,\deg(R(x))=n+\log n,\\ \text{输出 } d(x)=q(x)p(x)+R(x)\end{array}\right\}$$

定理 2　给定安全参数 n,任何攻击者 A 对 1.1 节提出的加密模式具有不可忽略的优势 ε,就能利用 A 构建一个算法 B 来解决近似最大公因多项式问题,成功的概率至少为 ε/n。B 的运行时间是多项式 poly(n,A,$1/\varepsilon$)。

证明　使用 $Q_{p(x)}(z(x))$、$R_{p(x)}(z(x))$ 分别表示 $z(x)/p(x)$ 的商和剩余,因此 $z(x)$ 可以表示为 $z(x)=Q_{p(x)}(z(x))\times p(x)+R_{p(x)}(z(x))$。

假定 A 为加密模式的攻击者,公钥和密文作为它的输入,密文对应的正确明文作为输出,成功概率为不可忽略的 ε。

下面利用 A 构建算法 B 来解决近似最大公因多项式问题。对于给定度为 $10n$ 的多项式 $p(x)$,算法 B 可以访问 D($p(x)$)中任意多的样本,目标就是为了找到 $p(x)$。其步骤如下:

a)构建一个公钥。B 为模式构建一个公钥作为开始。注意公钥元素和 $D(p(x))$ 中样本多项式之间的差别,公钥元素是具有 $a_i(x)=p(x)q_i(x)+k(x)r_i(x)$ 结构的多项式。$D(p(x))$ 分布中任意一个多项式 $d(x)=q(x)p(x)+R(x)=q(x)p(x)+k(x)r(x)+R_{k(x)}(R(x))$,取任何一个满足 $R_{k(x)}(R(x))=0$ 的样本 $d_0(x)$ 作为公钥的第一个元素,即 $a_0(x)=d_0(x)$,因为 $k(x)$ 是公开的度为 $\log n$ 的多项式,所以获得这样的样本概率为 $1/2^{\log n}=1/n$。

接下来,B 从 $D(p(x))$ 中随机选取 τ 个样本 $b_1(x)$,$b_2(x),\cdots,b_\tau(x)$,并得到公钥其余元素 $a_i(x)=(k(x)\times b_i(x))\bmod a_0(x)$,最后得到公钥 $pk=\langle a_0(x),\cdots,a_\tau(x)\rangle$。从生成公钥的过程可以看出,选取满足 $R_{k(x)}(R(x))=0$ 的样本作为公钥的第一个元素,构建的公钥的分布统计上接近实际公钥的分布。

b)高精度 LSB 猜测的子程序。给定任意多项式 $z(x)$ 满足 $\deg(z(x))>\deg(p(x))$,B 通过 A 得到 $z(x)$ 除以 $p(x)$ 的商的 LSB(LSB 即为多项式的常数项)。为此,B 使用下面的子程序:

Sub learn_LSB:

输入:$z(x)$ 满足 $\deg(z(x))>\deg(p(x))$,公钥 $pk=\langle a_0(x),\cdots,a_\tau(x),k(x)\rangle$。

输出:LSB($Q_{p(x)}(z(x))$)。

for $j=1$ to poly(n)/ε do: //ε 是 A 的总优势

选择一个随机子集 $S_j\subset\{0,1,2,\cdots,\tau\}$,噪声 $r_j(x)$ 满足 $\deg(r_j(x))=n$ 和随机明文 $m_j(x)$ 满足 $\deg(m_j(x))<\log n$。

计算 $c_j(x)=z(x)+m_j(x)+k(x)r_j(x)+\sum_{i\in S_j}a_i(x)$

调用 A 获得密文 $c_j(x)$ 对应明文的预测 $M_j(x)\leftarrow A(pk,c_j(x))$。

计算 LSB($Q_{p(x)}(z(x))$)$\leftarrow$LSB($M_j(x)\oplus z(x)\oplus m_j(x)$)

循环结束后输出 LSB($Q_{p(x)}(z(x))$)的多数票。

步骤 b)第 3 行密文 $c_j(x)$ 的分布几乎等同于有效的加密多项式 $[R_{p(x)}(z(x))]_{k(x)}\oplus m_j(x)$。另外,因为 $p(x)$ 常数项为 1 且 $k(x)$ 常数项为 0,LSB($Q_{p(x)}(z(x))$)=LSB($R_{p(x)}(z(x))\oplus z(x)$)总是成立。综上所述,步骤 b)第 5 行 LSB($Q_{p(x)}(z(x))$)计算方法是正确的。由此可知,如果攻击者 A 具有不可忽略的优势 ε 猜到公钥 pk 加密的明文,那么算法 learn_LSB 经过 poly(n)/ε 次迭代,将具有无法阻挡的概率获得 LSB

