·学术论文与技术报告·

基于二进制冗余数的递归余数和算法*

陈 运** 龚耀寰

（电子科技大学通信与信息工程学院，电子工程学院 成都 610054）

【摘要】 介绍了递归余数和(RSR)算法，在此基础上又提出了一种改进的算法。理论分析表明，改进算法的迭代步数平均减少了17.2%。与传统的二进制算法(BR算法)相比，新算法的计算速度平均提高了约58.6%。

关 键 词 密码学； 公钥密码体制； RSA公钥密码体制； 快速算法

中图分类号 TN911.2； TN911.7

随着社会信息化进程的加速，不仅政治经济领域和生活领域发生了很大变化，军事领域也由机械战发展成为信息战。信息网络化是产生这些变革的基础，使信息交换规模、容量迅速扩大，速度大幅度提高，内容更加丰富。在信息战中通过网络控制和指挥的海、陆、空、天、电五位一体的立体战能更准确、更有效地打击敌方目标，赢得战争胜利。与此同时，信息安全成了倍受关注的问题。尤其是在信息战中，信息安全是保障信息网络正常运行、决定战争胜负的重要因素。

信息安全除了物理上的安全之外，更重要的是技术安全。运用高强度保密体制进行通信是实现技术安全的有效途径之一，公钥密码体制以其高强度保密性并可在公开信道上传输和分配密钥而倍受重视。在众多公钥密码体制中，以RSA(Rivest,Shamir&Adleman)公钥密码体制最为引人注目。其形式简单、保密性强，不但可以实现信息加密，还能实现认证、鉴别和数字签名等功能，是实现信息网络技术安全的理想密码体制之一。但RSA运算速度十分缓慢，成了实际应用的瓶颈问题。为了提高RSA公钥密码体制的运算速度，研究者一直在寻找快速算法。目前国际上流行的其他几种公钥密码体制与RSA有相同的核心运算，因此，研究RSA快速算法具有特别重要的意义。

本文提出的快速算法是在文献[1]提出的快速算法的基础上，通过减少运算的迭代步数，使RSA体制的运算速度进一步提高。

1 二进制算法简述

几乎所有的快速算法都是建立在二进制算法(Binary Representations, 简称BR算法)的基础上，下面对BR算法进行简要介绍。

RSA公钥密码体制的核心是大数幂剩余运算，其数学表达式为

$$y \equiv x^e \pmod N \tag{1}$$

$$x \equiv y^d \pmod N \tag{2}$$

式中

$$N=pq \tag{3}$$

且

$$ed=1 \pmod{\Phi(N)} \tag{4}$$

式中 x 为明文；y 为密文；p、q 均为大素数；e、d 均为正整数且满足式(4)的关系；$\Phi(N)$为 N 的欧拉数[2]。式(1)是加密算式，式(2)是解密算式。

1999年3月1日收稿

* 电子部预研基金资助项目

** 女 41岁 硕士 副教授

将指数 e 表示成二进制形式

$$e=\sum_{i=0}^{n-1} e_i 2^i \qquad e_i \in \{0,1\} \tag{5}$$

BR 算法是将幂剩余变成一系列平方剩余和乘同余的迭代，即将式(1)变为

$$y \equiv ((((((1\, x^{e_{n-1}})^2_N\ x^{e_{n-2}})_N)^2_N \cdots x^{e_1})_N)^2_N\ x^{e_0})_N \tag{6}$$

式中 $(\cdot)_N$表示括号中的数对 N 求模；$(\cdot)^2_N$表示先对括号中的数求平方再对 N 求模。

BR 算法的迭代步数为[3]

$$L=n+h(e) \tag{7}$$

式中 $h(e)$表示 e 的汉明重量。

2 递归余数和(RSR)算法简述

任何一个正整数 x 可表示成如下的二进制形式

$$x=\sum_{i=0}^{n-1} x_i 2^i \qquad x_i \in \{0,1\} \tag{8}$$

x 对 N 求模

$$x \equiv \sum_{i=0}^{n-1} x_i 2^i \pmod N \equiv \sum_{i=0}^{n-1} x_i (2^i \pmod N) \pmod N \equiv \sum_{i=0}^{n-1} x_i r_i \pmod N \tag{9}$$

式中 $r_i \equiv 2^i \pmod N$；$r_i \in \{0,1,\cdots,N-1\}$。

由于 x 只取 0、1 两个数，上述求模运算变成了 x 的非零位（x_i=1）相对应的一系列余数 r_i 之和。则

$$r_i \equiv 2\, r_{i-1} \pmod N \tag{10}$$

上式说明第 i 个余数可由前一个余数递推而来，即为递归余数和算法。

递归余数和的操作步骤为：将递归产生的余数序列预先排列成表，在幂剩余的每步迭代进行求模运算时，只需将乘积的二进制表达式中为 1 的各位找出来，查出相应的余数并求和即可。

例如 $2^i \pmod 7$

i	0	1	2	3	4	5…
2^i	2^0	2^1	2^2	2^3	2^4	2^5…
r_i	1	2	4	1	2	4…

计算 18 (mod 7)。$18=(10010)_2$为 1 的位是 2^1和 2^4，查表知 $r_1=r_4=2$，所以 18(mod 7)=4。余数表的大小为 $2n\times n$，当 n=200 bits 时，约需 4.88 k 字节的存贮空间。若 k 表示$[\Phi(p)\times\Phi(q)]$的最小公倍数($n \leqslant k < 2n$)，则存贮空间可缩小为$[(k-n)\times n]$[4]。

3 改进的递归余数和算法

上述算法的迭代步数 L 取决于指数的二进制长度及汉明重量—非零元素的个数。如果能够降低二进制指数的汉明重量，迭代步数必将减少。

用 $\bar{1}$ 表示-1，二进制的连 1 可表示成如下形式

$$\begin{aligned}
&(11)_2=(100)_2-(1)_2=10\,\bar{1}\\
&(111)_2=(1000)_2-(1)_2=100\,\bar{1}\\
&(1111)_2=(10000)_2-(1)_2=1000\,\bar{1}\\
&\qquad\cdots\cdots\\
&(\underbrace{11\cdots1}_{k\text{个}})
\end{aligned} \tag{11a}$$

当 110 和 1110 码型之后出现 s 个($s \geqslant 2$)连 1 时，也可进行如下二次代换

$$(11011)_2=(100000)_2-(1)_2-(100)_2=10000\,\bar{1}-(100)_2=100\,\bar{1}0\,\bar{1}$$

$$\cdots\cdots$$

$$(110\underbrace{11\cdots1}_{s})_2 = 100\ \bar{1}\ \underbrace{0\cdots0}_{(s-1)个}\ \bar{1} \tag{11b}$$

式(11a)和(11b)等号右边由 1、0、$\bar{1}$组成的数称为二进制冗余数。容易看出，当连 1 个数大于等于 3 或 110 及 1110 码型之后的连 1 个数大于等于 2 时，二进制冗余数的汉明重量低于二进制数的汉明重量。

用式(11a)和(11b)的方法对二进制序列中 3 个以上连 1 及 110 和 1110 码型之后两个以上连 1 进行替换。例如：$e=(101110101111)_2$，若 $R(e)$表示对应于 e 的二进制冗余数，则 $R(e)=11000\bar{1}0\bar{1}000\bar{1}$。不难验证 $e=R(e)$。但是 e 的汉明重量是 9，而 $R(e)$只有 5，明显小于 e。

若 e 的最高位含有 3 个以上连 1，则 $R(e)$的位数比 e 多 1，其他情况下两者位数相等[5]。

用 $R(e)$代替 e，式(1)变为

$$y \equiv x^{R(e)} \pmod{N} \tag{12}$$

式中　$R(e)=\sum_{i=0}^{s} e_i 2^i$，$s=n$ 或 $n-1$，$e_i \in \{1,0,\bar{1}\}$。

用式(6)的方法对式(12)进行迭代计算时，假设 A_i 代表第 i 步迭代的中间结果，则每步迭代含有三种基本运算之一：1) $A_i^2 \pmod N$；2) $A_i x \pmod N$；3) $A_i x^{-1} \pmod N$。x^{-1}是 x 对模 N 的乘逆，即