$(Q_{p(x)}(z(x)))$。

c)PGCD 子程序。如果把封装了 A 获取 LSB$(Q_{p(x)}(z(x)))$的 learn_LSB 作为神谕,那么恢复私钥 $p(x)$ 就相当容易。最简单方法类似求最大公约数 GCD 算法。其基本思路是从公钥中任意选取两个元素 $z_1(x)$ 和 $z_2(x)$。算法 PGCD 对 $z_1(x)$、$z_2(x)$操作如下:

(a)如果 $z_2(x) > z_1(x)$ 那么交换它们 $z_1(x) \leftrightarrow z_2(x)$,保证 $z_1(x) > z_2(x)$。比较两个多项式大小是指从多项式高次数项依次比较其系数,下文与此相同,不再说明。

(b)使用神谕得到 LSB$(Q_{p(x)}(z_1(x)))$、LSB$(Q_{p(x)}(z_2(x)))$,如果两者都为 1,则用 $z_1(x) + z_2(x)$ 取代 $z_1(x)$,即 $z_1(x) \leftarrow z_1(x) + z_2(x)$,显然新的 LSB$(Q_{p(x)}(z_1(x)))$为 0。

(c)如果新的 LSB$(Q_{p(x)}(z_i(x)))(i = 0,1)$是 0,且 $z_i(x)$ 常数项亦为 0,则 $z_i(x) = z_i(x)/x$;如果 $z_i(x)$ 常数项不为 0,则 $z_i(x) = (z_i(x) + 1)/x$。

(d)重复步骤(a)~(c),当 $z_1(x)$ 和 $z_2(x)$ 都不为 0 且 $\deg(z_1(x)) = \deg(p(x))$ 或 $\deg(z_2(x)) = \deg(p(x))$ 停止迭代。如果 $z_1(x)$ 和 $z_2(x)$ 其中有一个度小于 $p(x)$ 的度,则重新选择一组公钥元素重新执行 PGCD。如果 $z_1(x)$ 和 $z_2(x)$ 正常停止迭代,则说明 $z_1(x)$ 和 $z_2(x)$ 最大公因式为 1。与两个整数互素的概率近似,两个随机多项式最大公因式为 1 的概率约为 $6/\pi^2 \approx 0.6$[10]。所以经过选取常数组 $z_1(x)$、$z_2(x)$,就能得到满足条件的结果。不失一般性,假定得到 $\deg(z_1(x)) = \deg(p(x))$。显然 $z_1(x) = p(x) + r(x)k(x)$。

(e)保留步骤(d)中得到的 $z_1(x)$,并在公钥中选取新的元素 $z^*(x)$,令 $z_2(x) = z^*(x)$,重复上述步骤(a)~(c)就可输出 $Q_{p(x)}(z^*(x))$的每一位,$Q_{p(x)}(z^*(x))$的值记做 $q^*(x)$,显然 $p(x) = Q_{q^*(x)}(z^*(x))$。

需要说明的是,在有限域上的上述各种操作都不会使 $z_i(x) \bmod p(x)$剩余的度增大,即满足 $\deg(R_{p(x)}(z_i(x))) < \deg(p(x))$。

2.2 B 成功概率和计算复杂性分析

2.1 节讨论了借助攻击者 A 的神谕,算法 B 能够有效地恢复私钥 $p(x)$。Learn_LSB 一共进行了 $\text{poly}(n)/\varepsilon$ 次加密和请求神谕的操作,因为神谕成功概率 ε 是不可忽略的,很显然此步骤计算复杂性是多项式的。由于两个多项式最大公因式为 1 的概率很大,所以 PGCD 只要尝试常数次即可得到满意结果。PGCD 中的除法实际上可以通过速度极快的移位操作实现,另外加上加法运算,总的计算复杂性为 $O(n^2)$。

综上所述,算法 B 计算复杂性为 A、n、$1/\varepsilon$ 的多项式。

$D(p(x))$分布中任意多项式可以表示为 $b(x) = q(x)p(x) + R(x) = q(x)p(x) + k(x)r(x) + R_{k(x)}(R(x))$,在设计的公钥模式中 $k(x)$是公开的度为 $\log n$ 的多项式,所以公钥分布与 $D(p(x))$分布吻合的概率为 $1/2^{\log n} = 1/n$。如果把发生这样事件称为理想事件的话,那么如果理想事件发生,就能借助神谕 A 恢复私钥 $p(x)$,所以算法 B 成功的概率为 ε/n,此概率同样是不可忽略的,这样就把本文的公钥方案归约到求解近似最大公因多项式问题之上了。