$$x\,x^{-1} \equiv 1 \pmod{N} \tag{13}$$

只要

$$(x, N)=1 \tag{14}$$

x^{-1} 必存在[2]。而几乎所有的 $x \in \{0,1,\cdots,N-1\}$都满足式(14)[5]。

我们构造了一种改进的递归余数和算法，步骤如下：1) 首先构造一个大小为$(n\times n)$或$[(k-n)\times n]$的余数表。n 为每步迭代结果的最高位数，$n \leqslant k < 2n$。2) 将加密指数 e 的二进制形式变换成二进制冗余数形式，记为 $R(e)$。变换原则是从 e 的高位开始，当 e 的二进制序列中有 k 个($k \geqslant 3$)连 1 时，用 $10\cdots0\bar{1}$将这 k 个连 1 替换掉。如果序列中 110 或 1110 码型之后有两个以上连 1 时，也可进行连续代换。如(11011)。第一次代换成 $1110\bar{1}$，第二次代换成 $100\bar{1}0\bar{1}$。再如(111011)，可连续代换成 $1000\bar{1}0\bar{1}$。3) 用欧几里德算法[2]，由式(14)求出 x 对模 N 的乘逆 x^{-1}。4) 从 $R(e)$的最高位开始，按式(6)迭代计算幂剩余 y。每步迭代含两种最基本运算：乘法和求模。若 A_i 为第 i 步迭代的中间结果，计算下述三种乘法之一：(1) $A'_{i+1}=A_i^2$；(2) $A'_{i+1}=A_i x$；(3) $A'_{i+1}=A_i x^{-1}$。5) 用递归余数和算法求模$A_{i+1}=A_{i+1}' \pmod N$。其具体操作步骤为：找出 A'_{i+1} 中的非零位，在事先建好的余数表中查出相应的余数并求和，即得到第 $i+1$ 步运算结果 A_{i+1}。

从 $R(e)$的最高位开始，重复执行步骤 4)和 5)，直至 $R(e)$的所有位都计算完为止。

容易推知，新算法的迭代步数为

$$L'=n+h[R(e)]-2 \tag{15}$$

式中　$h[R(e)]$为 $R(e)$的汉明重量。

4　新算法的速度分析

新算法是在递归余数和算法的基础上减少迭代步数得到的。递归余数和算法平均速度比传统的 BR 算法快 50%[1]。文献[5]提出的 RSA 改进算法是在乘同余对称特性快速算法的基础上采用二进制冗余数得到的，根据其理论分析，采用二进制冗余数后得到的速度改善是 17.2%。因此，新算法的平均速度比 BR 算法提高约50%+17.2×50%=58.6%。

5　结 束 语

递归余数和算法是目前 RSA 快速算法中最快的一种。本文新算法的运算速度超过了递归余数和算法。在实际应用系统中，RSA 算法的模数达到十进制的 200 位以上，指数达到 100 位以上，运

算速度十分缓慢。因而，得到 58.6%的速度改善是十分可观的。不过新算法事先建立余数表需要一定的时间，故仅适用于对长明文的加密。

参 考 文 献

1 Findley P A, Johnson B A. Modular exponentiation using recursive sums of residues. Advances in Cryptology-Euro CRYPTO-89, 1989:371~386

2 卢铁城. 信息加密技术. 成都：四川科学技术出版社，1989

3 陈 运. 一种新的快速 RSA 算法. 电子科技大学学报, 1995, 24(增刊):223~228

4 陈 运. 递归余数和算法分析. 通信保密. 1995, 63(3):66~69

5 陈 运. 基于乘同余对称特性的快速 RSA 算法的改进. 电子科技大学学报, 1997, 26(5):477~482

Recursive Sums of Residues Algorithm Based on Binary Redundant Representations

Chen Yun Gong Yaohuan

(Institute of Telecommunication & Information Engineering, Institute of Electronic Engineering,UEST of China Chengdu 610054)

Abstract Recursive sums of residues algorithm(RSR algorithm) is briefly introduced in this paper. An improved RSR algorithm is presented, which bases on binary redundant representations (BRR algorithm). It is shown by theoretical analysis that the proposed algorithm decreases the recursive steps by 17.2% on average. Compared with traditional BR algorithm, the new algorithm obtains the speed improvement by about 58.6% on average.

Key words cryptography; public-key cryptosystem; RSA public-key cryptosystem; fast algorithm

·科研成果介绍·

新型光纤免疫传感测量仪的研究

主研人员：王志玉 唐 雷 李毓琦 何 俊 周 波 黄文珍

新型光纤免疫传感测量仪的主要性能指标为：检测波长 400~760 mm，重现性为 0.27%。其结构简单、新颖的光纤传感头与用户的固相被测敏感膜注有机结合，构成新型的反射、分离式光纤免疫传感器，从而可单独、灵活地处理膜注，实现膜注一次性制备，多次使用，缩短检测时间踊机多项检测等一系列优点，该测量仪可对细菌、病毒、免疫球蛋白、激素、肿瘤细胞等物质进行检测。

·科 卞·