2.3 格规约攻击讨论

本文设计的公钥方案是基于有限域上问题的一个变种,其安全性基本等价于有限域上问题的难度。方案中给定 $a_i(x)$、$k(x)$作为公钥,这里将 $k(x)$作为公钥一部分是为了增加密文噪声,以抵抗基于格方法对该公钥方案的攻击。如果在密文中不添加噪声多项式 $k(x) \times r_0(x)$,方案就演变为一个多项式的背包方案,则可以基于公钥和密文构造多项式有限域上格 L 如下:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & a_0(x) \\ 0 & 1 & \cdots & 0 & a_1(x) \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_\tau(x) \\ 0 & 0 & \cdots & 0 & c(x) \end{pmatrix}$$

由于密文 $c(x) = m(x) + \sum_{i \in S} a_i(x)$,则向量$(0,0,\cdots,0, m(x))$在格 L 上。因此,使用 LLL[11] 算法和攻击背包方案的方法来攻击此公钥方案。

因此,本文构造的公钥方案其安全性系基于定理 1 中问题的计算难度假设,在 2.1 节已经归约到有限域上近似最大公因多项式问题上。近似最大公因多项式问题系新问题,与整数近似最大公因式[12]相对应,其具体计算难度还需要进一步研究,本文仅作为一个公开问题。

3 公钥方案性能比较

本文提出的公钥方案与 RSA、ElGamal 以及椭圆曲线离散对数等现有公钥方案在安全可靠性、计算速度等指标的比较如表 1 所示。

表 1 几种常用公钥方案与本文公钥方案的性能比较

指标	RSA	ElGamal	ECDLP	近似最大公因式
安全性及可靠性	基于大数因式分解,量子计算机已破解	基于有限域上离散对数的求解,量子计算机已破解	基于椭圆曲线离散对数,量子计算机已破解	基于求解近似最大公因多项式,目前求解算法未知
加/解密时间复杂性	$O(n \log^2 n)$[13]	$O(n \log^2 n)$	$O(n \log^2 n)$	$O(n \log n)$
公钥存储空间	2 048 bit	2 048 bit	160 bit	512k bit
密文膨胀率	1	2	2	$O(n/\log n)$

从表 1 中可看出,本文的方案虽然有公钥存储空间较大的缺点,但是加/解密时间在最坏的情况下也只有 $O(n \log n)$的开销,安全性和可靠性也能满足公钥系统的需求。虽然利用算法[13]RSA、ElGamal 和 ECDLP 在渐进的情况下基本达到 $O(n \log^2 n)$,但是在这些方案中要计算庞大的整数常数,而本文方案在有限域 F_2 上主要进行加法运算,特别适合计算机运算,所以速度优势明显。综合比较,基于近似最大公因多项式问题的公钥密码系统有一定的优势,在未来的工作中值得继续开展工作。

4 结束语

本文研究了有限域上近似最大公因多项式问题,并基于该问题难度提出了一个新的公钥方案,该方案仅需要进行有限域 F_2 上的多项式求和运算。因此,方案计算速度快,易于实现,具有 $O(n/\log n)$的密文膨胀率。

需要进一步研究的问题有:a)能否将本文的加密方案扩展为同态加密模式;b)求解近似最大公因多项式问题。

参考文献:

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal of Computing,1997,26(5):1484-1509. (下转第 2699 页)

(上接第 2692 页)

[2] PROOS J, ZALKA C. Shor's discrete logarithm quantum algorithm for elliptic curves[J]. Quantum Information and Computation, 2003, 3(4):317-344.

[3] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]//Proc of the 3rd International Symposium on Algorithmic Number Theory. London: Springer-Verlag, 1998: 267-288.

[4] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/average-case equivalence[C]//Proc of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM, 1997:284-293.

[5] REGEV O. New lattice-based cryptographic constructions[J]. Journal of the ACM, 2004, 51(6):899-942.

[6] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009:333-342.

[7] GOLDREICH O, GOLDWASSER S. On the limits of nonapproximability of lattice problems[J]. Journal of Computer and System Sciences, 2000, 60(3):540-563.

[8] AHARONOV D, REGEV O. Lattice problems in NP ∩ coNP[J]. Journal of the ACM, 2005, 52(5):749-765.

[9] KALTOFEN E, SHOUP V. Subquadratic-time factoring of polynomials over finite fields[J]. Mathematics of Computation, 1998, 67(223):1179-1197.

[10] luyuanhong. 任取两个正整数,它们互素的概率为 6/π^2 [EB/OL]. (2009-08-31)[2011-12-20]. http://bbs.mathchina.com/cgi-bin/topic.cgi?forum=5&topic=7377.

[11] LENSTRA A K, LENSTRA H W, LOVÁSZ L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen, 1982, 261(4):513-534.

[12] HOWGRAVE-GRAHAM N. Approximate integer common divisors[C]//Proc of International Conference on Cryptography and Lattices. Berlin: Springer, 2001:51-66.

[13] 唐勇,许金玲. 快速 RSA 算法研究[J]. 燕山大学学报, 2007, 31(6):481-484.